
# ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

**ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ**

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ


# Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης για Κατανεμημένα Περιβάλλοντα

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ


**Ευγενία Ι. Παπαγιαννακοπούλου**



Αθήνα, Ιανουάριος 2014

# ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

**ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ**

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ


# Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης για Κατανεμημένα Περιβάλλοντα

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ


**Ευγενία Ι. Παπαγιαννακοπούλου**


Συμβουλευτική Επιτροπή: Ιάκωβος Στ. Βενιέρης
Δήμητρα-Θεοδώρα Ι. Κακλαμάνη
Νικόλαος Κ. Ουζούνογλου

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 20η Ιανουαρίου 2014

| | | |
|---|---|---|
| ..... | ..... | ..... |
| Ι. Στ. Βενιέρης | Δ.-Θ. Ι. Κακλαμάνη | Ν. Κ. Ουζούνογλου |
| Καθηγητής Ε.Μ.Π. | Καθηγήτρια Ε.Μ.Π. | Καθηγητής Ε.Μ.Π. |
| ..... | ..... | ..... |
| Γ. Στασινόπουλος | Χρ. Ι. Κακλαμάνης | Κ. Κοντογιάννης |
| Καθηγητής Ε.Μ.Π. | Καθηγητής Παν. Πατρών | Αν. Καθηγητής Ε.Μ.Π. |

.....
Κ. Λαμπρινουδάκης
Αν. Καθηγητής Παν. Πειραιά

Αθήνα, Ιανουάριος 2014

.....
**Ευγενία Ι. Παπαγιαννακοπούλου**
Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

# Περίληψη

Μία σύγχρονη τάση στην εξέλιξη των συστημάτων λογισμικού συνίσταται στην απομάκρυνση από τη λογική της κάθετης ολοκλήρωσης και την υιοθέτηση πιο ευέλικτων αρχιτεκτονικών που βασίζονται στη δυναμική διασυνεργασία κατανεμημένων και ετερογενών οντοτήτων. Ωστόσο, η αλληλεπίδραση διαφορετικών φορέων και ετερογενών συστημάτων προϋποθέτει και συνεπάγεται διαμοιρασμό πόρων και χρήση και διακίνηση ευαίσθητων πληροφοριών, εγείροντας ταυτόχρονα ζητήματα ακεραιότητας και διαθεσιμότητας των υποκείμενων πόρων με σαφή αντίκτυπο στην ιδιωτικότητα.

Στο πλαίσιο αυτό, η Διατριβή έχει σαν αντικείμενο την ανάπτυξη τεχνολογιών ελέγχου πρόσβασης και χρήσης σε κατανεμημένα περιβάλλοντα, με έμφαση στην προστασία της ιδιωτικότητας. Βασικός στόχος είναι η ολιστική θεώρηση του ελέγχου πρόσβασης, ο οποίος δεν εστιάζει σε μεμονωμένες ενέργειες, αλλά η διαδικασία λήψης απόφασης για την παροχή πρόσβασης λαμβάνει επιπλέον υπόψη την αλληλεπίδραση μεταξύ συστημάτων.

Τη βάση του συστήματος συνιστά το Σημασιολογικό Μοντέλο Πληροφοριών που παρέχει αφαιρετική αναπαράσταση των βασικών οντοτήτων των κατανεμημένων συστημάτων, καθώς και τις μεταξύ τους συσχετίσεις, ενώ θεμελιώνεται στη βάση των απαιτήσεων που προκύπτουν από την επεξεργασία των νομικών και κανονιστικών διατάξεων που αφορούν την προστασία των δεδομένων. Το Σημασιολογικό Μοντέλο Πολιτικών χρησιμοποιείται για την προδιαγραφή κανόνων πάνω στις οντότητες του μοντέλου πληροφοριών, οι οποίοι χαρακτηρίζονται από υψηλό βαθμό εκφραστικότητας και δύνανται να περιγράψουν περιορισμούς που τα υφιστάμενα μοντέλα αδυνατούν να ενσωματώσουν. Μεταξύ άλλων, το μοντέλο επιτρέπει τον προσδιορισμό κανόνων σε οποιοδήποτε επίπεδο αφαίρεσης, καθώς και σύνθετων εξαρτήσεων μεταξύ ενεργειών και οντοτήτων, επιτρέποντας την προδιαγραφή προηγμένων περιορισμών διαχωρισμού και σύζευξης καθηκόντων.

Και τα δύο μοντέλα υλοποιούνται από σημασιολογικές οντολογίες, οι οποίες αποτελούν τη βάση για την εξαγωγή γνώσης. Η τελευταία πραγματοποιείται σε δύο στάδια. Το πρώτο αφορά την εξαντλητική εξαγωγή γνώσης σε μη πραγματικό χρόνο και περιλαμβάνει την εξαγωγή μετακανόνων και την εξαγωγή γνώσης από το σύνολο των κανόνων, παρέχοντας τη δυνατότητα για αποτίμηση μεμονωμένων ενεργειών πρόσβασης. Το δεύτερο στάδιο, εκμεταλλευόμενο τα αποτελέσματα του πρώτου, αφορά τη σε πραγματικό

χρόνο λήψη αποφάσεων αναφορικά με την αλληλεπίδραση μεταξύ των κατανεμημένων συστημάτων, τα επιτρεπτά σενάρια εκτέλεσης και την εξαγωγή συμπληρωματικών οδηγιών που πρέπει να ακολουθούνται.

**Λέξεις κλειδιά:** Έλεγχος πρόσβασης και χρήσης, κατανεμημένα περιβάλλοντα, ιδιωτικότητα, προστασία προσωπικών δεδομένων, σημασιολογικό μοντέλο, οντολογία, διαχωρισμός και σύζευξη καθηκόντων.

# Abstract

A current trend in the evolution of software systems consists in moving from the logic of vertical integration towards the adoption of more flexible architectures based on the dynamic and loosely-coupled interoperation of distributed and heterogeneous entities. However, the interaction between different actors and heterogeneous systems requires and, at the same time, involves resource sharing and use and handling of sensitive information, while raising issues regarding the integrity and availability thereof, with a clear consequent impact on privacy.

In this context, the goal of the present Thesis is the development of access and usage control technologies tailored for the specific needs of distributed environments, with special emphasis laid on the protection of privacy. Essentially, it aims at handling security and privacy requirements for distributed environments in a holistic and comprehensive manner, meaning that access decisions are not taken considering the actions "in isolation", but taking also into account the operational and data flows representing the interaction between systems.

The proposed system relies on a rich Semantic Information Model that provides abstract representation of the basic entities of distributed systems, as well as the relations between them, while it is ultimately grounded on the requirements stemming from the elaboration of legal and regulatory provisions regarding data protection. On the other hand, the Semantic Policy Model is leveraged for the specification of rules upon the entities of the information model, which are characterized by a high degree of expressiveness and may describe constraints that the existing models fail to incorporate. Among others, the proposed model provides flexibility to express concepts and rules at any level of abstraction, and it allows for the specification of complex dependencies among actions and entities, as well as sophisticated separation and binding of duty constraints.

Both models are implemented by means of semantic ontologies, which constitute the basis for knowledge extraction. The latter takes place in two stages. The first phase concerns exhaustive knowledge extraction in an offline manner, including the extraction of metarules and the subsequent knowledge extraction from the rules set, and it provides for the assessment of individual access actions. The second phase, exploiting the results of the first one, refers to real-time decisions regarding the interaction between distributed systems, the permitted execution scenarios and the extraction of additional instructions to be followed.

**Keywords:** Access and usage control, distributed environments, privacy, personal data protection, semantic model, ontology, separation and binding of duty.

# Ευχαριστίες

Η διατριβή αποτελεί το προϊόν της ερευνητικής μου δραστηριότητας στο εργαστήριο Ευφυών Επικοινωνιών και Δικτύων Ευρείας Ζώνης του ΕΜΠ. Αναγνωρίζοντας ότι η διατριβή μου θα ήταν αδύνατον να πραγματοποιηθεί χωρίς την καθοδήγηση και τη συμπαράσταση κάποιων σημαντικών για εμένα ανθρώπων, θα ήθελα στο σημείο αυτό να ευχαριστήσω όλους όσοι με βοήθησαν και με στήριξαν στην πορεία μου αυτή.

Ξεκινώντας από τη συμβουλευτική μου επιτροπή, θα ήθελα ιδιαίτερα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κύριο Ιάκωβο Βενιέρη, Καθηγητή ΕΜΠ, για την εμπιστοσύνη που επέδειξε στις δυνατότητές μου, για τις σημαντικές ευκαιρίες που μου προσέφερε ώστε να εξελιχθώ σαν μηχανικός και να διευρύνω τους επιστημονικούς μου ορίζοντες, αλλά και για την αδιάλειπτη υποστήριξη και συμπαράσταση όλα αυτά τα χρόνια, σε ερευνητικό και όχι μόνο επίπεδο. Συνεχίζοντας, θα ήθελα να ευχαριστήσω την Καθηγήτρια ΕΜΠ κυρία Δήμητρα Κακλαμάνη, για την άριστη συνεργασία, για την προθυμία να με βοηθήσει όποτε χρειάστηκα τη συμβουλή της και για τις πάντα εύστοχες υποδείξεις της. Επίσης, θερμές ευχαριστίες στους Καθηγητές ΕΜΠ κύριο Νικόλαο Ουζούνογλου και κύριο Γεώργιο Στασινόπουλο και στον Καθηγητή Πανεπιστημίου Πατρών κύριο Χρήστο Κακλαμάνη, που πάντοτε ευγενικοί στήριξαν την προσπάθεια μου, και φυσικά στον Αν. Καθηγητή ΕΜΠ κύριο Κώστα Κοντογιάννη και στον Αν. Καθηγητή Πανεπιστημίου Πειραιά κύριο Κωνσταντίνο Λαμπρινουδάκη, που μου έκαναν την τιμή να συμπεριληφθούν στην επταμελή επιτροπή μου.

Έναυσμα της διατριβής αποτέλεσε η άμεση εμπλοκή μου στο ευρωπαϊκό ερευνητικό πρόγραμμα DEMONS. Τα ερεθίσματα που εισέπραξα και οι τεχνικές προκλήσεις με τις οποίες ήρθα σε επαφή καθ' όλη τη διάρκεια εκπόνησης του εν λόγω ερευνητικού προγράμματος λειτούργησαν ως παρακαταθήκη, παρέχοντάς μου τις βάσεις για την ολοκλήρωση της εργασίας, ενώ παράλληλα, στα πλαίσια του έργου, μου δόθηκε η ευκαιρία να συνεργαστώ με αξιόλογους μηχανικούς και ερευνητές, κάποιους από τους οποίους έχω την τιμή να θεωρώ πλέον φίλους και θα ήθελα να τους ευχαριστήσω για τη στήριξή τους αλλά και τις πολύτιμες συμβουλές τους.

Φυσικά, ένα μεγάλο ευχαριστώ οφείλω σε όλα τα παιδιά του εργαστηρίου. Για τη δημιουργική συνεργασία, για τις καταστάσεις που βιώσαμε μαζί και που μέσα από αυτές ωριμάσαμε, αλλά και για όλες εκείνες τις στιγμές αποσυμπίεσης. Ιδιαίτερα όμως θα ήθελα

να ευχαριστήσω τους στενούς μου συνεργάτες, και δεύτερη πλέον οικογένεια, Γιώργο Λιουδάκη, Μαρίζα Κουκοβίνη και Νίκο Δέλλα. Πέρα από το γεγονός ότι η συμβολή τους στην ερευνητική μου εργασία υπήρξε καθοριστική, χάρη σε αυτούς θα θυμάμαι πάντα τα τελευταία πολύ έντονα χρόνια με νοσταλγία κι ένα μεγάλο χαμόγελο.

Άφησα για το τέλος τους πιο σημαντικούς για εμένα ανθρώπους, την οικογένειά μου, το Νίκο μου και τους πολύτιμους φίλους μου, οι οποίοι μου στάθηκαν υπομονετικά όλα αυτά τα χρόνια, μου έδωσαν το κουράγιο να συνεχίσω όταν αισθάνθηκα "λίγη" και με συγχώρεσαν για όλες τις φορές που δεν ήμουν εκεί για αυτούς. Χωρίς την αγάπη και τη στήριξή τους δε θα τα είχα καταφέρει.

# Πίνακας Περιεχομένων


**Σελ.**

**Περίληψη** **vi**

**Abstract** **viii**

**Ευχαριστίες** **x**

**Πίνακας Περιεχομένων** **xi**

**Πίνακας Σχημάτων** **xv**

**1 Εισαγωγή** **1**

1.1 Κατανεμημένα περιβάλλοντα . . . . . 1

1.2 Ιδιωτικότητα και Απαιτήσεις . . . . . 4

1.3 Διάρθρωση της Διατριβής . . . . . 8

**2 Τεχνολογίες Ελέγχου Πρόσβασης** **11**

2.1 Έλεγχος Πρόσβασης . . . . . 11

2.1.1 Διακριτικός Έλεγχος Πρόσβασης (DAC) . . . . . 12

2.1.2 Υποχρεωτικός Έλεγχος Πρόσβασης (MAC) . . . . . 12

2.1.3 Έλεγχος Πρόσβασης Βάσει Ρόλων (RBAC) . . . . . 14

2.1.4 Έλεγχος Πρόσβασης Βάσει Ιδιοτήτων (ABAC) . . . . . 15

2.1.5 Έλεγχος Πρόσβασης Βάσει Οργανισμού (OrBAC) . . . . . 16

2.1.6 Η Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης (XACML) . . . 18

2.2 Έλεγχος Πρόσβασης για Προστασία της Ιδιωτικότητας . . . . . 22

2.2.1 Έλεγχος Πρόσβασης Βάσει Σκοπού (PBAC) . . . . . 23
2.2.2 Έλεγχος Πρόσβασης Βάσει Ρόλων για Προστασία της Ιδιωτικότητας (P-RBAC) . . . . . 26
2.2.3 Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση Σκοπού (PuRBAC) . . 28
2.2.4 Το Μοντέλο Ελέγχου Πρόσβασης PRIME . . . . . 29
2.2.5 Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης PRISM . . . . . 31
2.2.6 Παρατηρήσεις . . . . . 34
2.3 Χρήση των Οντολογιών στον Έλεγχο Πρόσβασης . . . . . 35
2.3.1 Οντολογική Υλοποίηση του Μοντέλου RBAC . . . . . 35
2.3.2 Σημασιολογική Επέκταση του Μοντέλου Ιδιοτήτων της XACML . . . . 37
2.3.3 Επίγνωση Πλαισίου Βασισμένη σε Οντολογίες . . . . . 38
2.3.4 Οντολογικός Προσδιορισμός Προτιμήσεων Ιδιωτικότητας . . . . . 40
2.3.5 Σημασιολογικός Έλεγχος Πρόσβασης σε Υπηρεσίες Κοινωνικής Δικτύωσης . . . . . 41
2.3.6 Παρατηρήσεις . . . . . 42

**3 Γενικές Αρχές της Προτεινόμενης Λύσης** **45**
3.1 Μοντέλο Συστήματος . . . . . 45
3.2 Διμερής Συσχετισμός . . . . . 47
3.2.1 Εργασίες . . . . . 47
3.2.2 Ροές . . . . . 48
3.3 Βασικές Αρχές της Προτεινόμενης Λύσης . . . . . 49
3.4 Απαιτήσεις για Εξαγωγή Γνώσης . . . . . 53
3.5 Αφηρημένο Μοντέλο για Έλεγχο Πρόσβασης για Προστασία της Ιδιωτικότητας 55

**4 Μοντέλο Ελέγχου Πρόσβασης και Χρήσης** **57**
4.1 Μοντέλο Πληροφοριών . . . . . 58
4.1.1 Δεδομένα και Τύποι Δεδομένων . . . . . 61
4.1.2 Χρήστες και Ρόλοι . . . . . 62
4.1.3 Λειτουργίες . . . . . 63
4.1.4 Πληροφορίες Πλαισίου . . . . . 65

4.1.5 Σκοποί . . . . . 65
4.1.6 Ιδιότητες . . . . . 67
4.2 Ενέργειες και Οντότητες . . . . . 68
4.2.1 Ενέργεια . . . . . 68
4.2.2 Οντότητες Ενέργειας . . . . . 70
4.3 Κανόνες Ελέγχου Πρόσβασης και Χρήσης . . . . . 71
4.4 Κληρονομικότητα των Εξουσιοδοτήσεων . . . . . 74
4.5 Διαχωρισμός και Σύζευξη Καθηκόντων . . . . . 77

**5 Οντολογική Υλοποίηση του Μοντέλου Ελέγχου Πρόσβασης και Χρήσης 79**
5.1 Σημασιολογικό Μοντέλο Πληροφοριών . . . . . 80
5.2 Σημασιολογικό Μοντέλο Πολιτικών . . . . . 82
5.2.1 Εκφράσεις και Λογικές Σχέσεις . . . . . 82
5.2.2 Ενέργειες και Οντότητες . . . . . 85
5.2.3 Οντολογικοί Κανόνες Ελέγχου Πρόσβασης . . . . . 87
5.2.4 Σκελετοί . . . . . 89
5.2.5 Διαχωρισμός και Σύζευξη Καθηκόντων . . . . . 89

**6 Εξαγωγή Γνώσης 91**
6.1 Εξαγωγή Μετακανόνων . . . . . 92
6.2 Συλλογιστική στη Βάση των Κανόνων Ελέγχου Πρόσβασης . . . . . 98
6.2.1 Επέκταση του Σημασιολογικού Μοντέλου Πολιτικών . . . . . 98
6.2.2 Μηχανισμός Εξαγωγής Γνώσης . . . . . 102

**7 Αποτίμηση Αιτημάτων 109**
7.1 Οδηγίες Εξουσιοδότησης . . . . . 110
7.2 Διαδικασία Επαλήθευσης Διμερούς Συσχετισμού . . . . . 111
7.3 Έλεγχος Συμμόρφωσης Σκοπών . . . . . 114
7.4 Εξαγωγή των Αυτόνομα Έγκυρων Εργασιών . . . . . 115
7.5 Επαλήθευση του Διμερούς Μετασυσχετισμού . . . . . 121
7.5.1 Εντοπισμός Απόλυτων Συγκρούσεων . . . . . 123

7.5.2 Επαλήθευση της Αλληλεπίδρασης των Εργασιών . . . . . 125
7.5.3 Προσδιορισμός Απαραίτητων και Απαγορευμένων Εργασιών . . . . . 132
7.6 Επαλήθευση Διμερών Συσχετισμών στο Πλαίσιο Επαλήθευσης Ροής Εργασιών 136

**8 Αξιολόγηση της Προτεινόμενης Λύσης 139**
8.1 Αξιολόγηση σε Σχέση με τις Απαιτήσεις του Συστήματος . . . . . 139
8.1.1 Έλεγχος Πρόσβασης — Πολυδιάστατος Προσδιορισμός Δικαιωμάτων Πρόσβασης . . . . . 139
8.1.2 Σκοπός Συλλογής και Επεξεργασίας Δεδομένων . . . . . 140
8.1.3 Έλεγχος Ροής Πληροφορίας . . . . . 141
8.1.4 Μη Διασύνδεση . . . . . 142
8.1.5 Διαχωρισμός και Σύζευξη Καθηκόντων . . . . . 143
8.1.6 Συμπληρωματικές Ενέργειες . . . . . 143
8.1.7 Επίγνωση Πλαισίου . . . . . 144
8.1.8 Ετερογενή Περιβάλλοντα . . . . . 144
8.1.9 Μηχανισμοί Ασφάλειας . . . . . 145
8.1.10 Σημασιολογική Αναπαράσταση Πληροφοριών . . . . . 145
8.2 Αξιολόγηση Επίδοσης . . . . . 146

**9 Συμπεράσματα — Μελλοντική Εργασία 151**

**Βιβλιογραφία 153**

**Δημοσιεύσεις 165**

**Συνοπτικό Βιογραφικό Σημείωμα 167**

# Πίνακας Σχημάτων

**Σελ.**


1 Οντότητες και έννοιες του μοντέλου OrBAC. . . . . 17

2 Διάγραμμα ροής πληροφορίας XACML . . . . . 20

3 Οντολογία PRISM. . . . . 33

4 Μοντέλο Συστήματος . . . . . 46

5 Διμερής Συσχετισμός . . . . . 47

6 Σημασιολογικό Μοντέλο Πληροφοριών (Information Model Ontology — IMO). 81

7 Σημασιολογικό Μοντέλο Πολιτικών (Policy Model Ontology — PMO). . . . . 83

8 Παράδειγμα Οντολογικού Κανόνα Ελέγχου Πρόσβασης και Χρήσης . . . . . 83

9 Λογικές Σχέσεις . . . . . 84

10 Παράδειγμα Εξαγωγής Μετακανόνα . . . . . 99

11 Επέκταση της Οντολογίας PMO. . . . . 100

12 Εξαγωγή Επιτρεπόμενης Ενέργειας . . . . . 107

13 Υπό εξέταση διμερής συσχετισμός . . . . . 113

14 Παράδειγμα Εξαγωγής Αυτόνομα Έγκυρων Εργασιών . . . . . 120

15 Παράδειγμα εξαγωγής αυτόνομα έγκυρων εργασιών από μη πλήρως προσδιορισμένη εργασία . . . . . 121

16 Διμερείς μετασυσχετισμοί που προέκυψαν για τον υπό εξέταση διμερή συσχετισμό . . . . . 122

17 Επαλήθευση Αλληλεπίδρασης χωρίς Μετασχηματισμό . . . . . 127

18 Περίπτωση Επιλογής Μεταδιδόμενων Δεδομένων . . . . . 129

19 Περίπτωση Προβολής Μεταδιδόμενων Δεδομένων . . . . . 130
20 Περίπτωση Αλλαγής Κατάστασης Μεταδιδόμενων Δεδομένων . . . . . 132
21 Συνδυαστική Προσθήκη Εργασιών Μετασχηματισμού . . . . . 133
22 Εξαγωγή Οδηγιών Απαίτησης Εκτέλεσης . . . . . 135
23 Επαλήθευση Ροής Εργασιών . . . . . 138

# Κεφάλαιο 1

# Εισαγωγή

Η διατριβή πραγματεύεται την ανάπτυξη τεχνολογιών ελέγχου πρόσβασης και χρήσης σε κατανεμημένα περιβάλλοντα, με έμφαση στην προστασία της ιδιωτικότητας. Το παρόν κεφάλαιο παρέχει μία εισαγωγή στις έννοιες των κατανεμημένων περιβαλλόντων και της ιδιωτικότητας, ενώ σκιαγραφεί τους ιδιαίτερους κινδύνους που διατρέχει η ιδιωτικότητα λόγω της εξέλιξης και καθιέρωσης των υποκείμενων τεχνολογιών και συνοψίζει τις απαιτήσεις που πρέπει να ικανοποιεί ένα τεχνολογικό σύστημα που στοχεύει στην προστασία των προσωπικών δεδομένων.

## 1.1 Κατανεμημένα περιβάλλοντα

Μία σύγχρονη τάση στην εξέλιξη των συστημάτων λογισμικού συνίσταται στην απομάκρυνση από τη λογική της κάθετης ολοκλήρωσης και την υιοθέτηση πιο ευέλικτων αρχιτεκτονικών που βασίζονται στη δυναμική διασυνεργασία κατανεμημένων και ετερογενών οντοτήτων, δημιουργώντας *κατανεμημένα περιβάλλοντα*. Έτσι, ενώ μέχρι πρότινος τα συστήματα σχεδιάζονταν με στόχο να λειτουργούν αυτόνομα και ανεξάρτητα, πλέον χαρακτηρίζονται από δυναμικότητα, διαμοιρασμό πόρων και αποκέντρωση λειτουργιών. Ετερογενή συστήματα είναι σε θέση να συνεργάζονται *κατά περίπτωση* (*ad hoc*), αναπτύσσοντας ελαστικούς δεσμούς μεταξύ τους, για την εξυπηρέτηση κάποιου σκοπού, ενώ είναι δυνατόν να συμμετέχουν σε διάφορες τέτοιες συνεργασίες για την παροχή διαφορετικής κάθε φορά λειτουργικότητας.

Η τάση αυτή αντανακλάται στις τεχνολογίες *Ιστού Δεύτερης Γενιάς* (*Web 2.0*) [1], όπου η παροχή των υπηρεσιών ξεφεύγει από το μοντέλο του μοναδικού παρόχου υπηρεσίας, στις τεχνολογίες *Υπολογιστικού Νέφους* (*Cloud Computing*) [2] που χρησιμοποιούνται κατά κόρον για το διαμοιρασμό κατανεμημένων πόρων, στη δημιουργία *Εικονικών Οργανισμών* (*Virtual Organisations*) [3] και στην έλευση του *Διαδικτύου των Πραγμάτων* (*Internet of Things*) [4]. Χαρακτηριστικό παράδειγμα κατανεμημένων αρχιτεκτονικών αποτελούν οι

*Υπηρεσιοστρεφείς Αρχιτεκτονικές* (*Service Oriented Architectures — SOAs*) [5], οι οποίες προωθούν την ενσωμάτωση λογικής εφαρμογών μέσα σε *υπηρεσίες* ελαστικά συνδεδεμένες μεταξύ τους, διευκολύνοντας την επαναχρησιμοποίηση και τη δυναμική κατανομή των απαραίτητων πόρων. Η πλέον δημοφιλής σχετική τεχνολογία είναι οι *Υπηρεσίες Ιστού* (*Web Services*) [6], με τη διαδικασία *σύνθεσης Υπηρεσιών Ιστού* [7] να οδηγεί στη δημιουργία πιο πολύπλοκων υπηρεσιών με αθροιστική λειτουργικότητα.

Η υιοθέτηση κατανεμημένων αρχιτεκτονικών αλλάζει σημαντικά τα δεδομένα σε ό,τι αφορά την προστασία των υποκείμενων πόρων. Πράγματι, η συνεργασία μεταξύ διαφορετικών φορέων και ετερογενών συστημάτων προϋποθέτει και συνεπάγεται διαμοιρασμό πόρων, καθώς και χρήση και διακίνηση ευαίσθητων πληροφοριών, εγείροντας ταυτόχρονα ζητήματα ακεραιότητας και διαθεσιμότητας των υποκείμενων πόρων. Επομένως, η εξέλιξη και η καθιέρωση των σχετικών τεχνολογιών, πέραν της πολυπλοκότητας που εισάγουν στην προστασία της ασφάλειας των κατανεμημένων συστημάτων, έχουν αντίκτυπο και στην *ιδιωτικότητα*, δηλαδή την *"αξίωση των ατόμων, ομάδων και οργανισμών να καθορίζουν το χρόνο, τον τρόπο και την έκταση αναφορικά με τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων"* [8], η οποία αποτελεί αναμφίβολα ένα από τα πιο σημαντικά ζητήματα αναφορικά με τα δικαιώματα του ανθρώπου που επηρεάζονται από την εξελισσόμενη "Εποχή της Πληροφορίας". Με βάση τα παραπάνω, καθίσταται σαφές ότι η ασφάλεια των πληροφοριών και η προστασία της ιδιωτικότητας, συμπεριλαμβανομένης της εμπιστευτικότητας των επιχειρηματικών πληροφοριών, αποτελούν βασικές απαιτήσεις. Από τη μία πλευρά, οι οργανισμοί πρέπει να εμπιστεύονται τις πηγές πληροφοριών και άλλους οργανισμούς, ενώ από την άλλη, οι τελικοί χρήστες των εν λόγω συστημάτων δηλώνουν ιδιαιτέρως ανήσυχοι αναφορικά με την προστασία των προσωπικών τους δεδομένων και της ιδιωτικής τους ζωής.

Συνεπώς, τα κατανεμημένα περιβάλλοντα, πέρα από τις προφανείς θετικές πλευρές τους, δημιουργούν σοβαρούς κινδύνους· ειδικά σε ό,τι αφορά την ιδιωτικότητα, αυτό οφείλεται κυρίως στους παρακάτω λόγους:

- Στο πλαίσιο της λειτουργίας ενός κατανεμημένου συστήματος ενδέχεται να απαιτείται η συλλογή δεδομένων ή/και η αλληλεπίδραση πολλαπλών ετερογενών οργανισμών και αντίστοιχα η ανταλλαγή, ο συσχετισμός και ο διαμοιρασμός δεδομένων, καθώς και η διασύνδεση αρχείων, με αποτέλεσμα η προστασία προσωπικών δεδομένων να καθίσταται παράμετρος που είναι δύσκολο να ελεγχθεί.

- Με δεδομένο ότι ορισμένοι τύποι δεδομένων αποτελούν ταυτοποιητικά στοιχεία για προσωπικές πληροφορίες σε πολλαπλές υποκείμενες βάσεις δεδομένων, ενδέχεται η *συνδεσιμότητα* (*linkability*) μεταξύ των δεδομένων σε κατανεμημένα συστήματα που αλληλεπιδρούν να είναι ευθεία και άμεση. Ως εκ τούτου, ελλοχεύει ο κίνδυνος συνδυασμού δεδομένων από ετερόκλητες πηγές και η ολοκλήρωσή τους με αποτέλεσμα τη δημιουργία λεπτομερών προφίλ των χρηστών και τη δυνατότητα εξαγωγής περαι-

τέρω συμπερασμάτων.

- Η διασυνεργασία συνήθως αφορά οντότητες, π.χ., οργανισμούς, που ακολουθούν διαφορετικές πολιτικές, ενώ είναι δυνατόν να ξεφεύγει από τα διοικητικά σύνορα μίας χώρας. Στο πλαίσιο αυτό, ο έλεγχος της ροής πληροφορίας μεταξύ των αλληλεπιδρώντων συστημάτων καθίσταται απαραίτητος.

Σε αυτό το πλαίσιο, οι υποκείμενες τεχνολογίες θα πρέπει να προβλέπουν μηχανισμούς ώστε να τηρούνται οι προϋποθέσεις για την προστασία της ιδιωτικότητας. Οι μηχανισμοί ασφάλειας, όπως η χρήση κρυπτογραφίας και ο έλεγχος πρόσβασης (access control) σε συστήματα και δεδομένα, αποτελούν τη στοιχειώδη βάση για την προστασία των κατανεμημένων πόρων και της ιδιωτικότητας, χωρίς ωστόσο να αποτελούν πανάκεια. Οι μέχρι σήμερα ερευνητικές προσπάθειες στην περιοχή του ελέγχου πρόσβασης παρουσιάζουν μία εγγενή αδυναμία ανταπόκρισης στους κινδύνους που δημιουργούνται από τα ιδιαίτερα χαρακτηριστικά των κατανεμημένων αρχιτεκτονικών και των σχετικών τεχνολογιών, καθώς είτε δεν έχουν σχεδιασθεί με γνώμονα τη λειτουργία τέτοιων συστημάτων, είτε δεν καλύπτουν ολόκληρο το φάσμα των υποκείμενων απαιτήσεων.

Υπό το πρίσμα των προαναφερθέντων ζητημάτων, στα πλαίσια της διδακτορικής διατριβής αναπτύχθηκε ένα καινοτόμο μοντέλο ελέγχου πρόσβασης και χρήσης, βασισμένο στις ειδικές ανάγκες που δημιουργεί η λειτουργία των κατανεμημένων περιβαλλόντων και στις απαιτήσεις που απορρέουν από τη νομοθεσία για την προστασία της ιδιωτικότητας. Εν προκειμένω, η ιδιαίτερη έμφαση που δίνεται στο ζήτημα της ιδιωτικότητας οφείλεται στο γεγονός ότι η ιδιωτικότητα αποτελεί την πλέον πολύπλοκη και πολυδιάστατη περίπτωση χρήσης στην ευρύτερη περιοχή της ασφάλειας. Η ικανοποίηση των απαιτήσεων για προστασία της ιδιωτικότητας, και κατ' επέκταση των απαιτήσεων που αφορούν την ασφάλεια, οδηγεί στην προδιαγραφή πολιτικών που είναι σε θέση να προστατέψουν όλα τα είδη πόρων των υποκείμενων συστημάτων, χωρίς να εστιάζουν αποκλειστικά στην προστασία προσωπικών δεδομένων, αλλά στοχεύοντας στην ευρύτερη έννοια της διατήρησης της εμπιστευτικότητας της πληροφορίας.

Το προτεινόμενο μοντέλο ελέγχου πρόσβασης και χρήσης στηρίζεται σε ένα σημασιολογικά πλούσιο Μοντέλο Πληροφοριών, το οποίο περιλαμβάνει όλη την απαραίτητη για τη λειτουργία ενός κατανεμημένου περιβάλλοντος γνώση και πάνω στο οποίο θεμελιώνεται το Μοντέλο Πολιτικών για τον ορισμό των σχετικών κανόνων. Οι τελευταίοι, σε συνδυασμό με τις συσχετίσεις μεταξύ των υποκείμενων εννοιών όπως αυτές περιγράφονται στο Μοντέλο Πληροφοριών, καθιστούν δυνατή την αποτίμηση της αλληλεπίδρασης μεταξύ δύο συστημάτων και υπαγορεύουν τον ενδεχόμενο μετασχηματισμό της, λαμβάνοντας υπόψη μία σειρά από παραμέτρους, όπως δικαιώματα πρόσβασης, σκοπούς, περιορισμούς διαχωρισμού και σύζευξης καθηκόντων, εξαρτήσεις μεταξύ των ενεργειών πρόσβασης και παραμέτρους πλαισίου. Βασική συνεισφορά της προτεινόμενης λύσης αποτελεί το γεγονός ότι ο έλεγχος πρόσβασης δεν εστιάζει σε μεμονωμένες ενέργειες, αλλά η διαδικα-

σία λήψης απόφασης για την παροχή πρόσβασης λαμβάνει υπόψη τόσο τη ροή λειτουργίας όσο και τη ροή δεδομένων στο πλαίσιο της αλληλεπίδρασης μεταξύ συστημάτων, με αποτέλεσμα μία ολιστική θεώρηση του ελέγχου πρόσβασης και ροή πληροφορίας με επίγνωση ιδιωτικότητας.

## 1.2 Ιδιωτικότητα και Απαιτήσεις

Η ιδιωτικότητα αναγνωρίζεται ως θεμελιώδες ανθρώπινο δικαίωμα από την Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα των Ηνωμένων Εθνών [9], καθώς και από τον Καταστατικό Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης [10], και ως εκ τούτου προστατεύεται από τη σχετική νομοθεσία σε όλες τις δημοκρατικές χώρες του κόσμου.

Σημαντικό ορόσημο για την ιδιωτικότητα υπήρξε η κωδικοποίηση των θεμελιωδών της αρχών από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (Organisation for Economic Co-operation and Development — OECD) [11] το 1980, οι οποίες στη συνέχεια αποτυπώθηκαν στην Ευρωπαϊκή Οδηγία 95/46/ΕΚ [12] "*για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη διακίνηση των δεδομένων αυτών*". Η Οδηγία αυτή αποτελεί το πιο επιδραστικό κείμενο στη νομοθεσία περί ιδιωτικότητας σε παγκόσμιο επίπεδο, επηρεάζοντας και πολλές χώρες εκτός Ευρώπης στην κατεύθυνση της θέσπισης παρόμοιων νόμων, ενώ μαζί με τις συμπληρωματικές μεταγενέστερες Οδηγίες 2002/58/ΕΚ [13], 2006/24/ΕΚ [14] και 2009/136/ΕΚ [15] προδιαγράφουν ένα πλήθος βασικών αρχών και απαιτήσεων που θα πρέπει να πληρούνται σε σχέση με την ιδιωτικότητα.

Αξίζει επίσης να σημειωθεί ότι τον Ιανουάριο του 2012 κατατέθηκε η πρόταση για τον "Κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων)" [16]. Ο προτεινόμενος Κανονισμός βασίζεται στις αρχές της Οδηγίας 95/46/ΕΚ, την οποία επεκτείνει και συμπληρώνει, ενώ με την ψήφισή του ουσιαστικά θα την καταργήσει. Τα κυριότερα νέα σημεία τα οποία εισάγονται από την εν λόγω πρόταση αφορούν το λεγόμενο δικαίωμα του προσώπου στο οποίο αναφέρονται τα δεδομένα *"να λησμονηθεί"*, το δικαίωμα διαγραφής, μη περαιτέρω διάδοσης και περιορισμού της επεξεργασίας των δεδομένων του, και το ρητό καθορισμό των υποχρεώσεων του υπευθύνου επεξεργασίας οι οποίες απορρέουν από τις αρχές της προστασίας των δεδομένων ήδη *από τον σχεδιασμό* και *εξ ορισμού*.

Σε εθνικό επίπεδο, η Ελλάδα κατοχυρώνει συνταγματικά ως ατομικό και κοινωνικό δικαίωμα το δικαίωμα στην προστασία προσωπικών δεδομένων και στο απόρρητο της επικοινωνίας. Συγκεκριμένα, το Άρθρο 9Α του Συντάγματος της Ελλάδας [17] αναφέρει ότι

"*καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων*", ενώ προβλέπει ότι η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη Αρχή. Επιπλέον, το Άρθρο 19 ορίζει ως απόλυτα απαραβίαστο το απόρρητο των επικοινωνιών, προβλέποντας ωστόσο το νομοθετικό ορισμό εγγυήσεων υπό τις οποίες η δικαστική Αρχή δε δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Προβλέπει επίσης το νομοθετικό ορισμό των σχετικών με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης Αρχής που διασφαλίζει το απόρρητο.

Η νομοθεσία για τα προσωπικά δεδομένα στην Ελλάδα συνίσταται κυρίως από τους Νόμους 2472/1997 [18] και 3471/2006 [19], οι οποίοι αποτελούν την υλοποίηση των Ευρωπαϊκών Οδηγιών 95/46/ΕΚ και 2002/58/ΕΚ, αντίστοιχα, στο ελληνικό δίκαιο. Αντικείμενο του Νόμου 2472/1997 είναι "*η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής*", ενώ ο Νόμος 3471/2006 εστιάζει στην προστασία προσωπικών δεδομένων και τη διασφάλιση του απορρήτου στον τομέα των ηλεκτρονικών επικοινωνιών. Υφίστανται δε δύο αρμόδιες ανεξάρτητες Αρχές, οι οποίες υλοποιούν, αντίστοιχα, τα Άρθρα 9Α και 19 του Συντάγματος: η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)[1], η οποία ιδρύθηκε με το Νόμο 2472/1997, και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)[2], η οποία συστάθηκε με το Νόμο 3115/2003 [20]. Τέλος, πρόσφατα μεταφέρθηκε στο ελληνικό νομικό σύστημα και η Οδηγία 2006/24/ΕΚ με το Νόμο 3917/2011 [21].

Οι βασικές αρχές και απαιτήσεις της ευρωπαϊκής και εθνικής νομοθεσίας μπορούν να συνοψιστούν ως εξής:

- *Νομιμότητα της επεξεργασίας των δεδομένων*: Το σύστημα θα πρέπει να είναι σε θέση να εξετάζει εάν η συλλογή και επεξεργασία των δεδομένων βρίσκεται σε συμφωνία με τους ισχύοντες νόμους και κανονισμούς.

- *Σκοπός της επεξεργασίας των δεδομένων*: Το σύστημα θα πρέπει να παρέχει τα μέσα για την ταυτοποίηση των σκοπών της συλλογής και επεξεργασίας δεδομένων, οι οποίοι θα πρέπει να είναι έννομοι και να κοινοποιούνται με σαφήνεια στο υποκείμενο των δεδομένων. Επιπλέον, θα πρέπει το σύστημα να είναι σε θέση να πραγματοποιεί έλεγχο των σκοπών συλλογής και επεξεργασίας, ούτως ώστε να αποφεύγεται η περαιτέρω επεξεργασία δεδομένων για σκοπούς άλλους από εκείνους για τους οποίους πραγματοποιήθηκε η συλλογή τους.

- *Αναγκαιότητα, καταλληλότητα και αναλογικότητα των δεδομένων υπό επεξεργασία*: Το σύστημα θα πρέπει να είναι σε θέση να εγγυηθεί ότι υφίστανται επεξεργασία

[1]Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, http://www.dpa.gr
[2]Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, http://www.adae.gr.

μόνο δεδομένα τα οποία είναι λειτουργικά, απαραίτητα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται.

- *Ποιότητα των δεδομένων υπό επεξεργασία*: Το σύστημα θα πρέπει να φροντίζει ότι τα δεδομένα υπό επεξεργασία είναι σωστά, ακριβή και ενημερωμένα. Σε αντίθετη περίπτωση, τα δεδομένα θα πρέπει να διορθώνονται, να ενημερώνονται ή να διαγράφονται.

- *Ταυτοποιήσιμα δεδομένα*: Το σύστημα θα πρέπει να παρέχει τα μέσα ούτως ώστε τα δεδομένα που υφίστανται επεξεργασία να διατηρούνται σε μορφή που να ταυτοποιούν το υποκείμενο των δεδομένων μόνο για το χρονικό διάστημα το οποίο είναι απαραίτητο προκειμένου να επιτευχθούν οι σκοποί της επιδιωχθείσας επεξεργασίας.

- *Ειδικές κατηγορίες δεδομένων — ευαίσθητα δεδομένα*: Το σύστημα θα πρέπει να είναι σε θέση να εγγυηθεί ότι η επεξεργασία ειδικών κατηγοριών δεδομένων θα πραγματοποιείται σε συμφωνία με τις συγκεκριμένες απαιτήσεις οι οποίες ορίζονται από την ισχύουσα νομοθεσία. Για παράδειγμα, ο Νόμος 2472/1997 ορίζει ως ευαίσθητα *"τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων"*, ενώ το Άρθρο 6 του Νόμου 3471/2006 θεσπίζει ειδικούς κανόνες για τα δεδομένα θέσης και κίνησης.

- *Πληροφόρηση, συγκατάθεση και λοιπά δικαιώματα των υποκειμένων των δεδομένων*: Το σύστημα θα πρέπει να έχει τη δυνατότητα να ενημερώνει τα υποκείμενα των δεδομένων αναφορικά με την επεξεργασία των δεδομένων τους. Επιπλέον, το σύστημα θα πρέπει να εγγυάται ότι η ρητή συγκατάθεση των υποκειμένων των δεδομένων θα απαιτείται προκειμένου να πραγματοποιηθεί επεξεργασία των δεδομένων, εφόσον η ισχύουσα νομοθεσία ορίζει σχετικά, ενώ η επεξεργασία οποιασδήποτε μορφής των δεδομένων θα λαμβάνει χώρα λαμβάνοντας υπόψη τις προτιμήσεις των υποκειμένων των δεδομένων αναφορικά με την ιδιωτικότητα. Επιπροσθέτως, το σύστημα θα πρέπει να παρέχει τη δυνατότητα στα υποκείμενα των δεδομένων να εξασκούν τα δικαιώματα πρόσβασης στα δεδομένα τους τα οποία προβλέπονται από την ισχύουσα νομοθεσία. Τέτοια δικαιώματα πρόσβασης αφορούν –για παράδειγμα– την ενημέρωση των δεδομένων τα οποία βρίσκονται αποθηκευμένα σε κάποια βάση δεδομένων, τη διαγραφή τους, το δικαίωμα αποτροπής της επεξεργασίας τους, κλπ.

- *Ειδοποιήσεις και λοιπές αρμοδιότητες/εξουσιοδοτήσεις των αρμοδίων Αρχών*: Το σύστημα θα πρέπει να έχει τη δυνατότητα να παρακολουθεί τη συμμόρφωση με την απαίτηση για την παροχή ειδοποιήσεων προς την αρμόδια Αρχή Προστασίας Δεδομένων, καθώς και την παροχή οποιασδήποτε άλλης αρμοδιότητας/εξουσιοδότησης

διαθέτει η Αρχή. Επιπλέον, το σύστημα θα πρέπει να παρέχει τα μέσα επικοινωνίας μεταξύ της Αρχής και του συστήματος.

- *Εποπτεία και επιβολή προστίμων*[3]: Οι αρμόδιες Αρχές Προστασίας Δεδομένων θα πρέπει να διαθέτουν τη δυνατότητα εποπτείας και ελέγχου όλων των ενεργειών συλλογής και επεξεργασίας προσωπικών δεδομένων.

- *Διασύνδεση δεδομένων*: Η διασύνδεση δεδομένων μπορεί να λάβει χώρα μόνο υπό συγκεκριμένους όρους και σε κάθε περίπτωση κατόπιν ενημέρωσης προς την αρμόδια Αρχή. Επιπλέον, σύμφωνα με το Άρθρο 8 του Νόμου 3471/2006, *"εάν ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα, ή εάν η διασύνδεση έχει ως συνέπεια την αποκάλυψη ευαίσθητων δεδομένων, ή εάν για την πραγματοποίηση της διασύνδεσης, πρόκειται να γίνει χρήση ενιαίου κωδικού αριθμού, η διασύνδεση επιτρέπεται μόνον με προηγούμενη άδεια της Αρχής (άδεια διασύνδεσης)"*.

- *Ασφάλεια και εμπιστευτικότητα*: Το σύστημα θα πρέπει να είναι ασφαλές, ούτως ώστε να είναι σε θέση να εγγυηθεί την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, προστατεύοντάς τα από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας, εξασφαλίζοντας επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Επιπλέον, το σύστημα θα πρέπει να είναι σε θέση να αποτρέπει την οποιαδήποτε υποκλοπή ή παρακολούθηση των δεδομένων εκτός εάν υπάρχει η ρητή συγκατάθεση του υποκειμένου των δεδομένων ή εφόσον προβλέπεται από την ισχύουσα νομοθεσία για λόγους που τεκμηριώνονται από το δημόσιο συμφέρον.

- *Περιορισμός πρόσβασης*: Το σύστημα τα πρέπει να παρέχει διαδικασίες εξουσιοδοτημένης πρόσβασης στα δεδομένα, το επίπεδο της οποίας θα πρέπει απαραιτήτως να διαφοροποιείται με βάση διάφορα κριτήρια, όπως το είδος των δεδομένων καθεαυτών, τους ρόλους και τους υποκείμενους σκοπούς. Επιπλέον, κάθε πρόσβαση σε δεδομένα θα πρέπει να καταγράφεται.

- *Αποθήκευση*: Το σύστημα θα πρέπει να διαγράφει ή καθιστά ανώνυμα με αυτόματο τρόπο εκείνα τα δεδομένα για τα οποία η αναγκαιότητά τους για την επίτευξη κάποιου σκοπού έχει λήξει ή για τα οποία έχει παρέλθει το οριζόμενο βάσει της νομοθεσίας χρονικό διάστημα διατήρησής τους.

- *Μεταφορά και διάδοση δεδομένων*: Όταν μέρος της επεξεργασίας ανατίθεται για εκτέλεση σε τρίτα μέρη, πρέπει να παρέχονται συγκεκριμένες εγγυήσεις ότι η συνακόλουθη επεξεργασία των δεδομένων είναι σύμφωνη με τους υποκείμενους κανονισμούς και συμβάσεις με το υποκείμενο των δεδομένων. Επιπλέον, ενώ η διαβίβαση

[3]Εξυπακούεται ότι η επιβολή προστίμων δεν είναι δυνατό να αποτελεί αντικείμενο ενός τεχνολογικού συστήματος· αναφέρεται ωστόσο εδώ για λόγους πληρότητας.

δεδομένων προς χώρες – μέλη της Ευρωπαϊκής Ένωσης είναι ελεύθερη (σύμφωνα πάντα με τα παραπάνω), για τις υπόλοιπες χώρες ισχύουν ειδικοί κανόνες και συνθήκες. Γενικότερα, θα πρέπει να εξετάζονται τόσο ο τύπος των μεταφερόμενων δεδομένων όσο και οι συνθήκες υπό τις οποίες πραγματοποιείται η διατομεακή μεταφορά αυτών.

Οι παραπάνω απαιτήσεις θα αποτελέσουν τη βάση για το σχεδιασμό της προτεινόμενης λύσης, όπως θα περιγραφεί αναλυτικά στη συνέχεια της διατριβής.

## 1.3 Διάρθρωση της Διατριβής

Η διατριβή αποτελείται από συνολικά εννέα κεφάλαια. Πέρα από το παρόν εισαγωγικό κεφάλαιο, το περιεχόμενο των υπολοίπων κεφαλαίων συνοψίζεται ως ακολούθως.

Στο δεύτερο κεφάλαιο πραγματοποιείται επισκόπηση των προτύπων καθώς και των διαφόρων ερευνητικών προσπαθειών που πραγματοποιήθηκαν μέχρι σήμερα στον τομέα του ελέγχου πρόσβασης και χρήσης. Ιδιαίτερη αναφορά γίνεται σε εκείνες τις τεχνολογίες οι οποίες, όπως και η διατριβή, κάνουν χρήση σημασιολογικών οντολογιών. Από την ανάλυση αναδεικνύονται οι περιορισμοί των υφιστάμενων προσεγγίσεων και προσδιορίζονται χαρακτηριστικά που η λύση που προτείνεται από τη διατριβή θα πρέπει να καλύπτει.

Στη συνέχεια, το τρίτο κεφάλαιο περιγράφει τις γενικές αρχές της προτεινόμενης λύσης, παρέχοντας μία γενική επισκόπηση και παραθέτοντας κάποιες βασικές έννοιες. Στο πλαίσιο αυτό, τεκμηριώνεται το μοντέλο συστήματος και εισάγεται η έννοια του διμερούς συσχετισμού, που αναφέρεται στη στοιχειώδη αλληλεπίδραση μεταξύ δύο οντοτήτων, και των εννοιών που τον αποτελούν, δηλαδή των εργασιών που εκτελούν οι οντότητες και της μεταξύ τους ροής. Στη συνέχεια, καταγράφονται οι θεμελιώδεις αρχές που πρέπει να διέπουν ένα μοντέλο ελέγχου πρόσβασης σε κατανεμημένα περιβάλλοντα, βάσει των αρχών και απαιτήσεων για προστασία της ασφάλειας και της ιδιωτικότητας, αλλά και των διακριβωμένων ελλείψεων και αναγκών των υφιστάμενων τεχνολογιών. Οι αρχές αυτές αποτελούν ουσιαστικά τις απαιτήσεις που πρέπει να ικανοποιεί η προτεινόμενη λύση, από τις οποίες πηγάζουν και οι απαιτήσεις για εξαγωγή γνώσης από το μοντέλο ελέγχου πρόσβασης, οι οποίες ακολούθως επισκοπούνται. Τέλος, συνοψίζεται το μοντέλο ελέγχου πρόσβασης σε υψηλό επίπεδο αφαίρεσης.

Το τέταρτο κεφάλαιο αποτελεί την αναλυτική τεκμηρίωση του προτεινόμενου μοντέλου ελέγχου πρόσβασης και χρήσης. Αφού αναλυθεί το υποκείμενο μοντέλο πληροφοριών που παρέχει αφαιρετική αναπαράσταση των βασικών οντοτήτων των κατανεμημένων συστημάτων και περιγράφει τις μεταξύ τους συσχετίσεις, εισάγονται οι βασικές έννοιες της ενέργειας και των οντοτήτων που συμμετέχουν σε αυτήν. Οι έννοιες αυτές αποτελούν τη βάση πάνω στην οποία θεμελιώνονται οι κανόνες ελέγχου πρόσβασης και χρήσης, οι οποίοι παρουσιάζονται στη συνέχεια. Η προσέγγιση που προτείνεται από τη

διατριβή αναφορικά με την προδιαγραφή των κανόνων αποτελεί μία από τις σημαντικές καινοτομίες της, καθώς οι κανόνες, λόγω της εκφραστικότητάς τους και των χαρακτηριστικών τους, δύνανται να περιγράψουν περιορισμούς που τα υφιστάμενα μοντέλα αδυνατούν να ενσωματώσουν. Επιπλέον, το κεφάλαιο αυτό διερευνά θέματα κληρονομικότητας των κανόνων, ενώ κλείνει με την περιγραφή των μηχανισμών για διαχωρισμό και σύζευξη καθηκόντων.

Στο πέμπτο κεφάλαιο, παρουσιάζεται ο τρόπος υλοποίησης του μοντέλου ελέγχου πρόσβασης και χρήσης χρησιμοποιώντας σημασιολογικές οντολογίες. Ουσιαστικά πρόκειται για δύο οντολογίες που υλοποιούν, αντίστοιχα, το σημασιολογικό μοντέλο πληροφοριών και το σημασιολογικό μοντέλο πολιτικών, με το δεύτερο να προδιαγράφει κανόνες πάνω στα στοιχεία του πρώτου. Η οντολογική υλοποίηση καθαυτή παρουσιάζει πληθώρα καινοτόμων χαρακτηριστικών, κυρίως σε ό,τι αφορά την αναπαράσταση διαφόρων δομών, όπως οι λογικές σχέσεις. Κατά τον τρόπο αυτό, το μοντέλο ελέγχου πρόσβασης και χρήσης επωφελείται από τη σημασιολογία και τις δυνατότητες εξαγωγής συμπερασμάτων των οντολογιών, ενώ καθίσταται δυνατή η προδιαγραφή πολύπλοκων συσχετισμών.

Το έκτο κεφάλαιο είναι αφιερωμένο στην εξαγωγή γνώσης από το μοντέλο ελέγχου πρόσβασης και χρήσης. Περιγράφεται όλη η διαδικασία της απαραίτητης συλλογιστικής, προκειμένου να καλυφθούν πλήρως οι υποκείμενες ανάγκες για τη λήψη των σχετικών αποφάσεων σε κατανεμημένα συστήματα. Η προσέγγιση που ακολουθείται είναι εκείνη της εκ των προτέρων συλλογιστικής, που αναφέρεται στην ενδελεχή εξαγωγή γνώσης σε μη πραγματικό χρόνο, ούτως ώστε το σύστημα να δύναται να ανταπεξέλθει στα αιτήματα πρόσβασης, όταν αυτά υποβάλλονται, στον ελάχιστο δυνατό χρόνο.

Το έβδομο κεφάλαιο πραγματεύεται θέματα εξαγωγής γνώσης και λήψης αποφάσεων σε πραγματικό χρόνο. Το κέντρο βάρους της αντίστοιχης συλλογιστικής είναι ο διμερής συσχετισμός, όπως τεκμηριώθηκε στο τέταρτο κεφάλαιο, που αντανακλά την αλληλεπίδραση μεταξύ δύο συστημάτων. Έχοντας ως αφετηρία τη λήψη ενός διμερούς συσχετισμού, το σύστημα τον επαληθεύει και αποφαίνεται αναφορικά με την εκτέλεσή του, σε ό,τι αφορά τόσο τους επιτρεπτούς συνδυασμούς εκτέλεσης, όσο και τις συμπληρωματικές οδηγίες που πρέπει να ακολουθηθούν.

Η αξιολόγηση της προτεινόμενης λύσης αποτελεί το αντικείμενο του όγδοου κεφαλαίου. Η αξιολόγηση αφορά διάφορους άξονες, που αναδεικνύουν τα πλεονεκτήματα της προτεινόμενης από τη διατριβή λύσης. Ιδιαίτερης σημασίας είναι η αξιολόγηση της λύσης σε ό,τι αφορά την ικανοποίηση των βασικών απαιτήσεων που τεκμηριώθηκαν ως οι επιμέρους στόχοι της προτεινόμενης λύσης.

Τέλος, το ένατο κεφάλαιο αποτελεί τον επίλογο της διατριβής, υπογραμμίζοντας κάποια βασικά συμπεράσματα, αλλά και σκιαγραφώντας τις βασικές κατευθύνσεις που θα αποτελέσουν τους άξονες της συνέχισης της έρευνας έχοντας ως βάση τη λύση που προτείνεται από τη διατριβή.

# Κεφάλαιο 2

# Τεχνολογίες Ελέγχου Πρόσβασης

Στο κεφάλαιο αυτό παρουσιάζονται κάποιες σύγχρονες προσεγγίσεις για έλεγχο πρόσβασης, με ιδιαίτερη έμφαση στα μοντέλα εκείνα που στοχεύουν στην προστασία της ιδιωτικότητας, ενώ επίσης διερευνώνται οι ερευνητικές προσπάθειες που κάνουν χρήση οντολογιών για τη μοντελοποίηση και εφαρμογή ελέγχου πρόσβασης.

## 2.1 Έλεγχος Πρόσβασης

Μία σημαντική απαίτηση για τα συστήματα διαχείρισης πληροφοριών είναι η προστασία της πληροφορίας από καταχρηστική κοινοποίηση ή τροποποίηση, δηλαδή η προστασία της *εμπιστευτικότητας* και της *ακεραιότητας*, αντίστοιχα. Ο έλεγχος πρόσβασης αποτελεί βασική τεχνολογία για την επίτευξη αυτού του στόχου [22]˙ κάθε αίτημα πρόσβασης ελέγχεται και αποτιμάται. Τα συστήματα ελέγχου πρόσβασης περιλαμβάνουν *πολιτικές*, *μοντέλα* και *μηχανισμούς*. Οι πολιτικές αποτελούν οδηγίες υψηλού επιπέδου που καθορίζουν τον τρόπο με τον οποίο ελέγχεται η πρόσβαση και λαμβάνονται οι αποφάσεις για παροχή πρόσβασης. Εν συνεχεία, μία πολιτική ορίζεται φορμαλιστικά μέσω ενός μοντέλου και επιβάλλεται μέσω μηχανισμών ελέγχου πρόσβασης.

Ωστόσο, η πολυπλοκότητα των απαιτήσεων προστασίας που θα πρέπει να ικανοποιούν τα σύγχρονα συστήματα καθιστά τον ορισμό των πολιτικών ελέγχου πρόσβασης κάθε άλλο παρά ασήμαντη διαδικασία. Για παράδειγμα, σε πολλές περιπτώσεις οι ιδιότητες ενός χρήστη, και όχι η ταυτότητα του, αποτελούν το κριτήριο για την παροχή πρόσβασης, ή διαφορετικά συστήματα ενδέχεται να συνεργάζονται, διατηρώντας όμως παράλληλα την αυτονομία τους όσον αφορά τον έλεγχο της πρόσβασης στους πόρους τους [23][24]. Η παρούσα ενότητα αποτελεί επισκόπηση της εξέλιξης του ελέγχου πρόσβασης, από τα βασικά μοντέλα *Διακριτικού Ελέγχου Πρόσβασης*, *Υποχρεωτικού Ελέγχου Πρόσβασης* και *Ελέγχου Πρόσβασης Βάσει Ρόλων*, στον *Έλεγχο Πρόσβασης Βάσει Ιδιοτήτων* και πιο σύνθετα μοντέλα, όπως το *Μοντέλο Ελέγχου Πρόσβασης Βάσει Οργανισμού*. Τέλος, παρου-

σιάζεται η *Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης* που αποτελεί το πιο διαδεδομένο πρότυπο για την προδιαγραφή πολιτικών.

### 2.1.1 Διακριτικός Έλεγχος Πρόσβασης (DAC)

Τα μοντέλα *Διακριτικού Ελέγχου Πρόσβασης* (*Discretionary Access Control — DAC*) [25] προέρχονται κυρίως από υλοποιήσεις λειτουργικών συστημάτων. Σε ένα στατικό κόσμο, τα μοντέλα αυτού του τύπου αντιπροσωπεύουν τα *δικαιώματα πρόσβασης* (*access modes*) *ανά πόρο* και *ανά χρήστη* (ή ομάδες χρηστών), καταγεγραμμένα με τη μορφή ενός *πίνακα πρόσβασης*. Η βασική αρχή των μοντέλων αυτών είναι ότι οι χρήστες διατηρούν το δικαίωμα να ορίζουν δικαιώματα σε αντικείμενα των οποίων έχουν την κυριότητα.

Υπάρχουν διάφορες προσεγγίσεις για την υλοποίηση του πίνακα πρόσβασης, με τις πιο διαδεδομένες να αποτελούν οι *Λίστες Ελέγχου Πρόσβασης* (*Access Control Lists — ACLs*), στις οποίες τα αντικείμενα συσχετίζονται με ένα σύνολο ζευγών χρήστη-δικαιωμάτων, οι *δυνατότητες* (*capabilities*), όπου ο κάθε χρήστης συσχετίζεται με ζεύγη αντικειμένου-δικαιωμάτων, και οι *σχέσεις εξουσιοδότησης* (*authorization relations*), οι οποίες παραπέμπουν σε σχεσιακές βάσεις δεδομένων, με την κάθε σχέση να προσδιορίζει ένα δικαίωμα πρόσβασης ενός υποκειμένου σε ένα αντικείμενο.

Οι πολιτικές διακριτικού ελέγχου πρόσβασης εξελίχθηκαν ώστε να συμπεριλάβουν *συνθήκες* (*conditions*) για τον περιορισμό της ισχύος των εξουσιοδοτήσεων, καθώς και τον προσδιορισμό αφαιρετικών δομών για τη δημιουργία *ιεραρχιών* χρηστών και αντικειμένων. Η συμπερίληψη ιεραρχιών με τη σειρά της οδήγησε στη θεώρηση θετικών και αρνητικών εξουσιοδοτήσεων, για τη διαχείριση *εξαιρέσεων* λόγω της διάδοσης των εξουσιοδοτήσεων κατά μήκος των εν λόγω ιεραρχιών.

Η περιορισμένη δυνατότητα εφαρμογής των παραπάνω μοντέλων, οφείλεται όχι μόνο στα προβλήματα που σχετίζονται με την αποθήκευση της πληροφορίας που αφορά στην έλεγχο πρόσβασης, αλλά κυρίως με την αδυναμία να διαχειριστούν δυναμικά μεταβαλλόμενες καταστάσεις, όπου νέοι χρήστες εισέρχονται στο σύστημα, παλιοί διαγράφονται, ενώ στην δεύτερη αυτή περίπτωση, θα πρέπει να αποφασιστεί ποια από τα δικαιώματα που αυτοί οι χρήστες είχαν δημιουργήσει θα παραμείνουν μετά τη διαγραφή τους και ποια όχι. Για την αντιμετώπιση ενδεχόμενης *αλυσιδωτής ανάκλησης δικαιωμάτων* (*cascading revocation of rights*), έχουν προταθεί διάφορες λύσεις (π.χ., [26]) είναι ωστόσο προφανές ότι οι δυνατότητες του μοντέλου να διαχειριστεί μεγάλο αριθμό χρηστών και δυναμικά μεταβαλλόμενες συνθήκες είναι εξαιρετικά περιορισμένες.

### 2.1.2 Υποχρεωτικός Έλεγχος Πρόσβασης (MAC)

Σημαντικό μειονέκτημα των πολιτικών διακριτικού ελέγχου πρόσβασης αποτελεί το γεγονός ότι δεν είναι δυνατόν να προστατεύσουν τη ροή πληροφορίας σε ένα σύστημα,

καθώς δεν είναι σε θέση να ελέγξουν τη μετέπειτα χρήση της πληροφορίας από έναν χρήστη, από τη στιγμή που ο τελευταίος απέκτησε πρόσβαση σε αυτήν. Σε αυτό το πλαίσιο, ο *Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control — MAC)* [25] ελέγχει τη διάδοση της πληροφορίας εμποδίζοντας τη ροή από αντικείμενα υψηλής διαβάθμισης σε αντικείμενα χαμηλής διαβάθμισης, στη βάση μίας ταξινόμησης των υποκειμένων και αντικειμένων ενός συστήματος. Σημειώνεται ότι στις υποχρεωτικές πολιτικές η έννοια του υποκειμένου δεν αναφέρεται στους χρήστες αλλά σε διεργασίες που εκτελούνται για λογαριασμό των χρηστών.

Έτσι, κάθε υποκείμενο και κάθε αντικείμενο συσχετίζεται με ένα *βαθμό ασφάλειας* (*security level*), ο οποίος για τα αντικείμενα υποδηλώνει την ευαισθησία της πληροφορίας που περιέχεται στο αντικείμενο, ενώ στην περίπτωση των υποκειμένων αντανακλά την αξιοπιστία τους όσον αφορά τη μη αποκάλυψη ευαίσθητης πληροφορίας σε χρήστες οι οποίοι δεν είναι καταλλήλως εξουσιοδοτημένοι. Στην πιο απλή περίπτωση, ο βαθμός ασφάλειας αποτελεί στοιχείο ενός ιεραρχικά διατεταγμένου συνόλου και κάθε βαθμός επικρατεί σε όσους βρίσκονται πιο χαμηλά στην ιεραρχία από αυτόν, συμπεριλαμβανομένου και του ιδίου. Η πρόσβαση σε ένα αντικείμενο παρέχεται σε ένα υποκείμενο, εάν ικανοποιείται κάποια σχέση ανάμεσα στους αντίστοιχους βαθμούς ασφάλειας των δύο. Συγκεκριμένα, θα πρέπει να ικανοποιούνται οι εξής αρχές για την παρεμπόδιση ροής πληροφορίας που περιέχεται σε αντικείμενα υψηλής διαβάθμισης προς αντικείμενα χαμηλότερης διαβάθμισης:

- **Προς τα κάτω ανάγνωση (Read down):** Ο βαθμός ασφάλειας του υποκειμένου θα πρέπει να επικρατεί του αντίστοιχου βαθμού του αντικειμένου που πρόκειται να αναγνωστεί.
- **Προς τα πάνω εγγραφή (Write up):** Ένα υποκείμενο έχει δικαίωμα εγγραφής σε ένα αντικείμενο εάν ο βαθμός ασφάλειας του δεύτερου επικρατεί του αντίστοιχου βαθμού του πρώτου.

Σημειώνεται ότι για λόγους λεπτομερέστερης ταξινόμησης ασφάλειας, τα υποκείμενα και αντικείμενα είναι δυνατόν να συσχετίζονται επιπλέον με *κατηγορίες* (*categories*), που δηλώνουν τις συγκεκριμένες περιοχές στις οποίες ένα υποκείμενο είναι δυνατόν να δράσει και στις οποίες η πληροφορία ενός αντικειμένου αναφέρεται, αντίστοιχα, με αποτέλεσμα η διαβάθμισή τους τελικά να προσδιορίζεται ως ένα ζεύγος που περιλαμβάνει ένα βαθμό ασφάλειας και ένα σύνολο κατηγοριών.

Επιπλέον, ο υποχρεωτικός έλεγχος πρόσβασης μπορεί να εφαρμοστεί για την προστασία της ακεραιότητας της πληροφορίας. Για το σκοπό αυτό, ορίζονται *βαθμοί ακεραιότητας* (*integrity levels*), οι οποίοι υποδηλώνουν την εμπιστοσύνη προς την πληροφορία που είναι αποθηκευμένη σε κάποιο αντικείμενο και τις επιπτώσεις μη εξουσιοδοτημένης τροποποίησής της, και την αξιοπιστία του υποκειμένου σχετικά με την εισαγωγή, τροποποίηση ή διαγραφή δεδομένων, αντιστοίχως. Οι αρχές που πρέπει να ικανοποιούνται για τη

διαφύλαξη της ακεραιότητας είναι ανάλογες με εκείνες για τη διαφύλαξη της μυστικότητας, με αντιστροφή όμως της κατεύθυνσης της ροής πληροφορίας (read up, write down).

### 2.1.3 Έλεγχος Πρόσβασης Βάσει Ρόλων (RBAC)

Οι πολιτικές που βασίζονται σε ρόλους καθορίζουν την πρόσβαση που έχουν οι χρήστες σε ένα σύστημα βάσει των υποχρεώσεων και δραστηριοτήτων που τους έχουν ανατεθεί στα πλαίσια του συστήματος. Ένας ρόλος μπορεί να οριστεί ως ένα σύνολο ενεργειών και αρμοδιοτήτων που σχετίζονται με μία συγκεκριμένη εργασιακή δραστηριότητα και, κατόπιν, αντί να προσδιορίζεται κάθε πρόσβαση που ο κάθε χρήστης έχει τη δυνατότητα να πραγματοποιήσει, οι εξουσιοδοτήσεις πρόσβασης σε αντικείμενα προσδιορίζονται για ρόλους, οι οποίοι ανατίθενται σε χρήστες. Συνεπώς, ο *Έλεγχος Πρόσβασης Βάσει Ρόλων* (*Role-based Access Control — RBAC*) [27] απλοποιεί σημαντικά τη διαχείριση εξουσιοδοτήσεων. Ένα άλλο πλεονέκτημα των μοντέλων RBAC είναι ότι υποστηρίζουν την αρχή της απόδοσης των *ελάχιστων προνομίων* (*least privilege*) για την εκτέλεση κάποιας συγκεκριμένης εργασίας, δηλαδή οι χρήστες με ισχυρούς ρόλους δεν χρειάζεται να τους ασκήσουν μέχρι τα προνόμια αυτά να κριθούν πράγματι αναγκαία. Σημειώνεται ότι ένας χρήστης είναι δυνατόν να κατέχει διαφορετικούς ρόλους σε διαφορετικές περιστάσεις, ενώ επίσης, ο ίδιος ρόλος είναι δυνατόν να χρησιμοποιείται ταυτόχρονα από διαφορετικούς χρήστες, με κάποιες προσεγγίσεις να επιτρέπουν στο χρήστη να ασκήσει πολλαπλούς ρόλους ταυτόχρονα και κάποιες άλλες να επιτρέπουν τη χρήση ενός μοναδικού ρόλου κάθε φορά ή να αναγνωρίζουν ότι ορισμένοι ρόλοι μπορούν να ασκηθούν από κοινού ή ότι είναι αμοιβαίως αποκλειόμενοι.

Το NIST[4] πρότυπο RBAC [28] είναι ένα γενικό μοντέλο που μπορεί να καλύψει τα κενά των μοντέλων τύπου MAC και DAC και αποτέλεσε τη βάση για πληθώρα άλλων μοντέλων ελέγχου πρόσβασης. Υπάρχουν τέσσερις διαφορετικές εκδοχές του RBAC: το $RBAC_0$, γνωστό και ως *Βασικό RBAC* (*Core RBAC*), είναι η απλούστερη εκδοχή και αποτελεί τον πυρήνα για τις επόμενες μορφές του μοντέλου, το $RBAC_1$ αποτελεί το ιεραρχικό RBAC, που υποστηρίζει την κληρονομικότητα εξουσιοδοτήσεων, το $RBAC_2$ κάνει χρήση περιορισμών, ενώ το $RBAC_3$ είναι γνωστό και ως συμμετρικό RBAC και επεκτείνει τις δυνατότητες των προηγούμενων υποστηρίζοντας κληρονομικότητα και ιεραρχίες.

Οι βασικές έννοιες του $RBAC_0$ είναι οι *χρήστες*, οι *ρόλοι*, τα *αντικείμενα*, οι *λειτουργίες*, οι *άδειες* και οι *συνεδρίες* (*sessions*). Οι ρόλοι ανατίθενται σε χρήστες και οι άδειες, δηλαδή οι συσχετίσεις μεταξύ αντικειμένων και λειτουργιών που εκτελούνται στα εν λόγω αντικείμενα, αντιστοιχίζονται σε ρόλους, με τη σχέση μεταξύ ρόλων-χρηστών όπως και αυτή μεταξύ δικαιωμάτων-ρόλων να είναι πολλά-προς-πολλά. Η έννοια των συνεδριών εισάγεται προκειμένου να υποστηριχτεί η αρχή της απόδοσης των ελάχιστων προνομίων και αφορά την ενεργοποίηση ενός ρόλου για όσο διάστημα είναι αναγκαίο για την ολοκλή-

[4]National Institute of Standards and Technology (NIST), homepage: http://www.nist.gov/.

ρωση των λειτουργιών που έχουν ανατεθεί στο χρήστη στα πλαίσια του συστήματος. Ένας χρήστης στα πλαίσια μίας συνεδρίας μπορεί να ενεργοποιήσει διαφορετικούς ρόλους˙ μετά τον τερματισμό μίας συνεδρίας, όλοι οι ρόλοι που ενεργοποιήθηκαν στη διάρκειά της ανακαλούνται.

Στο $RBAC_1$ εισάγεται η έννοια της ιεραρχίας ρόλων, η οποία βασίζεται στις αρχές της γενίκευσης και της ειδίκευσης, και της κληρονομικότητας των εξουσιοδοτήσεων. Έτσι, ένας πιο εξειδικευμένος ρόλος κληρονομεί τις εξουσιοδοτήσεις πιο γενικών ρόλων. Ωστόσο, αυτό δημιουργεί επιπλοκές σε ό,τι αφορά την ενεργοποίηση ρόλων και τα σχετικά δικαιώματα πρόσβασης.

Το $RBAC_2$ εισάγει την έννοια των περιορισμών, όπως είναι οι περιορισμοί που αφορούν στις συνθήκες που πρέπει να πληροί ένας ρόλος προκειμένου να επιτραπεί η ενεργοποίησή του. Ένας άλλος τύπος περιορισμών είναι ο *Διαχωρισμός Καθηκόντων* (*Separation of Duty — SoD*). Οι περιορισμοί αυτοί συνιστούν ένα σημαντικό μηχανισμό για την πρόληψη απάτης, μέσω του διαμοιρασμού των καθηκόντων για την ολοκλήρωση ενός στόχου σε διαφορετικά μέρη. Υπάρχουν δύο τύποι περιορισμών διαχωρισμού καθηκόντων:

- Ο *Στατικός Διαχωρισμός Καθηκόντων* (*Static Separation of Duty — SSoD*) αφορά στις περιπτώσεις που δύο ή περισσότεροι ρόλοι δεν μπορούν να ενεργοποιηθούν ταυτόχρονα.
- Ο *Δυναμικός Διαχωρισμός Καθηκόντων* (*Dynamic Separation of Duty – DSoD*) αναφέρεται σε περιορισμούς που ελέγχονται και επιβάλλονται σε πραγματικό χρόνο και συνδέονται με την έννοια της συνεδρίας και της ενεργοποίησης των ρόλων. Έτσι, η ενεργοποίηση κάποιων ρόλων κατά τη διάρκεια μίας συνεδρίας είναι δυνατόν να οδηγεί σε απαγόρευση της ενεργοποίησης κάποιου τρίτου ρόλου στο πλαίσιο της ίδιας συνεδρίας.

### 2.1.4 Έλεγχος Πρόσβασης Βάσει Ιδιοτήτων (ABAC)

Στα ανακύπτοντα κατανεμημένα σενάρια (όπως η υπολογιστική νέφους) οι "κλασικές" παραδοχές για την επιβολή ελέγχου πρόσβασης δεν επαρκούν. Συνήθως, ένα αίτημα πρόσβασης είναι δυνατόν να προέρχεται από άγνωστους χρήστες και, συνεπώς, δεν είναι δυνατόν να εφαρμοστούν πολιτικές πρόσβασης βασισμένες στην ταυτότητα του αιτούντος. Εναλλακτικές λύσεις που έχουν διερευνηθεί σε μεγάλο βαθμό τα τελευταία χρόνια συνίστανται στην υιοθέτηση *Ελέγχου Πρόσβασης Βάσει Ιδιοτήτων* (*Attribute-Based Access Control — ABAC*), ο οποίος χρησιμοποιεί τα χαρακτηριστικά που σχετίζονται με τους πόρους/υπηρεσίες και τους αιτούντες για την αποτίμηση των αιτημάτων πρόσβασης (π.χ., [29][30][31]). Σε αυτό το πλαίσιο, στον έλεγχο πρόσβασης αυτού του τύπου τόσο το υποκείμενο όσο και το αντικείμενο στα οποία αναφέρεται μία εξουσιοδότηση αντικαθίστανται από ένα σύνολο ιδιοτήτων που σχετίζονται με αυτά. Τέτοιες ιδιότητες είναι δυνατόν να

αντιστοιχούν σε κάποιου είδους ταυτότητα ή σε μη ταυτοποιητικά χαρακτηριστικά ενός χρήστη (π.χ., ημερομηνία γέννησης, εθνικότητα), καθώς και σε μεταδεδομένα που συσχετίζονται με κάποιο αντικείμενο και παρέχουν επιπλέον πληροφορία πλαισίου (π.χ., ημερομηνία δημιουργίας).

Έτσι, οι εξουσιοδοτήσεις τύπου ABAC μοντελοποιούν περιορισμούς πρόσβασης στη βάση ιδιοτήτων των υποκειμένων και των αντικειμένων. Στη γενική περίπτωση, αυτού του είδους οι περιορισμοί αναφέρονται σε ιδιότητες συγκεκριμένων διαπιστευτηρίων ή σε αφαιρετικές δομές πιστοποιητικών. Τα βασικά στοιχεία μίας εξουσιοδότησης είναι τα ακόλουθα:

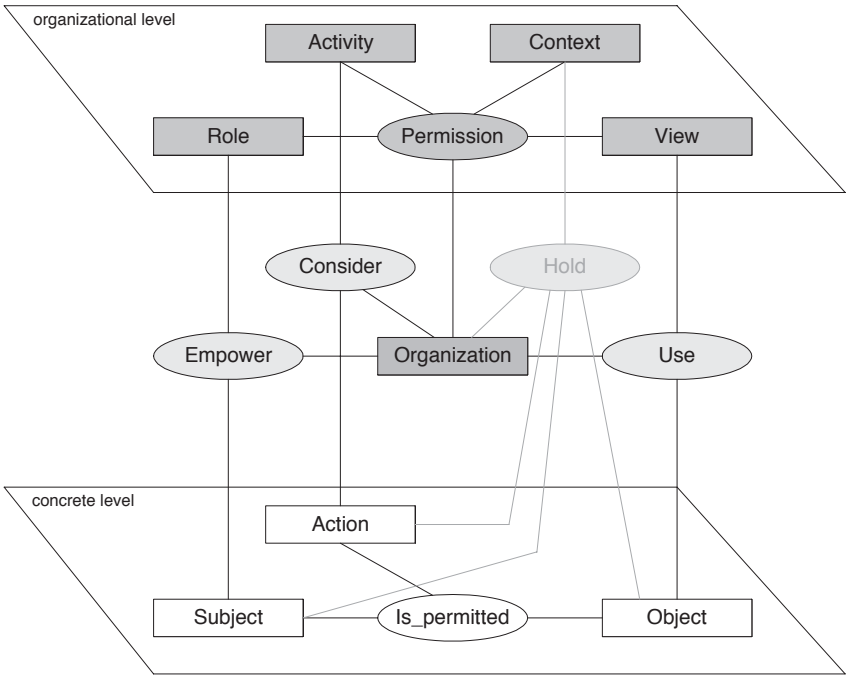
- *Έκφραση Υποκειμένου (Subject Expression):* Η έκφραση υποκειμένου προσδιορίζει ένα σύνολο υποκειμένων που εμφανίζουν συγκεκριμένες ιδιότητες.
- *Έκφραση Αντικειμένου (Object Expression):* Η έκφραση αντικειμένου προσδιορίζει τους πόρους/υπηρεσίες που θα πρέπει να προστατεύονται, στη βάση των ιδιοτήτων τους.
- *Ενέργεια (Action):* Η ενέργεια υποδηλώνει τη λειτουργία στην οποία αναφέρεται η εξουσιοδότηση.

### 2.1.5 Έλεγχος Πρόσβασης Βάσει Οργανισμού (OrBAC)

Το μοντέλο *Ελέγχου Πρόσβασης Βάσει Οργανισμού* (*Organization-based Access Control — OrBAC*) [32][33][34] αποτελεί μία ολοκληρωμένη λύση για τη μοντελοποίηση πολιτικών ελέγχου πρόσβασης και χρήσης σε πληροφοριακά συστήματα. Εισάγει ιδιαίτερα εκφραστικούς φορμαλισμούς, οι οποίοι επιτρέπουν τον πλήρη διαχωρισμό των πολιτικών από τη συγκεκριμένη υλοποίηση τους [35]. Αυτό επιτυγχάνεται μέσω της εισαγωγής ενός επιπέδου αφαίρεσης αναφορικά με τις τυπικές οντότητες ελέγχου πρόσβασης, δηλαδή το υποκείμενο, την ενέργεια και το αντικείμενο. Έτσι, εκτός από την ομαδοποίηση των χρηστών σε *ρόλους*, το μοντέλο αυτό επιπλέον κατατάσσει τις ενέργειες σε *δραστηριότητες* (*activities*) τις οποίες υλοποιούν, και τα αντικείμενα σε *όψεις* (*views*) στις οποίες αυτά χρησιμοποιούνται. Η έννοια του *οργανισμού* (*organization*) κατέχει κεντρική θέση στο OrBAC και επιτρέπει την καλύτερη ανάλυση της διαλειτουργικότητας και της προδιαγραφής ιεραρχιών, η οποία με τη σειρά της έχει σαν αποτέλεσμα την ευέλικτη προδιαγραφή του πλαισίου συνεργασίας και της ροής πληροφορίας μεταξύ διαφορετικών οργανισμών. Για παράδειγμα, στο [36] επιστρατεύονται οι OrBAC φορμαλισμοί και η εκφραστικότητα οντολογιών γενικού σκοπού για την επίτευξη ομαλής διαλειτουργικότητας μεταξύ οργανισμών. Επιπλέον, το μοντέλο OrBAC περιλαμβάνει αρνητικές εξουσιοδοτήσεις για την προδιαγραφή σύνθετων πολιτικών. Λόγω της ενδεχόμενης σύγκρουσης μεταξύ θετικών και αρνητικών εξουσιοδοτήσεων, παρέχονται επίσης μηχανισμοί ανίχνευσης και επίλυσης των πιθανών συγκρούσεων [37]. Σημαντική συνεισφορά της προσέγγισης αυτής αποτελεί η δυνατότητα

προσδιορισμού ιδιαίτερα δυναμικών κανόνων οι οποίοι βασίζονται σε ποικίλες πληροφορίες πλαισίου, π.χ., χρονικούς περιορισμούς και προτιμήσεις χρήστη˙ οι πληροφορίες πλαισίου μπορούν επομένως να χρησιμοποιηθούν για να οριστούν οι συνθήκες κάτω από τις οποίες οι εξουσιοδοτήσεις ενεργοποιούνται και απενεργοποιούνται.

Έτσι, όπως φαίνεται στο Σχήμα 1, το OrBAC θεωρεί δύο επίπεδα αφαίρεσης: το *επίπεδο οργανισμού* (*organizational level*), το οποίο περιλαμβάνει τις έννοιες *role*, *activity*, *view* και *context*, και το *επίπεδο προσδιορισμού* (*concrete level*) που περιλαμβάνει τις συγκεκριμένες έννοιες *subject*, *action* και *object*.




Σχήμα 1: Οντότητες και έννοιες του μοντέλου OrBAC.

Οι κανόνες διακρίνονται σε *άδειες* (*permissions*), *απαγορεύσεις* (*prohibitions*), *υποχρεώσεις* (*obligations*) και *απαλλαγές* (*dispensations*) και ορίζονται με χρήση λογικής πρώτου βαθμού (first order logic). Για τους διαφορετικούς τύπους κανόνων ορίζονται τα αντίστοιχα κατηγορήματα: *Is_permitted*, *Is_prohibited*, *Is_obliged* και *Is_dispensed*. Έτσι, με βάση τα παραπάνω, μία συγκεκριμένη άδεια ορίζεται ως εξής:

- $\forall$ *org*, $\forall$*s*, $\forall$*o*, $\forall\alpha$, $\forall$*r*, $\forall\nu$, $\forall$*a* , $\forall$*C*,
  *Permission*(*org*, *r*, *a*, $\nu$, *C* ) $\wedge$ *empower*(*org*, *s*, *r*)
  $\wedge$ *use*(*org*, *o*, $\nu$) $\wedge$ *consider*(*org*, $\alpha$, *a*) $\wedge$
  *hold*(*org*, *s*, *a*, *o*, *C* ) $\rightarrow$ *Is_permitted*(*s*, $\alpha$, *o*)

Το νόημα της έκφρασης αυτής είναι ότι εάν ένας οργανισμός *org* παραχωρήσει σε κάποιο ρόλο *r* την άδεια να πραγματοποιήσει κάποια δραστηριότητα *a* στην όψη $\nu$ όταν ισχύει κάποιο πλαίσιο *C* (*hold*), και εάν ο ρόλος *r* έχει ανατεθεί στο υποκείμενο *s* (*empower*),

το αντικείμενο *o* χρησιμοποιείται στην όψη $\nu$ (*use*) και η ενέργεια $\alpha$ υλοποιεί τη δραστηριότητα *a* (*consider*), τότε παρέχεται στο *s* η άδεια να πραγματοποιήσει την $\alpha$ στο *o*.

Ένα επιπρόσθετο σημαντικό χαρακτηριστικό του OrBAC αποτελεί η δυνατότητα ορισμού ιεραρχιών σε όλες τις αφηρημένες έννοιές του, δηλαδή ιεραρχιών οργανισμών, ρόλων, δραστηριοτήτων και όψεων. Ένα από τα πλεονεκτήματα της χρήσης ιεραρχιών έγκειται στο μηχανισμό κληρονομικότητας των εξουσιοδοτήσεων με βάση τις ιεραρχίες αυτές. Έτσι, η δομή ενός οργανισμού μπορεί να μοντελοποιηθεί ως μία ιεραρχία οργανισμού, με τα τμήματα, υπηρεσίες κλπ. που την απαρτίζουν να αποτελούν υπο-οργανισμούς, και στη συνέχεια μπορεί να οριστεί μία γενική πολιτική για τον οργανισμό, την οποία θα λάβουν και θα προσαρμόσουν οι υπο-οργανισμοί, μέσω του μηχανισμού κληρονομικότητας. Ο τρόπος διαχείρισης της κληρονομικότητας εξουσιοδοτήσεων παρουσιάζεται στο [38]. Ένα δεύτερο πλεονέκτημα αποτελεί η διαχείριση της συνεργασίας μεταξύ οργανισμών· ένα σύνολο οργανισμών μπορεί να θεωρηθεί ως ένας *μετα-οργανισμός*, οπότε τελικά η μοντελοποίηση του συνόλου ανάγεται στο πρόβλημα μοντελοποίησης ενός μεμονωμένου οργανισμού.

Το OrBAC επιτρέπει την τεχνική βελτίωση (refinement) των πολιτικών μέσω μίας διαδικασίας μετάφρασης του συνόλου των αφηρημένων κανόνων μίας πολιτικής σε μία σειρά συγκεκριμένων κανόνων, οι οποίοι στη συνέχεια επικοινωνούνται στα αρμόδια στοιχεία του συστήματος. Η διαδικασία μπορεί να θεωρηθεί ως μία επαναληπτική σειρά μετασχηματισμών, καθένας από τους οποίους εξαρτάται από το εκάστοτε σημείο εφαρμογής των κανόνων (π.χ. firewalls, IDSs και δρομολογητές VPN). Ουσιαστικά, λοιπόν, η καθολική πολιτική του συστήματος αναλύεται σε μία σειρά εντολών εκφρασμένων στη "γλώσσα" του κάθε στοιχείου.

Τέλος, θα πρέπει να σημειωθεί ότι, αν και το OrBAC δεν έχει σχεδιασθεί με πρωταρχικό στόχο την προστασία της ιδιωτικότητας, ωστόσο οι φορμαλισμοί που εισάγει του επιτρέπουν να χρησιμοποιηθεί για την αυτοματοποίηση της εφαρμογής πολιτικών ιδιωτικότητας. Ενδεικτικά, οι συμπληρωματικές ενέργειες που θα πρέπει να ακολουθούν την πρόσβαση μπορούν να μοντελοποιηθούν μέσω των υποχρεώσεων, με την ενέργεια πρόσβασης να ενεργοποιεί κάποιο πλαίσιο συσχετισμένο με την εκάστοτε υποχρέωση, ενώ εκείνες που πρέπει να προηγούνται είναι δυνατόν να συσχετίζονται με κάποιο πλαίσιο ούτως ώστε η εκτέλεσή τους να το ενεργοποιεί και αυτό με τη σειρά του να θέτει σε εφαρμογή την άδεια που αφορά το αίτημα πρόσβασης. Επίσης και ο σκοπός πρόσβασης μπορεί να μοντελοποιηθεί ως πληροφορία πλαισίου, όπως προτείνεται και στο [39], στο οποίο παρουσιάζεται μία επέκταση του OrBAC για προστασία της ιδιωτικότητας.

### 2.1.6 Η Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης (XACML)

Μία πολύ αξιόλογη προσπάθεια προδιαγραφής μίας δομημένης γλώσσας για την προδιαγραφή πολιτικών ιδιωτικότητας και κανόνων που θα μπορούν να είναι ευθέως εφαρ-

μόσιμοι από τα αντίστοιχα συστήματα έχει πραγματοποιηθεί από τον οργανισμό Organization for the Advancement of Structured Information Standards (OASIS)[5], με την προδιαγραφή της *Επεκτάσιμης Γλώσσας Σήμανσης Ελέγχου Πρόσβασης* (*eXtensible Access Control Markup Language — XACML*) καθώς και της αρχιτεκτονικής για την εφαρμογή της [40]. Η XACML συνιστά έτσι μία γλώσσα γενικού σκοπού για την άσκηση ελέγχου πρόσβασης, η οποία, αν και δεν προβλέπει η ίδια προστασία της ιδιωτικότητας, έχει ιδιαίτερη σημασία γιατί, εκτός από το να είναι ένα καλά εδραιωμένο πρότυπο OASIS, έχει αποτελέσει τη βάση για πολλά μοντέλα με στόχο την προστασία της ιδιωτικότητας.

Η γλώσσα XACML έχει δομηθεί γύρω από τις ακόλουθες βασικές έννοιες:

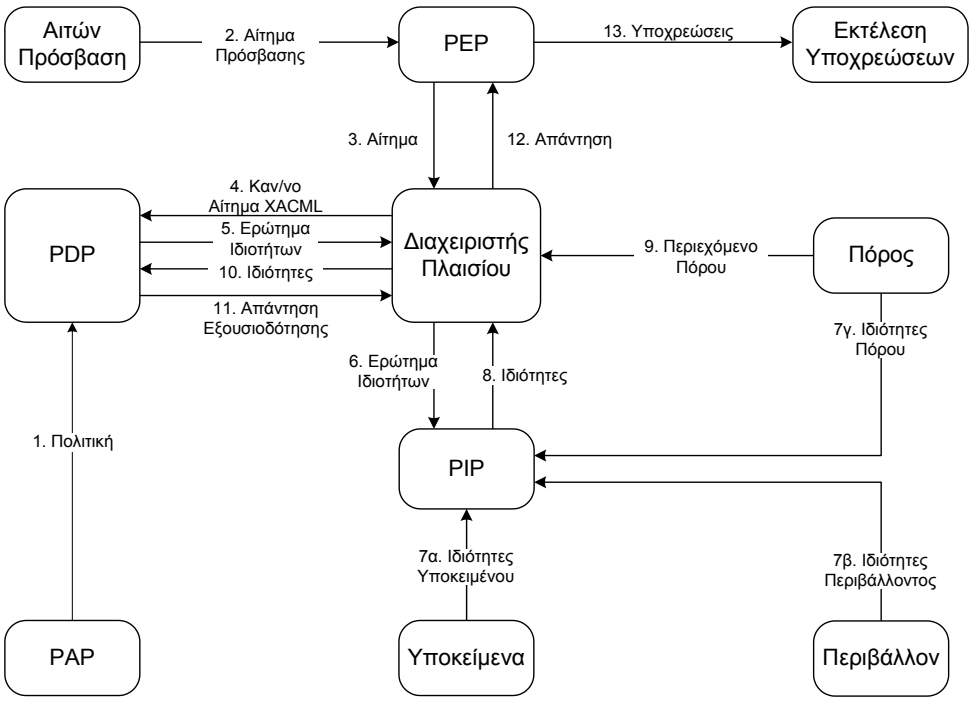
- **Πόρος (Resource)**: Προσωπικά δεδομένα, υπηρεσίες, συστήματα ή οτιδήποτε άλλο μπορεί να αποτελέσει αντικείμενο κάποιου αιτήματος για πρόσβαση.
- **Ενέργεια (Action)**: Οποιαδήποτε λειτουργία πάνω σε έναν πόρο που καλύπτεται από την πολιτική.
- **Υποκείμενο (Subject)**: Εκείνη η οντότητα που αιτείται να πραγματοποιήσει κάποια ενέργεια σε κάποιον πόρο.
- **Απόφαση Εξουσιοδότησης (Authorization Decision)**: Το αποτέλεσμα της αποτίμησης κάποιας πολιτικής. Το αποτέλεσμα μπορεί να λάβει τις τιμές: Έγκριση (permit), Απαγόρευση (deny) Απροσδιοριστία (indeterminate) και Ανεφάρμοστο (not applicable). Προαιρετικά, η απόφαση εξουσιοδότησης μπορεί να προσδιορίζει και ένα σύνολο από υποχρεώσεις.
- **Ιδιότητα (Attribute)**: Τα διάφορα χαρακτηριστικά που αφορούν σε υποκείμενα, πόρους, ενέργειες, περιβάλλοντα. Για παράδειγμα, το όνομα ενός χρήστη, το αρχείο που θέλει να προσπελάσει, κλπ. αποτελούν τιμές ιδιοτήτων.
- **Περιβάλλον (Environment)**: Το σύνολο των πιθανών ιδιοτήτων που σχετίζονται με μία απόφαση εξουσιοδότησης αλλά είναι ανεξάρτητες του υποκειμένου, του πόρου ή της ενέργειας.
- **Υποχρέωση (Obligation)**: Κάποια λειτουργία η οποία πρέπει να πραγματοποιηθεί κατά την εφαρμογή της απόφασης εξουσιοδότησης.
- **Σημείο Απόφασης Πολιτικής (Policy Decision Point — PDP)**: Η οντότητα του συστήματος που πραγματοποιεί την αποτίμηση της πολιτικής και καταλήγει σε μία απόφαση εξουσιοδότησης.
- **Σημείο Εφαρμογής Πολιτικής (Policy Enforcement Point — PEP)**: Η οντότητα του συστήματος που πραγματοποιεί τον έλεγχο της πρόσβασης, εφαρμόζοντας τις απο-

[5]Organization for the Advancement of Structured Information Standards (OASIS), homepage: http://www.oasis-open.org/.

φάσεις του σημείου PDP, στο οποίο απευθύνεται με τα αντίστοιχα αιτήματα αποτίμησης.

- **Σημείο Διαχείρισης Πολιτικής (Policy Administration Point — PAP)**: Η οντότητα του συστήματος στην οποία συγγράφονται οι πολιτικές.
- **Σημείο Πληροφόρησης Πολιτικής (Policy Information Point — PIP)**: Η οντότητα του συστήματος που λειτουργεί ως πηγή των τιμών των ιδιοτήτων.
- **Διαχειριστής Πλαισίου (Context Handler)**: Η οντότητα του συστήματος που πραγματοποιεί τη μετατροπή των αιτήσεων εξουσιοδότησης από την εγγενή τους μορφή σε κανονική XACML μορφή (canonical XACML form), καθώς και τη μετατροπή των αποφάσεων εξουσιοδότησης από την κανονική XACML μορφή στη μορφή εκείνη που αντιλαμβάνεται το σχετικό σύστημα.

Ο τρόπος λειτουργίας της γλώσσας και του γενικότερου πλαισίου της XACML συνοψίζεται στο διάγραμμα ροής πληροφορίας που παρουσιάζεται στο Σχήμα 2, όπου γίνεται σαφής ο λογικός διαχωρισμός των οντοτήτων ελέγχου πρόσβασης που συντελούν στην προδιαγραφή, εφαρμογή και αποτίμηση των πολιτικών, ικανοποιώντας έτσι τις ειδικές ανάγκες και απαιτήσεις που προκύπτουν από τη φύση των κατανεμημένων αρχιτεκτονικών. Συνοπτικά, η λειτουργία του μοντέλου XACML αποτελείται από τα παρακάτω βήματα:




Σχήμα 2: Διάγραμμα ροής πληροφορίας XACML

1. Οι πολιτικές ιδιωτικότητας συγγράφονται στο σημείο PAP και καθίστανται διαθέσιμες στο σημείο PDP.

2. Ο αιτών πρόσβαση σε κάποιον πόρο αποστέλλει το σχετικό αίτημα στο σημείο PEP.

3. Το σημείο PEP αποστέλλει το αίτημα για πρόσβαση στο διαχειριστή πλαισίου, στην πρωταρχική του μορφή.

4. Ο διαχειριστής πλαισίου δημιουργεί ένα κανονικοποιημένο αίτημα XACML και το αποστέλλει στο σημείο PDP.

5. Το σημείο PDP αιτείται από το διαχειριστή πλαισίου οποιαδήποτε επιπλέον ιδιότητα του υποκειμένου, του πόρου ή του περιβάλλοντος.

6. Ο διαχειριστής πλαισίου αιτείται τις ιδιότητες από το σημείο PIP.

7. Το σημείο PIP αποκτά τις ιδιότητες που αφορούν το σχετικό αίτημα.

8. Το σημείο PIP αποστέλλει στο διαχειριστή τις ιδιότητες που αφορούν το σχετικό αίτημα.

9. Προαιρετικά, ο διαχειριστής πλαισίου ενσωματώνει τον πόρο στο σχετικό αίτημα.

10. Ο διαχειριστής πλαισίου αποστέλλει τις ιδιότητες που ζητήθηκαν και (προαιρετικά) τον πόρο στο σημείο PDP.

    Το σημείο PDP πραγματοποιεί την αποτίμηση του αιτήματος.

11. Το σημείο PDP τροφοδοτεί το διαχειριστή πλαισίου με την απάντηση — αποτέλεσμα της αποτίμησης για την απόφαση εξουσιοδότησης.

12. Ο διαχειριστής πλαισίου μεταφράζει την απάντηση στην εγγενή μορφή που αντιλαμβάνεται το σημείο PEP.

    Ο διαχειριστής πλαισίου προωθεί την απάντηση στο σημείο PEP.

13. Το σημείο PEP εκτελεί τις υποχρεώσεις που προκύπτουν. Εφόσον σύμφωνα με την απόφαση εξουσιοδότησης η πρόσβαση επιτρέπεται, το σημείο PEP επιτρέπει την πρόσβαση στον αιτηθέντα προστατευμένο πόρο. Σε διαφορετική περίπτωση, το σημείο PEP προβαίνει σε άρνηση της πρόσβασης.

Όσον αφορά την XACML γλώσσα, είναι μία γλώσσα XML ικανή να εκφράσει πληθώρα πολιτικών, λαμβάνοντας υπόψη τις ιδιότητες των υποκειμένων και των προστατευόμενων αντικειμένων, καθώς επίσης και πληροφορίες πλαισίου. Οι XACML πολιτικές περιλαμβάνουν έναν *Στόχο* (*Target*), ένα σύνολο *Κανόνων* (*Rules*) και έναν *Αλγόριθμο Συνδυασμού Κανόνων* (*Rule-Combining Algorithm*). Ο Στόχος αποτελεί το πεδίο ορισμού του Κανόνα, Πολιτικής ή Συνόλου Πολιτικών, δηλαδή το σύνολο από υποκείμενα, πόρους, ενέργειες

και περιβάλλοντα στα οποία εφαρμόζεται ο εν λόγω Κανόνας, Πολιτική ή Σύνολο Πολιτικών. Κάθε Κανόνας με τη σειρά του περιλαμβάνει, εκτός από κάποιο Στόχο, μία *Συνθήκη* (*Condition*) και μία *Επίδραση* (*Effect*). Η Συνθήκη καθορίζει τους περιορισμούς σχετικά με τις τιμές των ιδιοτήτων που πρέπει να ισχύουν σε κάποιο αίτημα, προκειμένου το τελευταίο να επιτραπεί ή να απορριφθεί, απόφαση η οποία προσδιορίζεται από την Επίδραση. Ο Αλγόριθμος Συνδυασμού Κανόνων ορίζει τη διαδικασία βάσει της οποίας πολλαπλοί κανόνες καταλήγουν σε ένα συνδυαστικό αποτέλεσμα, περιλαμβάνοντας επίλυση των πιθανών συγκρούσεων μεταξύ των ισχυόντων κανόνων. Μία XACML πολιτική μπορεί επίσης να περιέχει μία ή περισσότερες *Υποχρεώσεις* (*Obligations*), οι οποίες αντιπροσωπεύουν λειτουργίες που θα πρέπει εκτελούνται σε συνδυασμό με την εκτέλεση μίας απόφασης εξουσιοδότησης.

Τέλος, αξίζει να αναφερθεί ότι η βασική προδιαγραφή της XACML επεκτείνεται μέσω των λεγόμενων προφίλ (profiles), τα οποία την καθιστούν ένα πολύ ισχυρό εργαλείο περιγραφής πολιτικών. Στο πλαίσιο αυτό, ιδιαίτερο ενδιαφέρον σε ό,τι αφορά την προστασία της ιδιωτικότητας παρουσιάζουν δύο προφίλ: το *Προφίλ Πολιτικής Ιδιωτικότητας* (*Privacy Policy Profile*) [41], το οποίο δίνει τη δυνατότητα διαχείρισης της έννοιας του σκοπού στο πλαίσιο μίας πολιτικής, και το *Προφίλ Διεπιχειρησιακής Ασφάλειας και Ιδιωτικότητας* (*Cross-Enterprise Security and Privacy profile*) [42] για την αντιμετώπιση των αναγκών ασφάλειας σε υπολογιστικά περιβάλλοντα που εδράζουν σε διαφορετικούς διαχειριστικούς τομείς.

## 2.2 Έλεγχος Πρόσβασης για Προστασία της Ιδιωτικότητας

Κάθε παραβίαση της ιδιωτικότητας αφορά και περιλαμβάνει αθέμιτη πρόσβαση στα αντίστοιχα δεδομένα· για το λόγο αυτό, οι τεχνολογίες ελέγχου πρόσβασης αποτελούν μηχανισμούς ιδιαίτερης σημασίας για την προστασία των προσωπικών δεδομένων. Ωστόσο, οι καθιερωμένοι μηχανισμοί ελέγχου πρόσβασης, όπως ο Διακριτικός Έλεγχος Πρόσβασης και ο Υποχρεωτικός Έλεγχος Πρόσβασης, καθώς και η οικογένεια των μοντέλων Ελέγχου Πρόσβασης Βάσει Ρόλων, αδυνατούν να ανταποκριθούν στο σύνολο των ειδικών απαιτήσεων που απορρέουν από τις θεμελιώδεις αρχές προστασίας της ιδιωτικότητας, όπως προβλέπεται από πρωτοβουλίες ορόσημο όπως οι Κατευθυντήριες Οδηγίες του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (Organisation for Economic Co-operation and Development — OECD) [11] ή την Ευρωπαϊκή Νομοθεσία [12], καλύπτοντας ένα μόνο μέρος τους. Για παράδειγμα, δε λαμβάνουν υπόψη τη θεμελιώδη παράμετρο του σκοπού για τον οποίο πραγματοποιείται η συλλογή και επεξεργασία των δεδομένων και δεν προδιαγράφουν την εκτέλεση συμπληρωματικών ενεργειών, αυτών που στη διεθνή βιβλιογραφία αναφέρονται συχνά ως *υποχρεώσεις* (*obligations*) [43], όπως είναι η ενημέρωση του υποκειμένου των δεδομένων αναφορικά με τη συλλογή ή επεξεργασία των δεδομένων του. Έτσι, τα τελευταία χρόνια έχει προκύψει μία νέα οικογένεια μηχανισμών, κυρίως

σε ερευνητικό επίπεδο, οι οποίοι κάνουν πράξη το λεγόμενο *Έλεγχο Πρόσβασης για Προστασία της Ιδιωτικότητας* (*Privacy-aware Access Control*) [44][45]. Οι μηχανισμοί αυτοί επεκτείνουν συνήθως τα μοντέλα RBAC, ενσωματώνοντάς τους επιπλέον κριτήρια για την παροχή πρόσβασης, τα οποία ξεπερνούν το *ποιος χρήστης*, κατέχοντας *ποιον ρόλο*, εκτελεί *ποια ενέργεια πάνω σε σε ποια δεδομένα*. Κοινό και θεμελιώδες χαρακτηριστικό όλων των μοντέλων που εμπίπτουν σε αυτήν την κατηγορία συνιστά η κεντρική θέση που κατέχει η έννοια του σκοπού για τον οποίο προσωπικά δεδομένα συλλέγονται ή/και υπόκεινται σε επεξεργασία.

Μία από τις πρώτες και πλέον επιδραστικές προσεγγίσεις για την ενσωμάτωση των βασικών αρχών περί προστασίας της ιδιωτικότητας στις διαδικασίες ελέγχου πρόσβασης σε δεδομένα αποτελούν οι *Ιπποκρατικές Βάσεις Δεδομένων* (*Hippocratic Databases*) [46]. Η ιδέα των Ιπποκρατικών Βάσεων Δεδομένων παρουσιάστηκε το 2002 από ομάδα ερευνητών της εταιρείας IBM, η οποία θέλησε να καταστήσει τα Σχεσιακά Συστήματα Βάσεων Δεδομένων (Relational Database Systems) συμβατά με τις βασικές αρχές προστασίας της ιδιωτικότητας. Η βασικότερη συνεισφορά της προσέγγισης αυτής ήταν ότι εισήγαγε την έννοια του σκοπού της συλλογής και επεξεργασίας, ενώ αποτέλεσε το αντικείμενο διαφόρων επεκτάσεων (π.χ., [47][48]). Αντικείμενο εκτενούς ακαδημαϊκής αλλά και βιομηχανικής έρευνας έχει αποτελέσει επίσης η αυτοματοποίηση της εφαρμογής πολιτικών ιδιωτικότητας μέσω ελέγχου πρόσβασης, με ολοκλήρωσή τους, ενώ κάποιες προσεγγίσεις προχωρούν περισσότερο και θεμελιώνονται αποκλειστικά στη βάση των κανονιστικών διατάξεων. Παράλληλα, τα μοντέλα Ελέγχου Πρόσβασης για Προστασία της Ιδιωτικότητας έχουν υιοθετήσει ένα μεγάλο σύνολο σύγχρονων εννοιών και τεχνολογιών, όπως επίγνωση πλαισίου, τυπική σημασιολογία (formal semantics) και οντολογική θεμελίωση, τεχνολογίες κρυπτογράφησης και συστήματα ανώνυμων διαπιστευτηρίων, καθώς και κατανεμημένη ευφυΐα.

### 2.2.1 Έλεγχος Πρόσβασης Βάσει Σκοπού (PBAC)

Οι Ιπποκρατικές Βάσεις Δεδομένων αποτέλεσαν το πρώτο βήμα για την προδιαγραφή συστημάτων βάσεων δεδομένων τα οποία λαμβάνουν υπόψη την προστασία της ιδιωτικότητας και ενέπνευσαν αρκετές αντίστοιχες ερευνητικές προσπάθειες. Μία από τις πιο σημαντικές και αντιπροσωπευτικές προσεγγίσεις αποτελεί το μοντέλο *Ελέγχου Πρόσβασης Βάσει Σκοπού* (*Purpose Based Access Control — PBAC*) [49][50][51]. Η βασική συνεισφορά του μοντέλου αυτού είναι ο αναλυτικός ορισμός της έννοιας του σκοπού, από τον οποίο παίρνει τελικά και το όνομά του. Αναφορικά με το *χαρακτηρισμό των δεδομένων* (*data labeling*), δηλαδή τον τρόπο με τον οποίο τα δεδομένα συσχετίζονται με τους σκοπούς, το μοντέλο PBAC ορίζει ένα ευέλικτο σχήμα που πραγματοποιεί τις συσχετίσεις σε διαφορετικά επίπεδα, από μεμονωμένα κελιά ενός πίνακα μέχρι ολόκληρο πίνακα της βάσης δεδομένων. Για τη διαχείριση των ρόλων, το μοντέλο PBAC υιοθετεί μία προσέγγιση που βασίζεται στο μοντέλο RBAC [28], ενώ, όπως και στις Ιπποκρατικές Βάσεις Δεδομένων, τα ερωτήματα υφίστανται μετασχηματισμό μετά την υποβολή τους.

Το μοντέλο PBAC διαχωρίζει τους *Προτιθέμενους Σκοπούς* (*Intended Purposes*) από τους *Σκοπούς Πρόσβασης* (*Access Purposes*). Οι πρώτοι αντιστοιχούν στους σκοπούς που έχουν συσχετιστεί με τα δεδομένα και ρυθμίζουν την πρόσβαση σε αυτά, αποτελώντας ουσιαστικά την περίληψη της υποκείμενης πολιτικής ιδιωτικότητας. Από την άλλη, ένας Σκοπός Πρόσβασης αντιστοιχεί στον ιδιαίτερο σκοπό μίας συγκεκριμένης ενέργειας πρόσβασης στα δεδομένα. Η απόφαση αναφορικά με την πρόσβαση στα δεδομένα λαμβάνεται τελικά με βάση τη συσχέτιση μεταξύ των αντίστοιχων Σκοπών Πρόσβασης και Προτιθέμενων Σκοπών, με την εισαγωγή της έννοιας της *συμμόρφωσης σκοπών* (*purpose compliance*)· όταν ζητείται πρόσβαση σε κάποιο δεδομένο, ο Σκοπός Πρόσβασης ελέγχεται σε σχέση με τους Προτιθέμενους Σκοπούς για το συγκεκριμένο δεδομένο.

Έχοντας σαν στόχο την απλοποίηση της διαχείρισης, το μοντέλο PBAC ορίζει μία ιεραρχική οργάνωση στο σύνολο των σκοπών $\mathcal{P}$, υπό μορφή δέντρου το οποίο καλείται *Δέντρο Σκοπών* (*Purpose Tree — $\mathcal{PT}$*). Κάθε κόμβος του δέντρου αντιπροσωπεύει κάποιο σκοπό στο $\mathcal{P}$, ενώ κάθε ακμή αντιπροσωπεύει μία ιεραρχική σχέση μεταξύ δύο σκοπών, εκφράζει δηλαδή κάποια σχέση γενίκευσης και ειδίκευσης μεταξύ δύο σκοπών. Η ρίζα του δέντρου συμβολίζεται ως Ρίζα($\mathcal{PT}$) (Root($\mathcal{PT}$)) και αντιπροσωπεύει τον πιο γενικό σκοπό στο $\mathcal{PT}$.

Για κάθε σκοπό $p_i$ στο Δέντρο Σκοπών $\mathcal{PT}$, ορίζονται δύο σύνολα:

- Σύνολο Des($p_i$), το οποίο περιλαμβάνει όλους τους απογόνους (descendants) του $p_i$, δηλαδή κάθε σκοπό $p_j$ στο $\mathcal{PT}$ για τον οποίο υπάρχει ένα καθοδικό μονοπάτι από τον $p_i$ στον $p_j$.
- Σύνολο Anc($p_i$), το οποίο περιλαμβάνει τους προγόνους (ancestors) του $p_i$, δηλαδή κάθε σκοπό $p_j$ στο $\mathcal{PT}$ για τον οποίο υπάρχει ένα ανοδικό μονοπάτι από τον $p_i$ στον $p_j$.

Σημειώνεται ότι ο σκοπός $p_i$ συμπεριλαμβάνεται και στα δύο αυτά σύνολα.

Οι περισσότερες πολιτικές και προτιμήσεις ιδιωτικότητας είναι εκ φύσεως "θετικές", υπό την έννοια ότι οι εκάστοτε δεδηλωμένοι σκοποί είναι επιτρεπόμενοι, δηλαδή λειτουργούν ως επιλεκτικό κριτήριο για την παροχή πρόσβασης στα αντίστοιχα δεδομένα. Στο πλαίσιο αυτό, υπονοείται ότι η απουσία ενός σκοπού από το σύνολο των επιτρεπόμενων σκοπών συνεπάγεται ότι η πρόσβαση για το σκοπό αυτό δεν είναι επιτρεπτή, προσέγγιση η οποία έχει υιοθετηθεί και από τα περισσότερα μοντέλα ελέγχου πρόσβασης. Αντίθετα, το μοντέλο PBAC εισάγει ένα διαχωρισμό μεταξύ των θετικών και των αρνητικών πολιτικών ιδιωτικότητας, ορίζοντας τους *Επιτρεπόμενους Προτιθέμενους Σκοπούς* (*Allowed Intended Purposes — AIP*) και τους *Απαγορευμένους Προτιθέμενους Σκοπούς* (*Prohibited Intended Purposes — PIP*). Η δομή αυτή παρέχει μεγαλύτερη ευελιξία στην άσκηση ελέγχου πρόσβασης, ενώ η χρήση των PIP διασφαλίζει ότι δε θα επιτραπεί ποτέ η πρόσβαση σε δεδομένα για κάποιους συγκεκριμένους σκοπούς. Σε περίπτωση που υπάρχει αντίθεση με-

ταξύ των επιτρεπόμενων και απαγορευμένων σκοπών σε κάποια δεδομένα, υπερισχύει ο απαγορευμένος σκοπός.

Με βάση τα παραπάνω, το μοντέλο PBAC ορίζει τελικά ως έναν Προτιθέμενο Σκοπό IP, σχετιζόμενο με κάποια δεδομένα, την πλειάδα ⟨AIP, PIP⟩, δηλαδή μία δομή η οποία περιλαμβάνει το σύνολο των δεδηλωμένων επιτρεπόμενων σκοπών AIP, καθώς και το σύνολο των απαγορευμένων σκοπών PIP.

Σύμφωνα με το μοντέλο PBAC, όταν κάποιος σκοπός $p_j$ δηλώνεται ως Επιτρεπόμενος Προτιθέμενος Σκοπός (δηλαδή $p_j \in$ AIP), τότε και οι απόγονοί του θεωρούνται ως επιτρεπόμενοι. Από την άλλη, όταν κάποιος σκοπός $p_k$ δηλώνεται ως Απαγορευμένος Προτιθέμενος Σκοπός (δηλαδή $p_k \in$ PIP), τότε τόσο οι απόγονοί του όσο και οι πρόγονοί του θεωρούνται ως απαγορευμένοι. Έτσι, ορίζονται τα εξής σύνολα:

- *Σύνολο Συνεπαγόμενων Επιτρεπόμενων Προτιθέμενων Σκοπών* $\text{AIP}^{\uparrow}$, το οποίο περιλαμβάνει όλους τους απογόνους όλων των σκοπών $\text{aip}_j \in \text{AIP}$, δηλαδή $\text{AIP}^{\uparrow} = \bigcup_{\text{aip}_j \in \text{AIP}} \text{Des}(\text{aip}_j)$.
- *Σύνολο Συνεπαγόμενων Απαγορευμένων Προτιθέμενων Σκοπών* $\text{PIP}^{\updownarrow}$, το οποίο περιλαμβάνει όλους τους προγόνους και απογόνους όλων των σκοπών $\text{pip}_k \in \text{PIP}$, δηλαδή $\text{PIP}^{\updownarrow} = (\bigcup_{\text{pip}_k \in \text{PIP}} \text{Des}(\text{pip}_k)) \cup (\bigcup_{\text{pip}_k \in \text{PIP}} \text{Anc}(\text{pip}_k))$.

Είναι προφανές ότι η διαφορά των δύο αυτών συνόλων εκφράζει το σύνολο (IP*) όλων των προτιθέμενων σκοπών για τους οποίους τελικά θα επιτραπεί η πρόσβαση, δηλαδή $\text{IP}^* = \text{AIP}^{\uparrow} - \text{PIP}^{\updownarrow}$. Σε αυτό το πλαίσιο, ορίζεται η *Συμμόρφωση του Σκοπού Πρόσβασης* (*Access Purpose Compliance*)· ένας Σκοπός Πρόσβασης AP *συμμορφώνεται* με έναν Προτιθέμενο Σκοπό IP, σε ένα Δέντρο Σκοπών $\mathcal{PT}$, όταν και μόνο όταν ικανοποιούνται οι σχέσεις $\text{AP} \notin \text{PIP}^{\updownarrow}$ και $\text{AP} \in \text{AIP}^{\uparrow}$, δηλαδή όταν $\text{AP} \in \text{IP}^*$. Υπονοείται, έτσι, ότι η προσέγγιση που ακολουθεί το PBAC για επίλυση συγκρούσεων μεταξύ AIP και PIP είναι η *πολιτική προτεραιότητας της άρνησης* (*denial-takes-precedence policy*)· σε κάθε περίπτωση, το σύνολο PIP υπερισχύει του συνόλου AIP.

Μία επιπλέον σημαντική συνεισφορά του PBAC έγκειται στον τρόπο προσδιορισμού του σκοπού για τον οποίο ένας συγκεκριμένος χρήστης αποκτά πρόσβαση σε κάποια δεδομένα. Για λόγους απλοποίησης της διαχείρισης εξουσιοδοτήσεων για σκοπούς πρόσβασης, οι χρήστες εξουσιοδοτούνται μέσω των ρόλων τους με μηχανισμούς RBAC. Ωστόσο, το PBAC όχι μόνο στηρίζεται σε συμβατικά μοντέλα RBAC, αλλά επιπλέον τα επεκτείνει με την εισαγωγή της έννοιας του *ρόλου υπό συνθήκη* (*conditional role*), η οποία θεμελιώνεται στις έννοιες των *ιδιοτήτων ρόλου* (*role attributes*) και *συστήματος* (*system attributes*). Με χρήση των ιδιοτήτων ρόλου, οι οποίες γίνονται διαθέσιμες από τη στιγμή που ο χρήστης ενεργοποιεί το συγκεκριμένο ρόλο, ένας Σκοπός Πρόσβασης μπορεί να ανατεθεί σε ένα συγκεκριμένο υποσύνολο χρηστών με τον ίδιο ρόλο. Οι ιδιότητες συστήματος, από την άλλη πλευρά, είναι διαθέσιμες πάντα για το σύστημα ελέγχου πρόσβασης και σχετίζο-

νται με τις καταστάσεις του συστήματος στις οποίες οι εξουσιοδοτήσεις ενεργοποιούνται (ή απενεργοποιούνται). Έτσι, μέσω του ρόλου υπό συνθήκη ουσιαστικά καθίσταται δυνατή η προδιαγραφή και η εφαρμογή RBAC πολιτικών με επίγνωση πλαισίου.

### 2.2.2 Έλεγχος Πρόσβασης Βάσει Ρόλων για Προστασία της Ιδιωτικότητας (P-RBAC)

Μία πολύ σημαντική και επιδραστική προσέγγιση αποτελεί ο λεγόμενος *Έλεγχος Πρόσβασης Βάσει Ρόλων για Προστασία της Ιδιωτικότητας* (*Privacy-aware Role Based Access Control — P-RBAC*) [52][53][54][55]. Πρόκειται για μία οικογένεια μοντέλων με στόχο την επέκταση του RBAC με ενσωμάτωση χαρακτηριστικών για προστασία της ιδιωτικότητας. Η κατευθυντήρια ιδέα πίσω από το P-RBAC έγκειται στο γεγονός ότι η προστασία της ιδιωτικότητας μπορεί να επιτευχθεί με ελάχιστες αλλαγές στις υπάρχουσες υποδομές, μειώνοντας έτσι το κόστος, αλλά και διευκολύνοντας την ολοκλήρωση, καθώς τόσο οι πολιτικές ασφάλειας όσο και ελέγχου πρόσβασης αφορούν τους ίδιους κυρίως πόρους. Σε αυτή τη βάση και σε συνδυασμό με τις Κατευθυντήριες Οδηγίες του OECD, τη νομοθεσία για προστασία της ιδιωτικότητας, καθώς και υπάρχουσες πολιτικές για το σκοπό αυτό, το μοντέλο P-RBAC επεκτείνει το κλασσικό RBAC με την εισαγωγή τριών πρόσθετων χαρακτηριστικών: τους *σκοπούς*, τις *συνθήκες* και τις *υποχρεώσεις*. Ο σκοπός αναφέρεται στην προτιθέμενη χρήση των δεδομένων, οι συνθήκες προσδιορίζουν τις περιπτώσεις στις οποίες επιτρέπεται μία ενέργεια να εκτελεστεί πάνω σε κάποιο αντικείμενο, ενώ οι υποχρεώσεις ορίζουν ενέργειες τις οποίες το υποκείμενο που αιτείται της πρόσβασης πρέπει να πραγματοποιήσει κάποια συγκεκριμένη στιγμή, προκειμένου να του επιτραπεί να εκτελέσει την αιτηθείσα ενέργεια στην παρούσα φάση. Σε αντιστοιχία με το RBAC, το P-RBAC περιλαμβάνει τέσσερα θεωρητικά μοντέλα: *Βασικό P-RBAC* (*Core P-RBAC*), *Ιεραρχικό P-RBAC* (*Hierarchical P-RBAC*), *P-RBAC με συνθήκες* (*Conditional P-RBAC*) και *Καθολικό P-RBAC* (*Universal P-RBAC*).

Το *Βασικό P-RBAC* στηρίζεται στο Βασικό RBAC [28], διατηρώντας το συσχετισμό των αδειών με χρήστες μέσω ρόλων, παραλείποντας όμως την έννοια των συνεδριών. Στο μοντέλο αυτό, σε κάθε άδεια προσδιορίζονται όχι μόνο τα δεδομένα και η ενέργεια που πρόκειται να εκτελεστεί σε αυτά, αλλά επίσης ο σκοπός της αιτηθείσας πρόσβασης, οι συνθήκες κάτω από τις οποίες η πρόσβαση είναι επιτρεπτή και οι υποχρεώσεις οι οποίες επιβάλλονται στο χρήστη. Το Βασικό P-RBAC περιορίζεται στο να προσφέρει μόνο βασικές λειτουργίες, επαρκείς όμως για την προδιαγραφή απλών πολιτικών ιδιωτικότητας. Επίσης, περιγράφει μία σειρά αλγόριθμων για επίλυση συγκρούσεων (conflict resolution) μεταξύ αναθέσεων αδειών και διαχείριση της ασάφειας των υποχρεώσεων. Μάλιστα, ιδιαίτερη προσοχή έχει δοθεί στις υποχρεώσεις, καθώς αποδεικνύονται η πιο σύνθετη συνιστώσα του P-RBAC, ιδιαίτερα σε ό,τι αφορά την αλληλεπίδρασή τους με τις άδειες. Στο πλαίσιο αυτό, παρουσιάζονται οι ακόλουθες σχεδιαστικές επιλογές για την επαρκή έκφραση των υποχρεώσεων, οι οποίες λαμβάνονται υπόψη στο μοντέλο υποχρεώσεων [52]:

- *Συσχέτιση ενεργειών* (*action binding*), υπό την έννοια ότι οι υποχρεώσεις αποτελούν προαπαιτούμενο για την εκτέλεση ορισμένων ενεργειών σε συγκεκριμένα αντικείμενα.
- *Χρονικοί περιορισμοί*, οι οποίοι προσδιορίζουν τη σωστή χρονική στιγμή για την εκτέλεση μίας υποχρέωσης, ορίζοντας αντίστοιχα *προ-υποχρεώσεις* (*pre-obligations*), *μετα-υποχρεώσεις* (*post-obligations*) και *επαναλαμβανόμενες υποχρεώσεις* (*repeating obligations*).
- *Διαφορετικά υποκείμενα*, για περιπτώσεις στις οποίες το υποκείμενο της υποχρέωσης δεν ταυτίζεται με εκείνο που αιτείται της πρόσβασης.
- *Υποχρεώσεις υπό συνθήκη*, για υποχρεώσεις που πρέπει να εκτελεστούν μόνο κάτω από συγκεκριμένες συνθήκες.

Το *Ιεραρχικό P-RBAC* ενισχύει το Βασικό P-RBAC με ιεραρχική οργάνωση των ρόλων, των σκοπών και των αντικειμένων. Οι *Ιεραρχίες Ρόλων* (*Role Hierarchies — RHs*) ακολουθούν τη σημασιολογία και το συμβολισμό του Ιεραρχικού RBAC και περιγράφονται ως μερικές διατάξεις (partial orders), οι οποίες στη γενική περίπτωση υποστηρίζουν πολλαπλή κληρονομικότητα. Οι *Ιεραρχίες Σκοπών* (*Purpose Hierarchies — PHs*) και *Ιεραρχίες Αντικειμένων* (*Object Hierarchies — OHs*) αναπαρίστανται ως δενδρικές δομές, έτσι ώστε κάθε αντικείμενο ή σκοπός να έχει το πολύ έναν απευθείας πρόγονο· συνεπώς, σε αυτήν την περίπτωση δεν υποστηρίζεται πολλαπλή κληρονομικότητα. Η κληρονομικότητα έχει το νόημα της ομαδοποίησης πιο συγκεκριμένων αντικειμένων ή σκοπών σε αντίστοιχες πιο γενικές έννοιες. Έτσι, μία άδεια που αφορά ένα αντικείμενο ή σκοπό υψηλότερου επιπέδου βρίσκει εφαρμογή και σε όλους τους απογόνους του και αντιστρόφως· για να επιτραπεί η πρόσβαση για έναν πατέρα κόμβο στο δέντρο σκοπών ή αντικειμένων, θα πρέπει η πρόσβαση να επιτρέπεται για όλα τα παιδιά του κόμβου αυτού. Σημειώνεται ότι, οι ιεραρχίες ρόλων προσφέρονται για μοντελοποίηση οργανωτικών δομών, όπου οι ιεραρχίες αποτελούν μέσο απεικόνισης αρμοδιοτήτων, ενώ οι ιεραρχίες σκοπών και αντικειμένων, αν και οδηγούν σε συμπαγείς αναθέσεις αδειών, εισάγουν πολυπλοκότητα στον έλεγχο συνέπειας. Επίσης, το Ιεραρχικό P-RBAC προβλέπει ανάλυση αδειών (permission analysis), με κατάλληλη τροποποίηση των αλγόριθμων ανίχνευσης συγκρούσεων του Βασικού P-RBAC.

Το *P-RBAC με συνθήκες* επεκτείνει το Βασικό P-RBAC υποστηρίζοντας πιο σύνθετες και εκφραστικές συνθήκες και πιο ευέλικτες σχέσεις μεταξύ των αναθέσεων αδειών, ουσιαστικά επιτρέποντας τόσο σχέσεις σύζευξης όσο και διάζευξης μεταξύ τους. Επιπλέον, ο έλεγχος της συνέπειας των αναθέσεων αδειών επεκτείνεται σε σχέση με το Βασικό P-RBAC, με την εισαγωγή αποδοτικών αλγόριθμων για τον εντοπισμό των συγκρούσεων, του ιντετερμινισμού στην εφαρμογή υποχρεώσεων και του πλεονασμού κάποιας νέας ανάθεσης άδειας σε σχέση με τις ήδη υπάρχουσες αναθέσεις.

Το *Καθολικό P-RBAC* συνδυάζει το Ιεραρχικό P-RBAC με το P-RBAC με συνθήκες, κληρονομώντας έτσι όλα τους τα χαρακτηριστικά και καθιστώντας πιο πολύπλοκο τον

έλεγχο συνέπειας. Παρουσία ιεραρχιών, οι σχέσεις προγόνου-απογόνου πρέπει να λαμβάνονται υπόψη κατά την ανάλυση αδειών, η οποία τώρα περιλαμβάνει δύο φάσεις: στην πρώτη φάση ελέγχεται αν μία νέα ανάθεση άδειας προκαλεί πλεονασμό, σύγκρουση ή ιντετερμινισμό σε σχέση με το υπάρχον σύνολο αναθέσεων του εκάστοτε ρόλου, των προγόνων και τους απογόνων του, αφού πραγματοποιηθούν οι απαραίτητες τροποποιήσεις με βάση τις ιεραρχίες σκοπών και αντικειμένων και διαδοθούν σε όλους τους προγόνους του συγκεκριμένου ρόλου. Στη δεύτερη φάση ενημερώνονται στο σύστημα όλες οι αναθέσεις αδειών που επηρέασε η πρώτη φάση. Τέλος, το Καθολικό P-RBAC προσθέτει τρία σημαντικά χαρακτηριστικά: *αρνητικές εξουσιοδοτήσεις*, *έλεγχο ροής για την εκτέλεση των υποχρεώσεων* και *αρχές για το συνδυασμό αδειών*.

### 2.2.3 Έλεγχος Πρόσβασης Βάσει Ρόλων με Επίγνωση Σκοπού (PuRBAC)

Το μοντέλο *Ελέγχου Πρόσβασης Βάσει Ρόλων με Επίγνωση Σκοπού* (*Purpose-Aware Role-Based Access Control — PuRBAC*) [56] αποτελεί μία ακόμη επέκταση του RBAC η οποία εστιάζει στην έννοια του σκοπού, στο πλαίσιο πολιτικών για προστασία της ιδιωτικότητας. Στο $PuRBAC_B$, το βασικό μοντέλο που πληροί τις ελάχιστες απαιτήσεις, ο σκοπός αποτελεί μία ξεχωριστή *ενδιάμεση* οντότητα μεταξύ του ρόλου και των αδειών: οι άδειες αντιστοιχίζονται στους σκοπούς για τους οποίους μπορούν να παραχωρηθούν και αυτοί με τη σειρά τους αντιστοιχίζονται στους κατάλληλους ρόλους. Οι ρόλοι ανατίθενται σε χρήστες από τους οποίους μπορούν να ενεργοποιηθούν και να απενεργοποιηθούν στις αντίστοιχες συνεδρίες. Ένα αίτημα πρόσβασης υποβάλλεται στη μορφή ⟨*συνεδρία*, *σκοπός*, *αιτηθείσα άδεια*⟩, όπου μόνο κάποιος από τους σκοπούς που έχουν ανατεθεί στους τρέχοντες ενεργούς ρόλους του χρήστη μπορεί να εισαχθεί, δηλαδή, ο χρήστης δεν μπορεί να χρησιμοποιήσει δεδομένα για ένα σκοπό χωρίς προηγουμένως να έχει εξουσιοδοτηθεί για το σκοπό αυτό. Με αυτό τον τρόπο είναι δυνατόν να επιτευχθεί έλεγχος στο σκοπό που δηλώνει ο χρήστης. Τέλος, τίθενται συνθήκες στις αναθέσεις αδειών σε σκοπούς (permission assignments), οι οποίες περιλαμβάνουν περιορισμούς, καθώς και υποχρεώσεις πριν και μετά την παραχώρηση της άδειας πρόσβασης (pre- και post- obligations αντίστοιχα). Με βάση τα ανωτέρω, η διαδικασία ελέγχου πρόσβασης μπορεί να συνοψιστεί ως εξής: δεδομένου του αιτήματος πρόσβασης, το σύστημα πραγματοποιεί έλεγχο για την ύπαρξη ισχύουσας άδειας, δηλαδή, μίας άδειας η οποία ταυτίζεται με εκείνη του αιτήματος και είναι συσχετισμένη με το σκοπό που παρέχεται, και είτε αποφασίζει υπό συνθήκη εξουσιοδότηση, είτε αποκρίνεται αρνητικά. Στην πρώτη περίπτωση, χορηγείται εξουσιοδότηση μόνο εάν πληρούνται οι συνθήκες που έχουν τεθεί στην ισχύουσα άδεια. Σημειώνεται επίσης, ότι το μοντέλο προβλέπει ότι κάποιες μετά-υποχρεώσεις μπορούν να εκτελεστούν ανεξάρτητα από την απόφαση πρόσβασης.

Το $PuRBAC_H$ επεκτείνει το $\text{PuRBAC}_\text{B}$ με ιεραρχίες ρόλων, σκοπών και αδειών: *ανώτεροι* (*senior*) ρόλοι κληρονομούν τους επιτρεπόμενους για *κατώτερους* (*junior*) ρόλους, η ιεραρχία σκοπών ορίζει σχέσεις *γενίκευσης-ειδίκευσης* ανάμεσα στους σκοπούς, ενώ η ιε-

ραρχία αδειών βασίζεται στην ιεραρχία των δεδομένων, έτσι ώστε εάν ένας χρήστης είναι εξουσιοδοτημένος για μία ενέργεια πάνω σε κάποιον τύπο δεδομένων, να είναι εξουσιοδοτημένος για την ίδια ενέργεια πάνω στους απογόνους του συγκεκριμένου τύπου δεδομένων. Το $PuRBAC_{HH}$ παρέχει ακόμα μεγαλύτερη ευελιξία, χρησιμοποιώντας υβριδική ιεραρχία για ρόλους και σκοπούς, η οποία διακρίνεται σε τρεις τύπους σχέσεων: *κληρονομικότητα* (*inheritance — I*), *ενεργοποίηση* (*activation — A*) και *κληρονομικότητα-ενεργοποίηση* (*inheritance-activation — IA*). Γενικά, η ιεραρχία επιφέρει ποικίλες αλλαγές σε σχέση με το βασικό μοντέλο, κυρίως σε ό,τι αφορά τις υπό συνθήκη αναθέσεις αδειών σε σκοπούς.

### 2.2.4 Το Μοντέλο Ελέγχου Πρόσβασης PRIME

Το FP6 έργο PRIME[6] αποτελεί ορόσημο στο ερευνητικό πεδίο της προστασίας της ιδιωτικότητας, ενώ το μοντέλο ελέγχου πρόσβασης που παρουσίασε ([31][57]) συνιστά ένα από τα πιο σημαντικά επιτεύγματά του, με επιρροές τόσο από τα μοντέλα τύπου ABAC [58], όσο και από τις Κατευθυντήριες Οδηγίες του OECD και την Ευρωπαϊκή νομοθεσία. Η σημασία του έγκειται κυρίως στο γεγονός ότι προτείνει και ενσωματώνει διάφορες έννοιες και τεχνολογίες, συμπεριλαμβανομένων των διαφορετικών τύπων πολιτικών, των κρυπτογραφικών ανώνυμων διαπιστευτηρίων, της αμφίδρομης διαπραγμάτευσης και διαδραστικής εφαρμογής των πολιτικών, των περιορισμών πλαισίου, των μεταδεδομένων για τον έλεγχο δευτερεύουσας χρήσης των δεδομένων, των οντολογιών, κλπ. Μία θεμελιώδης πτυχή του μοντέλου ελέγχου πρόσβασης PRIME αποτελεί η *ανθρωποκεντρικότητα* (*user-centricity*), με στόχο την ενσωμάτωση των υποκείμενων νομικών και κοινωνικών απαιτήσεων.

Το μοντέλο αυτό θεωρεί τρεις διαφορετικούς τύπους πολιτικών:

- **Πολιτικές ελέγχου πρόσβασης**, οι οποίες ορίζουν (θετικές) εξουσιοδοτήσεις για πρόσβαση σε δεδομένα ή υπηρεσίες.
- **Πολιτικές παραχώρησης**, οι οποίες ορίζουν τις προτιμήσεις μίας οντότητας αναφορικά με τη παραχώρηση προσωπικών της στοιχείων, για ποιο σκοπό και ποια ενέργεια, καθώς και κάτω από ποιες συνθήκες θα δημοσιοποιηθεί ένα σύνολο δεδομένων.
- **Πολιτικές διαχείρισης δεδομένων**, οι οποίες ορίζουν με ποιο τρόπο θα πρέπει να διαχειριστούν τα προσωπικά δεδομένα οι παραλήπτες.

Αν και συντακτικά ταυτόσημες, οι πολιτικές ελέγχου πρόσβασης και οι πολιτικές παραχώρησης διαφέρουν σημασιολογικά· οι μεν αφορούν τον πάροχο υπηρεσίας που προσφέρει τους πόρους στους οποίους αναφέρεται το αίτημα πρόσβασης, ενώ οι δε αφορούν το χρήστη που αιτείται πρόσβασης —δηλαδή το *υποκείμενο των δεδομένων*— και από τον οποίο ζητούνται προσωπικά δεδομένα προκειμένου να του επιτραπεί η πρόσβαση.

[6]FP6 IST Project PRIME (Privacy and identity management for Europe), https://www.prime-project.eu/.

Οι πολιτικές διαχείρισης δεδομένων επιτρέπουν στους χρήστες να ορίζουν οι ίδιοι με ποιο τρόπο μπορούν να χρησιμοποιηθούν τα προσωπικά τους δεδομένα από τον πάροχο υπηρεσιών ή/και από εξωτερικές οντότητες, δηλαδή *μετά* την παραχώρησή τους. Μία τέτοια πολιτική ακολουθεί τα δεδομένα ακόμα και όταν αυτά παραχωρούνται σε κάποια εξωτερική οντότητα, σχηματίζοντας έτσι μία αλυσίδα ελέγχου με αρχή της το υποκείμενο των δεδομένων, ακολουθώντας το παράδειγμα των λεγόμενων *sticky policies* [59]. Τα προσωπικά δεδομένα επισημειώνονται με αυτές τις *αντόνομες* πολιτικές, αντί οι τελευταίες να ολοκληρωθούν με τους κανόνες ελέγχου πρόσβασης, επιτυγχάνοντας έτσι το διαχωρισμό μεταξύ πολιτικών που εξυπηρετούν διαφορετικούς σκοπούς. Οι πολιτικές διαχείρισης δεδομένων διαμορφώνονται μέσω μίας διαδικασίας διαπραγμάτευσης, κατά την οποία ο χρήστης σταδιακά προσαρμόζει προκαθορισμένα πρότυπα της πολιτικής που προσφέρονται από τον πάροχο υπηρεσιών.

Επίσης πρέπει να σημειωθεί ότι το μοντέλο πραγματοποιεί εκτεταμένη χρήση αφαίρεσης στην προδιαγραφή των πολιτικών, η οποία διευκολύνεται από κατάλληλα ορισμένες οντολογίες στους πιο σημαντικούς τομείς του μοντέλου, δηλαδή τους χρήστες, τις υπηρεσίες/αντικείμενα, τα πιστοποιητικά, τις δηλώσεις, τις ενέργειες, τους σκοπούς, τους τύπους προσωπικών δεδομένων και τις κατηγορίες παραληπτών.

Με δεδομένο ένα αίτημα πρόσβασης της μορφής ⟨*αναγνωριστικό_χρήστη*, *ενέργεια*, *αντικείμενο*, *σκοποί*⟩, η αλληλεπίδραση μεταξύ των εμπλεκόμενων μερών περιλαμβάνει δύο φάσεις:

- **Αλληλεπίδραση χρήστη-παρόχου υπηρεσίας**: Ο πάροχος υπηρεσίας λαμβάνει το αίτημα, αναζητά εφαρμόσιμες πολιτικές ελέγχου πρόσβασης –με βάση την ενέργεια, το αντικείμενο και σκοπούς– και, εάν κριθεί απαραίτητο, ζητά προσωπικά δεδομένα του χρήστη, παρουσιάζοντας επίσης και ένα ή περισσότερα πρότυπα πολιτικών διαχείρισης δεδομένων που θα χρησιμοποιηθούν από τον χρήστη. Ο τελευταίος αποτιμά τις πολιτικές παραχώρησής του και, αν υπάρχει τουλάχιστον μία εφαρμόσιμη που να πληρούνται οι συνθήκες της, στέλνει τα δεδομένα του μαζί με ένα πιθανώς προσαρμοσμένο πρότυπο πολιτικής διαχείρισης δεδομένων. Ο πάροχος υπηρεσιών επαναξιολογεί τις αντίστοιχες πολιτικές ελέγχου πρόσβασης με βάση τα προσωπικά δεδομένα και εφόσον η αποτίμηση ολοκληρωθεί με επιτυχία, χορηγείται άδεια πρόσβασης. Σημειώνεται ότι η παραχώρηση των προσωπικών δεδομένων και η προσαρμογή του προτύπου πολιτικής διαχείρισης δεδομένων ενδέχεται να απαιτεί πολλαπλά βήματα διαπραγμάτευσης, προκειμένου να επιτευχθεί συμφωνία.
- **Αλληλεπίδραση εξωτερικής οντότητας-παρόχου υπηρεσίας**: Όταν, σε μετέπειτα στάδιο, μία εξωτερική οντότητα ζητάει προσωπικά δεδομένα του χρήστη, τα οποία είναι αποθηκευμένα στον πάροχο της υπηρεσίας, ο τελευταίος πρέπει να αξιολογήσει το αίτημα όχι μόνο με βάση τις δικές του πολιτικές ελέγχου πρόσβασης, όπως στην προηγούμενη φάση, αλλά επίσης λαμβάνοντας υπόψιν τις πολιτικές παραχώρησης

που επισυνάπτονται στα δεδομένα.

Τέλος, η προστασία της ιδιωτικότητας σε ένα τέτοιο σύστημα μπορεί να ενισχυθεί περαιτέρω με χρήση πρόσθετων τεχνολογιών, όπως είναι η ανώνυμη επικοινωνία, τα ιδιωτικά/ανώνυμα διαπιστευτήρια, κλπ., ή με την παροχή των κατάλληλων διεπαφών χρήστη.

### 2.2.5 Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης PRISM

Στα πλαίσια του Ευρωπαϊκού έργου PRISM[7], υλοποιήθηκε από την ερευνητική ομάδα του ΕΜΠ ένα σημασιολογικό μοντέλο ελέγχου πρόσβασης και εξουσιοδοτήσεων ειδικά για να καλύψει τις απαιτήσεις της παθητικής παρακολούθησης δικτύων, λαμβάνοντας παράλληλα υπόψη τις τεχνικές απαιτήσεις που απορρέουν από τις Κατευθυντήριες Οδηγίες του OECD και την Ευρωπαϊκή Νομοθεσία αναφορικά με την προστασία της ιδιωτικότητας. Προβλέπει ένα μηχανισμό μετασχηματισμών για αποτελεσματική ρύθμιση του βαθμού λεπτομέρειας των δεδομένων για τα οποία παρέχεται πρόσβαση, ενώ ένα άλλο σημαντικό χαρακτηριστικό της εν λόγω προσέγγισης αποτελούν οι μηχανισμοί που εισάγει για την αποφυγή της ιδιαίτερα απαιτητικής σε πόρους συλλογιστικής σε πραγματικό χρόνο.

Τα θεμελιώδη στοιχεία που συνθέτουν το μοντέλο αυτό είναι τα ακόλουθα [60][61]: ένα σύνολο *Τύπων Δεδομένων* (*Data Types — DT*), ένα σύνολο *Σκοπών* (*Purposes — Pu*), ένα σύνολο *Ρόλων* (*Roles — R*), ένα σύνολο *Δραστών* (*Actors — A*), ένα σύνολο *Κανόνων* (*Rules — Ru*), ένα σύνολο *Συνθηκών* (*Conditions — C*) και ένα σύνολο *Υποχρεώσεων* (*Obligations — O*).

Οι κανόνες και οι συνθήκες αντιπροσωπεύουν, αντίστοιχα, τους κανόνες ελέγχου πρόσβασης, δηλαδή άδειες και απαγορεύσεις, και τους περιορισμούς πλαισίου σε πραγματικό χρόνο σε ό,τι αφορά την εφαρμοσιμότητα των κανόνων, ενώ οι υποχρεώσεις αναφέρονται στις συμπληρωματικές προς την εφαρμογή ενός κανόνα ενέργειες. Το σύνολο των τύπων προσωπικών δεδομένων (*DT*) χαρακτηρίζεται από τρεις σχέσεις, οι οποίες ορίζουν μερικές διατάξεις των τύπων προσωπικών δεδομένων και αντικατοπτρίζουν, αντίστοιχα, την κληρονομικότητα χαρακτηριστικών, το επίπεδο λεπτομέρειας της ίδιας έννοιας και τη συμπερίληψη ενός τύπου δεδομένων σε κάποιον άλλο. Ομοίως, το σύνολο των σκοπών (*Pu*) χαρακτηρίζεται από δύο σχέσεις, για την κληρονομικότητα χαρακτηριστικών και την ανάλυση ενός σκοπού σε υπο-σκοπούς, οι οποίοι θα πρέπει να ικανοποιούνται στο σύνολό τους, αντίστοιχα. Οι ίδιες σχέσεις συναντώνται και στο σύνολο των ρόλων (*R*), όπου μία OR σχέση καθορίζει την κληρονομικότητα, ενώ μία AND σχέση αντικατοπτρίζει τη ρητή συμμετοχή κάποιων ρόλων σε έναν άλλο, υπονοώντας την ανάγκη αλληλεπίδρασης των συμμετεχόντων ρόλων για την εκτέλεση κάποιας ενέργειας. Οι δράστες συσχετίζονται με

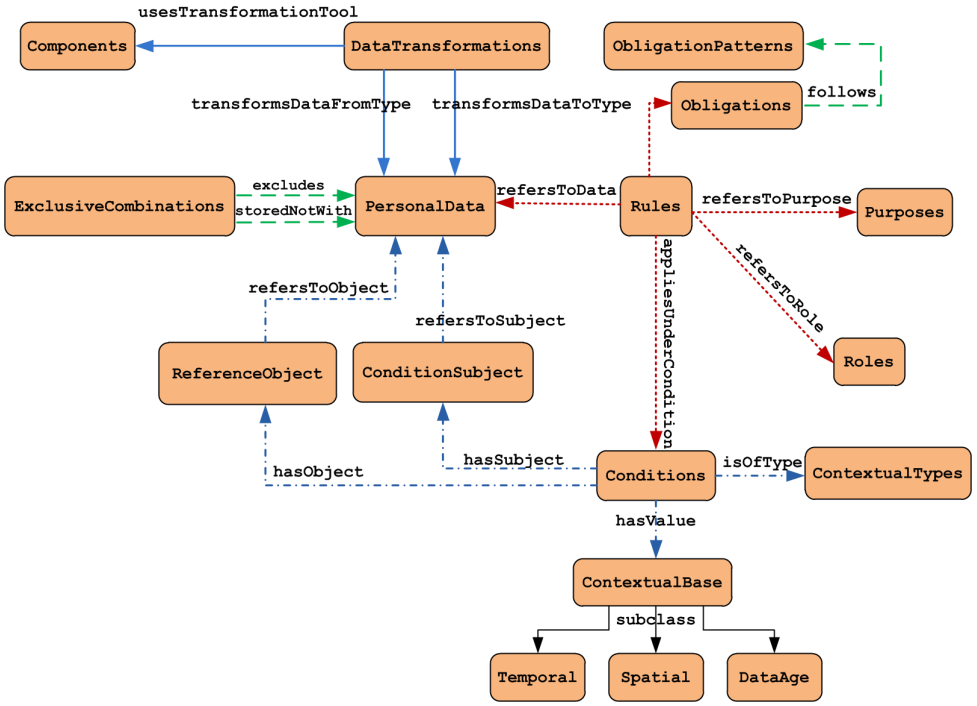
[7]FP7 ICT Project PRISM (Privacy-aware Secure Monitoring), http://www.fp7-prism.eu/.

ρόλους μέσω των σχετικών αναθέσεων (Role Assignments) και οι σκοποί ανατίθενται σε ρόλους με τη μορφή αδειών, καθώς δεν επιτρέπεται όλοι οι ρόλοι να ενεργήσουν για την ικανοποίηση όλων των πιθανών σκοπών. Τελικά, οι κανόνες ελέγχου πρόσβασης, από τους οποίους προκύπτουν οι σχετικές εξουσιοδοτήσεις, συσχετίζονται πάντα με μία πλειάδα της μορφής ⟨personal data types, purpose, role⟩˙ δηλαδή, τα τρία σύνολα αποτελούν το πεδίο ορισμού των κανόνων, ενώ μία πρόσθετη παράμετρος αντικατοπτρίζεται στις συνθήκες, εφόσον υπάρχουν: $Ru = DT^n \times Pu \times R \times C$. Οι κανόνες είναι είτε *θετικοί* είτε *αρνητικοί*.

Επίσης, το μοντέλο αυτό εισάγει τις έννοιες των *Επιτρεπόμενων Τύπων Δεδομένων* (*Permitted Data Types — PDT*) και των *Μη Επεξεργασμένων Επιτρεπόμενων Τύπων Δεδομένων* (*Raw Permitted Data Types — PDT**), καθώς και τα αντίστοιχα σύνολα *PDT* και *PDT**. Το πρώτο σύνολο αφορά τα δεδομένα τα οποία είναι εξουσιοδοτημένος να λαμβάνει ο χρήστης της εκάστοτε εφαρμογής παρακολούθησης για την εκπλήρωση κάποιου σκοπού, ενώ το δεύτερο απαρτίζεται από δεδομένα τα οποία περιλαμβάνονται ρητά στις ροές παρακολούθησης (π.χ., πεδία της επικεφαλίδας πρωτοκόλλου) και τα οποία επιτρέπεται να προσπελάσουν τα στοιχεία του συστήματος που πραγματοποιούν την επεξεργασία των δεδομένων, ώστε να παράξουν το σύνολο *PDT*. Αυτός ο διαχωρισμός αντανακλά τα δύο στάδια ελέγχου πρόσβασης που εφαρμόζει το PRISM˙ τόσο κατά τη συλλογή των δεδομένων κατευθείαν από το δίκτυο, όσο και κατά την παραχώρησή τους μετά από ενδεχόμενη επεξεργασία στην εφαρμογή παρακολούθησης. Επιπλέον, ο έλεγχος πρόσβασης πραγματοποιείται σε δύο φάσεις, που αφορούν σε *στατικό* και *δυναμικό* έλεγχο, αντίστοιχα. Στη φάση του στατικού ελέγχου εφαρμόζονται οι κανόνες που ισχύουν εκ των προτέρων, με βάση τα σημασιολογικά χαρακτηριστικά των δεδομένων, των ρόλων και των σκοπών, ενώ στη δεύτερη φάση γίνεται σε πραγματικό χρόνο αποτίμηση του *πλαισίου ιδιωτικότητας* (*privacy context*), για την προσαρμογή της διαδικασίας ελέγχου πρόσβασης στις συγκεκριμένες συνθήκες που διέπουν ένα αίτημα. Σημειώνεται ότι κατά την πρώτη φάση γίνεται χρήση X.509 πιστοποιητικών [62] για την κωδικοποίηση των στατικών πτυχών της πιστοποίησης, της εξουσιοδότησης και του ελέγχου πρόσβασης, τα οποία παράγονται μέσω εξαντλητικού συλλογισμού στην Οντολογία PRISM. Για παράδειγμα, ένα πιστοποιητικό *CertPDT* πιστοποιεί τους τύπους επεξεργασμένων δεδομένων στους οποίους επιτρέπεται να αποκτήσει πρόσβαση κάποιος ρόλος για κάποιο σκοπό, ενώ ένα πιστοποιητικό *CertRA* πιστοποιεί ότι στον κάτοχό του έχουν ανατεθεί οι αντίστοιχοι ρόλοι.

Τη βάση γνώσης του συστήματος PRISM σε ό,τι αφορά κανόνες ελέγχου πρόσβασης και εξουσιοδοτήσεων, καθώς και τα σχετικά μεταδεδομένα, συνιστά ένα σημασιολογικό μοντέλο για προστασία της ιδιωτικότητας υλοποιημένο σαν μία OWL [63] οντολογία. Όπως φαίνεται στο Σχήμα 3 [64][65], οι κλάσεις που απαρτίζουν την Οντολογία PRISM είναι οι ακόλουθες:

- `PersonalData`, για την αναπαράσταση των διαφορετικών τύπων προσωπικών δεδομένων και των μεταξύ τους συσχετίσεων




Σχήμα 3: Οντολογία PRISM.

- `Purposes`, η οποία αντανακλά τους σκοπούς για τους οποίους προσωπικά δεδομένα συλλέγονται και/ή υπόκεινται σε επεξεργασία
- `Roles`, για την περιγραφή των ρόλων τους οποίους κατέχουν οι δράστες στο σύστημα
- `Rules`, για τον ορισμό των κανόνων ελέγχου πρόσβασης
- `Components`, τα στιγμιότυπα της οποίας συνιστούν τη "σημασιολογική υπογραφή" των στοιχείων του συστήματος που επεξεργάζονται τα δεδομένα
- `DataTransformations`, η οποία ορίζει μετασχηματισμούς δεδομένων από έναν τύπο σε κάποιον άλλο
- `ExclusiveCombinations`, για τη περιγραφή αμοιβαίως αποκλειόμενων τύπων δεδομένων σε ό,τι αφορά την παραχώρησή τους και/ή την αποθήκευσή τους σε βάσεις δεδομένων
- `Conditions`, για τον ορισμό περιορισμών πλαισίου
- `ConditionSubject`, `ReferenceObject`, `ContextualBase`, για τον προσδιορισμό του υποκειμένου, του αντικειμένου και του τύπου των περιορισμών πλαισίου
- `Temporal`, `Spatial`, `DataAge`, οι οποίες αντικατοπτρίζουν κάποιους τύπους περιορισμών πλαισίου

- `Obligations`, η οποία περιγράφει τις συμπληρωματικές ως προς την εφαρμογή κάποιου κανόνα ενέργειες, ενώ η κλάση `ObligationPatterns` ορίζει κάποια στοιχειώδη πρότυπα τα οποία ακολουθούν οι υποχρεώσεις

Τέλος, σημειώνεται ότι ο βασικός περιορισμός της εν λόγω προσέγγισης έγκειται στο γεγονός ότι σχεδιάστηκε για περιβάλλοντα μοναδικού αισθητήρα δικτύου˙ σαν αποτέλεσμα, δεν περιλαμβάνει έννοιες όπως ο οργανισμός και δεν είναι κατάλληλη για κατανεμημένα περιβάλλοντα και για την επαλήθευση της μεταξύ τους αλληλεπίδρασης.

### 2.2.6 Παρατηρήσεις

Μολονότι οι προσεγγίσεις που παρουσιάστηκαν αποτελούν σημαντικές τεχνολογίες στον έλεγχο πρόσβασης και χρήσης, δεν έχουν σχεδιασθεί, και άρα δεν είναι κατάλληλες, για ιδιαίτερα δυναμικά και κατανεμημένα περιβάλλοντα, ενώ επιπλέον, στην πλειονότητά τους, είτε δεν υποστηρίζουν επίγνωση πλαισίου είτε υποστηρίζουν μόνο κάποιες εξαιρετικά απλές περιπτώσεις. Σαν αποτέλεσμα, παρουσιάζουν μία εγγενή αδυναμία ανταπόκρισης στους κινδύνους που δημιουργούνται από τα ιδιαίτερα χαρακτηριστικά των κατανεμημένων αρχιτεκτονικών και των υποκείμενων τεχνολογιών. Σε τέτοιου είδους περιβάλλοντα, ο έλεγχος πρόσβασης θα πρέπει να συντονίζεται μεταξύ των κατανεμημένων οντοτήτων που αλληλεπιδρούν για την εκπλήρωση σύνθετων λειτουργιών και σκοπών, ενώ η αυτοματοποίηση της εφαρμογής πολιτικών ιδιωτικότητας καθίσταται ιδιαίτερα κρίσιμη για την αποτελεσματικότητα και τη συνέπεια της αλληλεπίδρασης κατανεμημένων συστημάτων. Επιπλέον, τα μοντέλα αυτά δεν είναι σε θέση να ελέγξουν την αλληλεπίδραση καθεαυτή με όρους ροής πληροφορίας μεταξύ κατανεμημένων εργασιών, τόσο κατά την προδιαγραφή της εν λόγω αλληλεπίδρασης όσο και κατά την πραγματοποίησή της. Αν και έχει σημειωθεί σημαντική ερευνητική προσπάθεια για την εφαρμογή ελέγχου πρόσβασης στις συγγενικές περιοχές της *Διαχείρισης Ροών Εργασιών* (*Workflow Management*) (π.χ., [66][67]) και της *Μοντελοκεντρικής Ασφάλειας* (*Model-Driven Security*) ([68][69]), οι προσεγγίσεις αυτές περιορίζονται στην εφαρμογή των πολιτικών ιδιωτικότητας μόνο κατά την εκτέλεση και όχι κατά τη σχεδίαση κατανεμημένων διαδικασιών.

Μία επιπρόσθετη απαίτηση συνιστά η ευελιξία στον ορισμό κανόνων ελέγχου πρόσβασης. Οι τελευταίοι θα πρέπει να είναι δυνατόν να ορίζονται σε κάθε πιθανό επίπεδο αφαίρεσης, καθώς η προδιαγεγραμμένη αλληλεπίδραση μεταξύ συστημάτων μπορεί να περιλαμβάνει μόνο συγκεκριμένες (concrete), μόνο αφηρημένες (abstract), ή οντότητες και των δύο επιπέδων αφαίρεσης. Οι περισσότερες σύγχρονες προσεγγίσεις (π.χ., [31][51][56][53]) χρησιμοποιούν αφαίρεση μόνο για το υποκείμενο, ακολουθώντας το παράδειγμα του RBAC, ενώ και η πλειονότητα των καθιερωμένων μοντέλων ελέγχου πρόσβασης, όπως τα DAC και MAC [70], θεμελιώνονται αποκλειστικά σε συγκεκριμένες οντότητες.

## 2.3 Χρήση των Οντολογιών στον Έλεγχο Πρόσβασης

Η έλευση του Σημασιολογικού Ιστού και των συνακόλουθων τεχνολογιών, όπως είναι οι σημασιολογικές οντολογίες και οι μηχανισμοί συλλογιστικής, έχουν προσφέρει στον έλεγχο πρόσβασης νέες δυνατότητες. Ως εκ τούτου, διάφορες προσεγγίσεις έχουν ενσωματώσει τεχνολογίες του Σημασιολογικού Ιστού με διάφορους τρόπους, με στόχο τη συγχώνευση των πολιτικών ασφάλειας, όπως αυτές εκφράζονται από τους διάφορους εταίρους, καθώς και για να προσφέρουν υψηλή εκφραστικότητα στις υποκείμενες έννοιες και δυνατότητες ευφυούς εξαγωγής συμπερασμάτων. Καταρχήν, η γλώσσα OWL (Web Ontology Language) [63] χρησιμοποιήθηκε για την ανάπτυξη γλωσσών προδιαγραφής πολιτικών για τον Ιστό, όπως οι Rei και Kaos [71], καθώς και για την επίτευξη διαλειτουργικότητας κατά την πρόσβαση σε ετερογενείς βάσεις δεδομένων, όπως παρουσιάζεται στις εργασίες [72][73][74].

Η ενότητα αυτή παρέχει μία επισκόπηση των πιο χαρακτηριστικών προσεγγίσεων ελέγχου πρόσβασης που κάνουν χρήση τεχνολογιών Σημασιολογικού Ιστού [75]. Τα κίνητρα, το πεδίο εφαρμογής και τα πρότυπα χρήσης που ακολουθούνται από τις εξεταζόμενες προσεγγίσεις διαφέρουν σημαντικά. Ως εκ τούτου, οι ακόλουθες ενότητες υιοθετούν μία κατηγοριοποίηση που υπογραμμίζει τις σημαντικές διαφοροποιήσεις μεταξύ των εν λόγω προσεγγίσεων. Καθώς το μοντέλο RBAC αποτελεί τη βάση για την πραγματοποίηση ελέγχου πρόσβασης, η Ενότητα 2.3.1 ερευνά προσεγγίσεις που στοχεύουν στην οντολογική υλοποίησή του, ενώ οι Ενότητες 2.3.2, 2.3.3 και 2.3.4 αναφέρονται σε συστήματα τα οποία εστιάζουν σε πιο εξειδικευμένα χαρακτηριστικά. Συγκεκριμένα, η Ενότητα 2.3.2 παρουσιάζει προσεγγίσεις που επεκτείνουν σημασιολογικά το μοντέλο ιδιοτήτων της XACML, η Ενότητα 2.3.3 ερευνά τη χρήση των τεχνολογιών του Σημασιολογικού Ιστού για την επίτευξη επίγνωσης πλαισίου κατά τον έλεγχο πρόσβασης, και η Ενότητα 2.3.4 περιγράφει μηχανισμούς για τον οντολογικό προσδιορισμό των προτιμήσεων ιδιωτικότητας των χρηστών όσον αφορά τη διαδικασία ελέγχου πρόσβασης και χρήσης. Η έλευση των online υπηρεσιών κοινωνικής δικτύωσης δημιουργεί νέες προκλήσεις στην περιοχή του ελέγχου πρόσβασης, οπότε η Ενότητα 2.3.5 ασχολείται με τις αντίστοιχες σημασιολογικές προσεγγίσεις. Τέλος, η Ενότητα 2.3.6 προσφέρει μία σύγκριση των προσεγγίσεων που παρουσιάστηκαν στις προηγούμενες ενότητες στη βάση σημαντικών τάσεων και χαρακτηριστικών των υπό μελέτη προσεγγίσεων ελέγχου πρόσβασης.

### 2.3.1 Οντολογική Υλοποίηση του Μοντέλου RBAC

Τα τελευταία χρόνια έχουν παρουσιαστεί αρκετές προσεγγίσεις οι οποίες έχουν σαν στόχο την έκφραση πολιτικών τύπου RBAC [28] κάνοντας χρήση της γλώσσας OWL. Στο πλαίσιο αυτό, οι οντολογίες χρησιμοποιούνται για να αναπαραστήσουν τις κύριες έννοιες του RBAC —Ενέργεια (Action), Υποκείμενο (Subject), Αντικείμενο (Object), Ρόλος (Role), Άδεια (Permission)— καθώς επίσης ιεραρχίες ρόλων και δυναμικό και στατικό Δια-

χωρισμό Καθηκόντων.

Μία σημαντική εργασία στην περιοχή αυτή παρουσιάζεται στο [76], όπου οι Finin et al. εισάγουν το μοντέλο R*OWL*BAC, το οποίο προτείνει δύο διαφορετικές προσεγγίσεις σε ό,τι αφορά την αναπαράσταση ρόλων: η πρώτη αντιστοιχίζει ρόλους σε κλάσεις και υποκλάσεις στις οποίες τα υποκείμενα είναι δυνατόν να ανήκουν, ενώ η δεύτερη αναπαριστά ρόλους ως στιγμιότυπα (instances) της generic κλάσης `Role`. Και στις δύο περιπτώσεις, οι ενέργειες, τα υποκείμενα και τα αντικείμενα αντικατοπτρίζονται στις αντίστοιχες κλάσεις, ενώ οι αμοιβαίως αποκλειόμενες υποκλάσεις `PermittedAction` και `ProhibitedAction` της κλάσης `Action` εισάγονται με σκοπό τον έλεγχο της πρόσβασης. Στην πρώτη περίπτωση, οι ρόλοι (και οι ενεργοί ρόλοι) αναπαρίστανται ως κλάσεις χρηστών και η σχέση ιεραρχίας ρόλων αντιστοιχίζεται στη σχέση υπαγωγής (subsumption relation) της OWL. Επιπλέον, αυτή η προσέγγιση αντιστοιχίζει περιορισμούς στατικού και δυναμικού SoD σε περιορισμούς αμοιβαίως αποκλειόμενων OWL κλάσεων. Η δεύτερη προσέγγιση, η οποία μοντελοποιεί τους ρόλους ως στιγμιότυπα, χρησιμοποιεί τις ιδιότητες `role` και `activeRole` έτσι ώστε να συνδέσει τους χρήστες με τους δυνατούς και ενεργούς τους ρόλους, αντίστοιχα. Στην περίπτωση αυτή, η ιεραρχία των ρόλων επιτυγχάνεται με χρήση της ιδιότητας `subRole` και οι περιορισμοί SoD μέσω των εξειδικευμένων ιδιοτήτων `ssod` και `dsod`. Ωστόσο, στην προσέγγιση αυτή, δεν είναι δυνατόν να αξιοποιηθεί DL συλλογιστική για την εφαρμογή RBAC. Αντ' αυτού, οι κανόνες χρειάζεται να προστεθούν στην οντολογία, υποβαθμίζοντας κατά συνέπεια την απόδοση του συστήματος.

Παρόμοια με το μοντέλο R*OWL*BAC, οι Ferrini et al. παρουσιάζουν μία προσέγγιση, η οποία αναφέρεται ως XACML+OWL [77]. Σε αυτό το μοντέλο, η γλώσσα OWL χρησιμοποιείται σε συνδυασμό με την XACML [40], με στόχο την αποσύνδεση της διαχείρισης των περιορισμών και των RBAC ιεραρχιών από την προδιαγραφή και την εφαρμογή καθεαυτών των XACML πολιτικών. Επιπλέον, αντιμετωπίζει κάποιες ελλείψεις του μοντέλου R*OWL*BAC, όπως η ασυνέπεια που εμφανίζεται λόγω της δυνατότητας δύο κλάσεις που περιλαμβάνουν η μία την άλλη (σύμφωνα με την ιεραρχία των ρόλων) να υπόκεινται την ίδια στιγμή σε κάποιον περιορισμό Διαχωρισμού Καθηκόντων. Τα υποκείμενα αναπαρίστανται ως OWL στιγμιότυπα, ενώ πληροφορία σχετική με αυτά είναι δυνατό να εξαχθεί μέσω *σημασιολογικών λειτουργιών* που ορίζονται στο σύστημα. Επίσης, η προσέγγιση αυτή υιοθετεί ένα περισσότερο ευέλικτο σχήμα προδιαγραφής περιορισμών δυναμικού Διαχωρισμού Καθηκόντων, με την προσθήκη των κλάσεων `Resource` και `Permission`, οι οποίες, σε συνδυασμό με την κλάση `Action`, επιτρέπουν πιο περίπλοκους περιορισμούς που αφορούν όχι μόνο τα υποκείμενα, αλλά και τις ενέργειες και τους πόρους. Το μοντέλο XACML+OWL αξιοποιεί το μηχανισμό υποχρεώσεων της XACML για τη διαχείριση των περιορισμών δυναμικού SoD, έτσι ώστε για κάθε άδεια που χορηγείται, να προστίθεται στην οντολογία μία λίστα αξιωμάτων, ανάγοντας έτσι το πρόβλημα αξιολόγησης των περιορισμών στο πρόβλημα του ελέγχου της συνέπειας της οντολογίας.

Μία ακόμη προσέγγιση στην ίδια φιλοσοφία παρουσιάζεται στο [78], όπου οι He

et al. ορίζουν μία υψηλού επιπέδου OWL DL οντολογία και κανόνες εκφρασμένους στη Γλώσσα Κανόνων Σημασιολογικού Ιστού (Semantic Web Rule Language — SWRL) [79] που μπορούν να χρησιμοποιηθούν για να αναπαραστήσουν αλλά και να επεκτείνουν το NIST πρότυπο RBAC [28], συνδυάζοντας παράλληλα το τελευταίο με το μοντέλο ABAC [30], ώστε να υλοποιηθεί έλεγχος πρόσβασης για Υπηρεσίες Ιστού. Η προσέγγιση αυτή επιτυγχάνει δυναμική ανάθεση ρόλων βάσει των διαπιστευτηρίων (credentials) του εκάστοτε χρήστη και των ιδιοτήτων τους, καθώς και δυναμική συσχέτιση των δικαιωμάτων πρόσβασης με ρόλους μέσω ιδιοτήτων που σχετίζονται με υπηρεσίες. Ομοίως, το μοντέλο RBAC υιοθετείται στα [80] και [81] με παρεμφερή τρόπο και επεκτείνεται με ιδιότητες πλαισίου. Έτσι, παρουσιάζεται ένα σύστημα ελέγχου πρόσβασης με επίγνωση πλαισίου για συνεργαζόμενα περιβάλλοντα, σχεδιασμένο και υλοποιημένο με χρήση τεχνολογιών Σημασιολογικού Ιστού. Η RBAC οντολογία ορίζεται και στη συνέχεια ενσωματώνεται σε μία οντολογία για κάποιο συγκεκριμένο τομέα (domain specific ontology), ώστε να ληφθούν υπόψη τα χαρακτηριστικά της εκάστοτε εφαρμογής κατά την προδιαγραφή των πολιτικών και την απόφαση για τον έλεγχο πρόσβασης. Η περιορισμένη εκφραστική δύναμη της Περιγραφικής Λογικής (Description Logic) μετριάζεται με την εισαγωγή ερωτημάτων SPARQL [82] που είναι σε θέση να ελέγχουν πρόσθετους περιορισμούς σύμφωνα με κάποια διαθέσιμη βάση γνώσης.

### 2.3.2 Σημασιολογική Επέκταση του Μοντέλου Ιδιοτήτων της XACML

Εκτός από το μοντέλο XACML+OWL [77] που παρουσιάστηκε στην προηγούμενη ενότητα, αξιοσημείωτη ερευνητική προσπάθεια έχει επενδυθεί στην αξιοποίηση της XACML σε συνδυασμό με οντολογίες, με τις περισσότερες προσεγγίσεις να στοχεύουν στην αντιμετώπιση της περιορισμένης εκφραστικότητας του μοντέλου ABAC. Προς αυτήν την κατεύθυνση, η προσέγγιση που παρουσιάζεται στο [83] προτείνει ένα μηχανισμό εξαγωγής συμπερασμάτων βασισμένο σε οντολογίες, ο οποίος επεκτείνει τη διαχείριση ιδιοτήτων της XACML για την απλοποίηση της προδιαγραφής και της συντήρησης των ABAC πολιτικών. Η πρότυπη XACML αρχιτεκτονική ενισχύεται με δύο επεκτάσεις, το Μηχανισμό Εξαγωγής Συμπερασμάτων (Inference Engine) και το Σημείο Διαχείρισης Οντολογίας (Ontology Administration Point — OAP). Οι ιδιότητες των χρηστών, των πόρων και του περιβάλλοντος ορίζονται οντολογικά και διατίθενται από το Σημείο Διαχείρισης Οντολογίας και στη συνέχεια, ο Μηχανισμός Εξαγωγής Συμπερασμάτων πραγματοποιεί τις αντιστοιχίσεις μεταξύ των διαφορετικών ιδιοτήτων και των συνθηκών ιδιοτήτων. Η εξαγωγή γνώσης επιτυγχάνεται με τη βοήθεια SWRL κανόνων και οι εξαχθείσες ιδιότητες μπορούν στη συνέχεια να ερωτηθούν από τον Διαχειριστή Πλαισίου μέσω SPARQL ερωτημάτων.

Η προσέγγιση που παρουσιάζεται στο [84] επικεντρώνεται στους περιορισμούς εκφραστικότητας της XACML όσον αφορά την αναπαράσταση γνώσης. Συγκεκριμένα, επεκτείνει την XACML ούτως ώστε να υποστηρίζει συλλογιστική βάσει οντολογιών και εξαγωγή συμπερασμάτων βάσει κανόνων, διατηρώντας όμως τη χρηστικότητα των αρχικών

της χαρακτηριστικών. Στο πλαίσιο αυτό, ένα ευφυές XACML κέλυφος, το οποίο βασίζεται σε ένα πολυεπίπεδο σημασιολογικό σύστημα, χρησιμοποιείται για να ενισχυθεί η σημασιολογία και η αναπαράσταση γνώσης της XACML με χρήση τεχνολογιών Σημασιολογικού Ιστού. Σημειώνεται ότι, σε αντίθεση με την XACML όπου ο τύπος δεδομένων μίας ιδιότητας αναφέρεται σε κάποιο στοιχειώδη τύπο, η προσέγγιση αυτή επιτρέπει την αντιστοίχιση του τύπου δεδομένων σε κάποια οντολογική κλάση, με αποτέλεσμα να καθίσταται δυνατή η κληρονομικότητα σημασιολογικής γνώσης.

Επίσης, στο [85] παρουσιάζεται ένα XML φίλτρο ικανό να ρυθμίζει τη δημοσιοποίηση πληροφοριών, με βάση τόσο την XML δομή του εγγράφου, όσο και τη σημασιολογία του περιεχομένου του, με την απευθείας ενσωμάτωση μίας βάσης γνώσης, η οποία περιέχει μία περιγραφή του τομέα, σε μία μηχανή XACML. Ουσιαστικά, τα OWL αρχεία περιέχουν την περιγραφή των εννοιών και των μεταξύ τους σχέσεων, καθώς και την αντιστοίχιση των εννοιών σε στοιχεία του εγγράφου. Ένα Σημασιολογικό Σημείο Πολιτικών (Policy Semantic Point — PSP) λειτουργεί ως γέφυρα ανάμεσα στον έλεγχο πρόσβασης και το οντολογικό μοντέλο, με την αποδοχή και εκτέλεση SPARQL ερωτημάτων στην εξαχθείσα βάση γνώσης.

### 2.3.3 Επίγνωση Πλαισίου Βασισμένη σε Οντολογίες

Μία σημαντική πτυχή του ελέγχου πρόσβασης αντανακλάται από την έννοια του *πλαισίου*, το οποίο γενικά αναφέρεται σε πληροφορίες που περιγράφουν την κατάσταση στην οποία βρίσκεται το σύστημα. Με άλλα λόγια, το πλαίσιο περιλαμβάνει στατικά και δυναμικά χαρακτηριστικά του περιβάλλοντος, όπως εκείνα που αφορούν το χώρο, το χρόνο και το ιστορικό. Οι παράμετροι πλαισίου που αφορούν το υποκείμενο, το αντικείμενο ή την ενέργεια ενός αιτήματος πρόσβασης, επηρεάζουν συνήθως την ενεργοποίηση ενός ρόλου ή την εκτέλεση ενός κανόνα. Ο καθορισμός της πληροφορίας πλαισίου που σχετίζεται με μία συγκεκριμένη απόφαση για εξουσιοδότηση και ο τρόπος με τον οποίο η αντίστοιχη πληροφορία μπορεί να εξαχθεί και να καθοριστεί στα σχετικά μοντέλα αποτελούν βασικές πτυχές του ελέγχου πρόσβασης. Η σημασία του πλαισίου στον τομέα αυτόν είναι προφανής, καθώς έχουν προταθεί πολλές επεκτάσεις σε καθιερωμένα μοντέλα, προκειμένου αυτά να το περιλαμβάνουν, όπως το εκτεταμένο προφίλ RBAC της XACML (Extended RBAC Profile of XACML) [86].

Μία εξέχουσα προσέγγιση στην περιοχή αυτή αποτελεί το Μοντέλο Ελέγχου Πρόσβασης Βάσει Χρονικής Σημασιολογίας (Temporal Semantic Based Access Control — TSBAC) [87], το οποίο εμπλουτίζει την προδιαγραφή κανόνων εξουσιοδότησης από τους χρήστες θέτοντας περιορισμούς που αφορούν χρονικά διαστήματα και χρονικές εκφράσεις στη βάση του ιστορικού πρόσβασης των χρηστών, το οποίο διατηρείται σε μία Βάση Ιστορικού (History Base). Πράγματι, η έννοια του ιστορικού των ενεργειών πρόσβασης αποτελεί μία παράμετρο μεγάλης σημασίας, π.χ., για τις περιπτώσεις κατά τις οποίες η γνωστοποίηση ορισμέ-

νων δεδομένων θα πρέπει να αποκλείει τη μελλοντική πρόσβαση στα ίδια ή άλλα δεδομένα. Αυτό το μοντέλο χρησιμοποιεί την έννοια του λογικού χρόνου, και όχι του πραγματικού, στην προδιαγραφή των κανόνων, ενώ επιπλέον προσδιορίζει μία τυπική σημασιολογία για χρονικές εξουσιοδοτήσεις. Καθώς το μοντέλο TSBAC αποτελεί επέκταση του Μοντέλου Ελέγχου Πρόσβασης Βάσει Σημασιολογίας (Semantic Based Access Control — SBAC) [88][89], βασίζεται επίσης στη χρήση οντολογιών OWL για τη μοντελοποίηση των οντοτήτων ελέγχου πρόσβασης και των σημασιολογικών μεταξύ τους σχέσεων. Με αυτόν τον τρόπο, ορίζονται οι αντίστοιχες οντολογίες: *Οντολογία Υποκειμένων*, *Οντολογία Αντικειμένων* και *Οντολογία Ενεργειών*. Τη σημαντικότερη συμβολή του μοντέλου SBAC συνιστά η αποτελεσματική διάδοση των πολιτικών, με βάση τη σχέση υπαγωγής, μέσω διαφορετικών σημασιολογικών συσχετισμών στα τρία επίπεδα μίας οντολογίας, δηλαδή στο *Επίπεδο Εννοιών* (*concept-level*), το *Επίπεδο Ιδιοτήτων* (*property-level*) και το *Επίπεδο Στιγμιοτύπων* (*individual-level*), ενώ η διάδοση σημασιολογικών εξουσιοδοτήσεων λαμβάνει χώρα είτε σε κάποιο μεμονωμένο επίπεδο, είτε μεταξύ διαφόρων επιπέδων. Το μοντέλο που προτείνεται στο [90], και αναφέρεται ως GTHBAC, αποτελεί επέκταση του μοντέλου TSBAC και χρησιμοποιεί επιπλέον την έννοια του πραγματικού χρόνου. Περιορισμοί που αφορούν το ιστορικό ολοκληρώνονται με ένα γενικό μοντέλο ελέγχου πρόσβασης, αυξάνοντας έτσι την εκφραστικότητα των κανόνων εξουσιοδότησης, ενώ επιτρέπει τη λήψη αποφάσεων βάσει ιστορικού, με αποτέλεσμα να είναι δυνατόν να εφαρμοστεί σε μία ευρεία ποικιλία μοντέλων ελέγχου πρόσβασης.

Μεταξύ των προσεγγίσεων που συνιστούν την οικογένεια των σημασιολογικών μοντέλων με επίγνωση πλαισίου, το μοντέλο OrBAC [32][33][34] αποτελεί μάλλον την πιο ώριμη, καθώς είναι η πρώτη προσέγγιση η οποία εκφράζει όλους τους διαφορετικούς τύπους πλαισίου εντός ενός μοναδικού ενιαίου συστήματος. Ειδικότερα, το OrBAC ορίζει μία *Οντολογία Πλαισίου* (*Context Ontology*), η οποία περιλαμβάνει επιπλέον, πέρα από το χωρικό, το χρονικό και το ιστορικό, πλαίσιο *δηλωμένο από το χρήστη* (*user-declared*) και πλαίσιο *εξαρτώμενο από την εφαρμογή* (*application dependent*). Το τελευταίο εξαρτάται από τα χαρακτηριστικά που συνδέουν το υποκείμενο, την ενέργεια και το αντικείμενο και είναι δυνατόν να αποτιμηθεί με σχετικό ερώτημα προς τη βάση δεδομένων του συστήματος, ενώ το δηλωμένο από το χρήστη πλαίσιο επιτρέπει τη μοντελοποίηση πληροφορίας πλαισίου που είναι δύσκολο να περιγραφεί χρησιμοποιώντας περιβαλλοντικές συνθήκες. Σημειώνεται ότι ακόμα και απαραίτητα χαρακτηριστικά για προστασία της ιδιωτικότητας είναι δυνατόν να μοντελοποιηθούν με χρήση πληροφοριών πλαισίου, όπως προτείνεται στο [39], όπου η έννοια του σκοπού μοντελοποιείται ως ένα δηλωμένο πλαίσιο. Ξεκινώντας από αυτά τα στοιχειώδη πλαίσια, το OrBAC επιτρέπει τον προσδιορισμό σύνθετων πλαισίων, μέσω των σχέσεων σύζευξης, διάζευξης και άρνησης. Από την άλλη πλευρά, και όπως έχει ήδη αναφερθεί στην Ενότητα 2.1.5, η ιδιαιτερότητα της οντολογίας OrBAC συνίσταται στο ότι οι κλασικές πλειάδες ⟨υποκείμενο, ενέργεια, αντικείμενο⟩ (⟨subject, action, object⟩) ανάγονται στο επίπεδο αφαίρεσης του οργανισμού, σε πλειάδες τύπου ⟨ρόλος, δραστηριότητα, όψη⟩ (⟨role, activity, view⟩), με τις σχετικές οντότητες να σχηματίζουν αντίστοιχες ιεραρ-

χίες. Οι OrBAC οντολογίες έχουν χρησιμοποιηθεί επίσης για την περιγραφή συναγερμών (alerts) και την προδιαγραφή πολιτικών, με χρήση κανόνων εξαγωγής συμπερασμάτων για την αντιστοίχιση συγκεκριμένων (concrete) συναγερμών (εκφρασμένων με τη βοήθεια του προτύπου Intrusion Detection Message Exchange Format (IDMEF) [91]) σε πλαίσια OrBAC, τα οποία αντικατοπτρίζουν τα απαραίτητα για την αντιμετώπιση του προβλήματος μέτρα, όταν ένας συναγερμός ανιχνεύεται από το σύστημα παρακολούθησης [92].

Τέλος, το μοντέλο PRISM που παρουσιάστηκε στην Ενότητα 2.2.5 χρησιμοποιεί μία ενοποιημένη οντολογία για την περιγραφή όλων των σχετικών με τον έλεγχο πρόσβασης εννοιών, συμπεριλαμβανομένων των τύπων δεδομένων, των ρόλων, των σκοπών, αμοιβαίως αποκλειόμενων συνδυασμών δεδομένων, περιορισμών πλαισίου, κλπ. Σε ό,τι αφορά την υλοποίηση των περιορισμών πλαισίου, κάθε κανόνας συσχετίζεται με ένα ή περισσότερα στιγμιότυπα της κλάσης `Conditions`, καθένα από τα οποία αντιστοιχεί στον ορισμό ενός σχετικού περιορισμού. Μέσω υποκλάσεων της κλάσης `ContextualBase`, η προσέγγιση επιτρέπει τον ορισμό πληθώρας διαφορετικών τύπων πληροφορίας πλαισίου, που αναφέρονται, π.χ., στο χώρο, το χρόνο και σε γεγονότα που έχουν λάβει χώρα. Σε ό,τι αφορά τα γεγονότα, αξίζει να σημειωθεί η ενσωμάτωση μίας πρωτότυπης οντολογικής υλοποίησης του προτύπου IDMEF, όπως τεκμηριώνεται στο [93], ενώ άλλοι τύποι πληροφορίας πλαισίου που θεωρήθηκαν από το PRISM είναι η παλαιότητα των υπό επεξεργασία δεδομένων [94][95].

### 2.3.4 Οντολογικός Προσδιορισμός Προτιμήσεων Ιδιωτικότητας

Αρκετές προσεγγίσεις ελέγχου πρόσβασης συμπεριλαμβάνουν στη διαδικασία λήψης αποφάσεων και τους κανόνες που ορίζονται από τους χρήστες, οι οποίοι εκφράζουν κατ' αυτόν τον τρόπο τις δικές τους προτιμήσεις πρόσβασης και χρήσης. Η τάση αυτή συναντάται ιδιαίτερα στον έλεγχο πρόσβασης για προστασία της ιδιωτικότητας [44], όπου γλώσσες βασισμένες στην XML, όπως οι P3P [96] και APPEL [97], χρησιμοποιούνται για την τυπική αναπαράσταση των προτιμήσεων ιδιωτικότητας.

Προκειμένου να ενισχύσουν την εκφραστική δύναμη αυτών των γλωσσών και να εφαρμόσουν τη σημασιολογία των προθέσεων ενός ατόμου σχετικά με την προστασία των δεδομένων, οι ερευνητές κάνουν χρήση οντολογιών. Στο πλαίσιο αυτό, ένα μοντέλο για αναπαράσταση και διαχείριση των προτιμήσεων ιδιωτικότητας, στο οποίο οι κανόνες προτιμήσεων εκφράζονται στη γλώσσα OWL, περιγράφεται στο [98]. Το μοντέλο αυτό περιλαμβάνει τυπικές περιγραφές για το πώς ορίζονται τα αιτήματα και οι κανόνες προτιμήσεων, ποιες είναι οι ιδιότητες ενός συνεπούς συνόλου κανόνων που πρέπει να πληρούνται, πώς αντιστοιχίζονται τα αιτήματα στις προτιμήσεις, και πώς εξασφαλίζεται η συνέπεια του συνόλου των κανόνων.

Στο [99], οι Sacco et al. παρουσιάζουν την Οντολογία Προτιμήσεων Ιδιωτικότητας (Privacy Preference Ontology — PPO) και το Διαχειριστή Προτιμήσεων Ιδιωτικότητας (Pri-

vacy Preference Manager — PPM) που επιτρέπουν λεπτομερή έλεγχο πρόσβασης για τον Ιστό Δεδομένων. Η PPO προσφέρει το λεξιλόγιο για τον προσδιορισμό λεπτομερών προτιμήσεων ιδιωτικότητας για δομημένα δεδομένα, σε συνδυασμό με την Οντολογία Ελέγχου Πρόσβασης Ιστού (WAC[8]), ενώ ο PPM επιτρέπει στους χρήστες να δημιουργήσουν προτιμήσεις ιδιωτικότητας βάσει της PPO και περιορίζει την πρόσβαση στα δεδομένα τους από τρίτους χρήστες. Η `PrivacyPreference` αποτελεί την κύρια κλάση της PPO και διάφοροι τύποι ιδιοτήτων επιτρέπουν να προσδιοριστούν περιορισμοί πρόσβασης σε προτάσεις (statements), πόρους και ονομαστικούς γράφους (named graphs), συνθήκες για να προσδιοριστούν ποιες είναι οι συγκεκριμένες προτάσεις, οι πόροι και οι ονομαστικοί γράφοι που πρέπει να περιοριστούν, ποια δικαιώματα πρόσβασης θα πρέπει να χορηγηθούν, καθώς και τα πρότυπα ιδιοτήτων που θα πρέπει να ικανοποιούνται από τους αιτούντες. Ειδικά για τις προδιαγραφές των προτύπων ιδιοτήτων, γίνεται χρήση SPARQL `ASK` ερωτημάτων.

Στο ίδιο πλαίσιο, στο [100] προτείνεται ότι το σημασιολογικό τυπικό μοντέλο για την P3P μπορεί να εφαρμοστεί και να εκφραστεί ως μία ποικιλία οντολογιών και συνδυασμών κανόνων, είτε σε μία *ομοιογενή ολοκλήρωση*, όπου όλοι οι σημαντικοί όροι προσδιορίζονται σε οντολογίες και γίνεται χρήση κανόνων για να αντιμετωπιστούν οι εκφραστικοί περιορισμοί των οντολογιών, ή σε μία *υβριδική ολοκλήρωση*, όπου ορισμένοι από τους όρους των πολιτικών προστασίας της ιδιωτικότητας δε θα ορίζονται ρητά στις οντολογίες, αλλά θα πρέπει να δηλώνονται ως κατηγορήματα σε κάθε κανόνα. Προτείνονται τρεις τύποι οντολογιών, συγκεκριμένα η *οντολογία χρηστών δεδομένων* για κατηγοριοποίηση των τύπων χρηστών, η *οντολογία τύπων δεδομένων* που περιγράφει προσωπικά προφίλ και ψηφιακά ίχνη και τέλος, η *οντολογία σκοπών* για την περιγραφή των σκοπών για τους οποίους οι χρήστες δεδομένων χρησιμοποιούν κάποιο συγκεκριμένο τύπο δεδομένων.

Μία άλλη προσέγγιση σε P3P παρουσιάζεται από τους συγγραφείς στο [101], η οποία στηρίζεται στην οντολογική αναπαράσταση ενός σχήματος δεδομένων το οποίο βασίζεται στο πρότυπο P3P. Η εσωτερική δομή σύνθετων διαπιστευτηρίων παρουσιάζεται με όρους πιο λεπτομερών στοιχείων, ενώ η P3P οντολογία εφαρμόζεται προκειμένου να επεκταθούν με αυτόματο τρόπο οι διαθέσιμες XACML πολιτικές, ώστε να συμπεριλάβουν σημασιολογικά ισοδύναμες συμπληρωματικές συνθήκες (conditions) με βάση την περιγραφή των μεταδεδομένων των χρηστών και των πόρων. Οι διευρυμένες πολιτικές ελέγχου πρόσβασης μπορούν να αντικαταστήσουν τις αρχικές, ενσωματώνοντας αυτόματα γνώση από την οντολογία.

### 2.3.5 Σημασιολογικός Έλεγχος Πρόσβασης σε Υπηρεσίες Κοινωνικής Δικτύωσης

Οι Υπηρεσίες Κοινωνικής Δικτύωσης αποτελούν πλέον έναν από τους σημαντικότερους τύπους online εφαρμογών που επιτρέπουν την ανταλλαγή πληροφοριών μεταξύ

[8]Web Access Control (WAC), homepage: http://www.w3.org/ns/auth/acl

μεγάλου αριθμού χρηστών, ωστόσο, την ίδια στιγμή, δημιουργούν νέους κινδύνους που σχετίζονται με την ασφάλεια και την προστασία της ιδιωτικότητας. Οι περίπλοκες σχέσεις που θεωρούνται σε τέτοιες εφαρμογές υπογραμμίζουν την ανάγκη για σημασιολογική οργάνωση της γνώσης και για μηχανισμούς σημασιολογικού ελέγχου πρόσβασης.

Στο πλαίσιο αυτό, οι Giunchiglia et al. [102] προτείνουν ένα μοντέλο ελέγχου πρόσβασης βάσει σχέσεων (Relation Based Access Control — RelBAC), το οποίο προσφέρει ένα τυπικό μοντέλο αδειών με βάση τις σχέσεις ανάμεσα στις κοινότητες και τους πόρους. Το μοντέλο RelBAC είναι δυνατόν να χρησιμοποιηθεί για τη μοντελοποίηση του ελέγχου πρόσβασης καθώς περιλαμβάνει οντολογίες χρηστών, αντικειμένων και αδειών, επιτρέποντας έτσι την αυτόματη διαχείριση των αδειών. Ομοίως, η προσέγγιση που παρουσιάζεται στο [103] εκμεταλλεύεται τις σχέσεις με τα άτομα και την κοινότητα, προκειμένου να καθοριστούν οι περιορισμοί πρόσβασης στους πόρους της κοινότητας. Όλη αυτή η γνώση αναπαριστάται σε μία οντολογία με χρήση OWL DL, ενώ οι σημασιολογικοί κανόνες προστίθενται στην οντολογία παρέχοντάς της επαρκή εκφραστικότητα και αποκρισιμότητα ώστε να συναχθούν οι έμμεσες σχέσεις.

Οι Carminati et al. προσφέρουν στο [104] μία πολύ πλουσιότερη OWL οντολογία για τη μοντελοποίηση διαφόρων πτυχών των online κοινωνικών δικτύων, ενώ προτείνουν επίσης *εξουσιοδότηση*, *διαχείριση* και *φιλτράρισμα* πολιτικών που εξαρτώνται από τις σχέσεις εμπιστοσύνης μεταξύ των διαφόρων χρηστών και μοντελοποιούνται με χρήση OWL και SWRL. Ειδικότερα, οι συγγραφείς προτείνουν τη μοντελοποίηση με χρήση οντολογιών Σημασιολογικού Ιστού των ακόλουθων πέντε πτυχών των online κοινωνικών δικτύων: προσωπική πληροφορία, σχέσεις μεταξύ των χρηστών, πόροι, σχέσεις μεταξύ χρηστών και πόρων, και ενέργειες.

Μία πιο λεπτομερής προσέγγιση παρουσιάζεται στο [105], η οποία προτείνει το μοντέλο Ελέγχου Πρόσβασης Κοινωνικών Δικτύων βάσει Οντολογιών (Ontology-based Social Network Access Control — OSNAC). Το μοντέλο αυτό περιλαμβάνει δύο οντολογίες˙ την Οντολογία συστημάτων Κοινωνικής Δικτύωσης (Social Networking systems Ontology — SNO), η οποία αντανακλά τη σημασιολογία των πληροφοριών που σχετίζονται με ένα κοινωνικό δίκτυο, και την Οντολογία Ελέγχου Πρόσβασης (Access Control Ontology — ACO), η οποία επιτρέπει τον προσδιορισμό SWRL κανόνων ελέγχου πρόσβασης με βάση τις σχέσεις μεταξύ των εννοιών της SNO. Τέλος, το μοντέλο αυτό παρέχει δυνατότητα για μετάθεση (delegation) εξουσιοδοτήσεων και επιτρέπει τόσο στους χρήστες όσο και στο σύστημα να εκφράζουν λεπτομερείς πολιτικές ελέγχου πρόσβασης.

### 2.3.6 Παρατηρήσεις

Στις προηγούμενες ενότητες παρουσιάστηκαν κάποια από τα πιο αντιπροσωπευτικά σύγχρονα σημασιολογικά μοντέλα ελέγχου πρόσβασης. Στοχεύοντας στην περιγραφή της κληρονομικότητας εξουσιοδοτήσεων και ιδιοτήτων, καθώς και σε προηγμένες δυνατό-

τητες συλλογιστικής, ένα κοινό χαρακτηριστικό αυτών των μοντέλων είναι ότι χρησιμοποιούν οντολογίες προκειμένου να δημιουργήσουν ιεραρχίες των εξεταζόμενων εννοιών. Η υποστήριξη ιεραρχιών μπορεί να ποικίλει, από την απλή ιεραρχία ρόλων (όπως, π.χ., στο [76]), σε ιεραρχίες επιπλέον εννοιών που συνδέονται με την άδεια πρόσβασης, όπως σκοπούς ή λειτουργίες (π.χ., τα μοντέλα PRISM [60] και OrBAC [32]).

Επιπλέον, εκτός από τα κύρια χαρακτηριστικά που υποστηρίζουν, τα μοντέλα αυτά μπορούν να αξιολογηθούν περαιτέρω με βάση μία σειρά από βασικές πτυχές του ελέγχου πρόσβασης. Ο Πίνακας 1 παρέχει μία επισκόπηση των χαρακτηριστικών που το κάθε μοντέλο υποστηρίζει, είτε άμεσα είτε μερικώς.

Βασικό κριτήριο ώστε να ενταχθεί ένα μοντέλο ελέγχου πρόσβασης στην κατηγορία των μοντέλων εκείνων που στοχεύουν στην προστασία της ιδιωτικότητας αποτελεί το εάν αυτό λαμβάνει υπόψη κατά τη διαδικασία λήψης απόφασης το σκοπό για τον οποίο ζητείται πρόσβαση σε πόρους˙ για παράδειγμα, το [98] βασίζει ρητά τις εξουσιοδοτήσεις στην έννοια του σκοπού. Άλλες προσεγγίσεις, όπως αυτή που παρουσιάζεται στο [105], επιτρέπουν τον προσδιορισμό πολιτικών χρήσης από τους ιδιοκτήτες των πόρων προς τους οποίους ζητείται πρόσβαση, ενώ άλλα μοντέλα, π.χ. το [85], εντάσσονται σε αυτήν την κατηγορία λόγω του ότι στοχεύουν στην ελαχιστοποίηση των δεδομένων που γνωστοποιούνται, ικανοποιώντας κατ' αυτόν τον τρόπο τις αρχές της *αναγκαιότητας*, της *καταλληλότητας* και της *αναλογικότητας*.

Πίνακας 1: Συγκριτική επισκόπηση των σημασιολογικών μοντέλων ελέγχου πρόσβασης. Τα σύμβολα "✓", "✳", "✗" υποδεικνύουν αντίστοιχα άμεση, μερική/έμμεση και μη υποστήριξη του υπό εξέταση χαρακτηριστικού.

| **Semantic Models** | **Privacy-aware** | **Context-aware** | **Attribute-based** | **Semantic rules** | **SoD** | **XACML support** |
|---|---|---|---|---|---|---|
| *ROWL*BAC [76] | ✗ | ✳ | ✳ | ✓ | ✓ | ✗ |
| XACML+OWL [77] | ✗ | ✳ | ✓ | ✗ | ✓ | ✓ |
| He et al. [78] | ✗ | ✳ | ✓ | ✓ | ✓ | ✗ |
| Cruz et al. [81] | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Priebe et al. [83] | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ |
| Ching Hsu [84] | ✗ | ✳ | ✓ | ✗ | ✗ | ✓ |
| Rota et al. [85] | ✓ | ✳ | ✓ | ✗ | ✗ | ✓ |
| GTHBAC [87][88][89][90] | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ |
| OrBAC [32][33][34][39][92] | ✳ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Bodorik et al. [98] | ✓ | ✳ | ✗ | ✓ | ✗ | ✗ |
| Hu et al. [100] | ✓ | ✳ | ✳ | ✓ | ✗ | ✗ |
| Ardagna et al. [101] | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ |
| Elahi et al. [103] | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ |
| Carminati et al. [104] | ✓ | ✗ | ✳ | ✓ | ✗ | ✗ |
| OSNAC [105] | ✓ | ✗ | ✳ | ✓ | ✗ | ✗ |
| PRISM [60] | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |

Η πλειονότητα των μοντέλων που εξετάστηκαν χρησιμοποιεί τεχνολογίες Σημασιολογικού Ιστού για τον προσδιορισμό κανόνων ελέγχου πρόσβασης. Έτσι, τα περισσό-

τερα από τα μοντέλα αυτά κάνουν χρήση της γλώσσας SWRL για να εκφράσουν κανόνες πάνω από οντολογίες που αντανακλούν το εκάστοτε πεδίο εφαρμογής, ενώ κάποιες προσεγγίσεις, όπως οι [81] και [60], ολοκληρώνουν πλήρως τον έλεγχο πρόσβασης με οντολογίες, μέσω ξεχωριστών οντολογιών ελέγχου πρόσβασης, και αξιολογούν τα αιτήματα πρόσβασης μέσω συλλογιστικής στη βάση των εν λόγω οντολογιών. Η μη υποστήριξη σημασιολογικών κανόνων υπονοεί ότι το υπό εξέταση μοντέλο κάνει χρήση προτύπων βασισμένων σε XML, όπως είναι η γλώσσα πολιτικών XACML, για τον προσδιορισμό των αντίστοιχων εξουσιοδοτήσεων, χρησιμοποιώντας όμως παράλληλα τεχνολογίες Σημασιολογικού Ιστού για τη σημασιολογική τους επέκταση. Μάλιστα, η υποστήριξη καθεαυτή του προτύπου XACML αποτελεί σημαντικό χαρακτηριστικό, καθώς με αυτόν τον τρόπο ένα μοντέλο ελέγχου πρόσβασης μπορεί να χρησιμοποιηθεί από τα συστήματα που χρησιμοποιούν ήδη το πρότυπο XACML, ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για τον καθορισμό των κανόνων ελέγχου πρόσβασης.

Επιπλέον κάποια μοντέλα παρέχουν τα μέσα για τον προσδιορισμό περιορισμών SoD. Τα περισσότερα από αυτά υποστηρίζουν τόσο στατικούς όσο και δυναμικούς SoD περιορισμούς που αφορούν τους δράστες των ενεργειών πρόσβασης, ενώ το μοντέλο που περιγράφεται στο [92] επιτρέπει τον προσδιορισμό SoD και BoD περιορισμών όχι μόνο για το δράστη αλλά και για κάθε οντότητα που σχετίζεται με την ενέργεια πρόσβασης.

Τέλος, επειδή το *πλαίσιο* και οι *ιδιότητες* δεν αντιμετωπίζονται πάντα ως ανεξάρτητα σύνολα, στην παρούσα μελέτη οι ιδιότητες αναφέρονται σε παραμέτρους που χαρακτηρίζουν περαιτέρω τις οντότητες της ενέργειας πρόσβασης, ενώ οι πληροφορίες πλαισίου αναφέρονται σε όλες τις εξωτερικές παραμέτρους. Ο σκοπός για τον οποίο χρησιμοποιούνται οι δύο αυτές έννοιες στον έλεγχο πρόσβασης είναι παρόμοιος, καθώς αμφότερες εξυπηρετούν την ανάγκη για τον εμπλουτισμό των κανόνων ελέγχου πρόσβασης με παραμέτρους που είτε είναι δυναμικές και εξωτερικές είτε περιγράφουν παραλλαγές παρεμφερών εννοιών. Το πλαίσιο και οι ιδιότητες επιτρέπουν την περιγραφή εκφραστικών πολιτικών, αλλά ταυτόχρονα απαιτούν υψηλή εκφραστικότητα από τα υποκείμενα μοντέλα. Εν προκειμένω, διάφορες προσεγγίσεις έχουν χρησιμοποιήσει τεχνολογίες του Σημασιολογικού Ιστού για την περιγραφή των περιορισμών σχετικών με το πλαίσιο και τις ιδιότητες, όπως επίσης υπονοείται από τη δημοφιλία αυτών των χαρακτηριστικών στον Πίνακα 1.

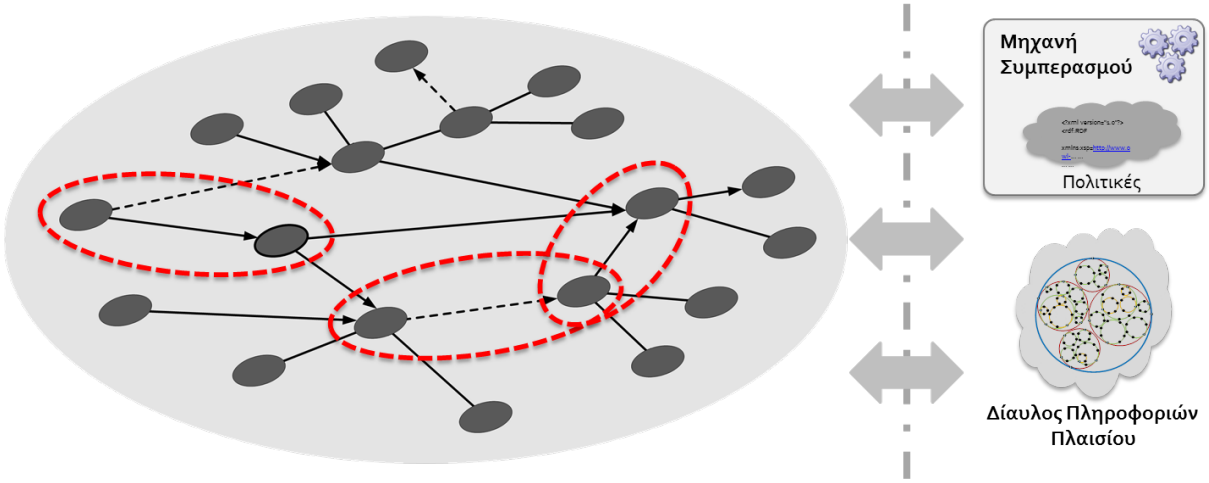
# Κεφάλαιο 3

# Γενικές Αρχές της Προτεινόμενης Λύσης

Το παρόν κεφάλαιο περιγράφει τις γενικές αρχές της προτεινόμενης λύσης, παρέχοντας μία γενική επισκόπηση και παραθέτοντας κάποιες βασικές έννοιες. Στο πλαίσιο αυτό, τεκμηριώνεται το μοντέλο συστήματος και εισάγεται η έννοια του *διμερούς συσχετισμού*, που αναφέρεται στη στοιχειώδη αλληλεπίδραση μεταξύ δύο οντοτήτων, και των εννοιών που τον αποτελούν, δηλαδή των εργασιών που εκτελούν οι οντότητες και της μεταξύ τους ροής. Στη συνέχεια, καταγράφονται οι θεμελιώδεις αρχές που πρέπει να διέπουν ένα μοντέλο ελέγχου πρόσβασης σε κατανεμημένα περιβάλλοντα, βάσει των αρχών και απαιτήσεων για προστασία της ασφάλειας και της ιδιωτικότητας, αλλά και των διακριβωμένων ελλείψεων και αναγκών των υφιστάμενων τεχνολογιών. Οι αρχές αυτές αποτελούν ουσιαστικά τις απαιτήσεις που πρέπει να ικανοποιεί η προτεινόμενη λύση, από τις οποίες πηγάζουν και οι απαιτήσεις για εξαγωγή γνώσης από το μοντέλο ελέγχου πρόσβασης, οι οποίες ακολούθως επισκοπούνται. Τέλος, συνοψίζεται το μοντέλο ελέγχου πρόσβασης σε υψηλό επίπεδο αφαίρεσης.

## 3.1 Μοντέλο Συστήματος

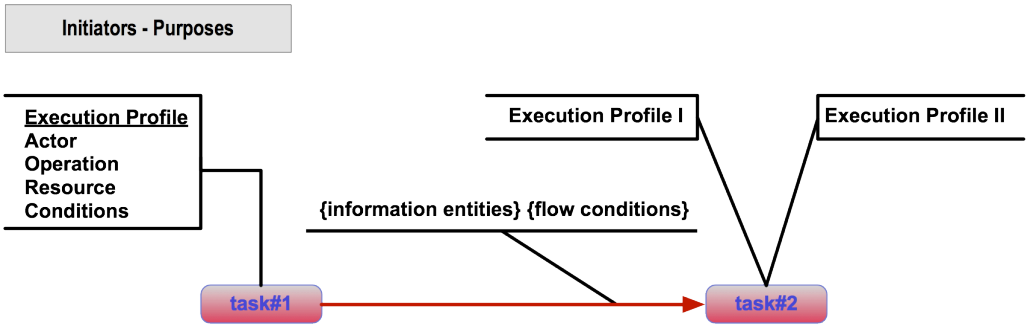
Ένα κατανεμημένο σύστημα συνίσταται σε ένα σύνολο κατανεμημένων οντοτήτων που αλληλεπιδρούν, με την κάθε τέτοια οντότητα να είναι σε θέση να εκτελεί ένα σύνολο *εργασιών*. Οι οντότητες αυτές αντιστοιχούν στους κόμβους του Σχήματος 4 και αναφέρονται ως *πράκτορες* (*agents*), οι οποίοι αντιπροσωπεύουν το εκάστοτε υποκείμενο υποσύστημα. Έτσι, μία εργασία που εκτελεί εσωτερικά το εκάστοτε σύστημα της κατανεμημένης υποδομής είναι δυνατόν να προσφέρεται ως αυτόνομη λειτουργικότητα από τον αντίστοιχο πράκτορα. Οι πράκτορες αλληλεπιδρούν τόσο σε επίπεδο ανταλλαγής δεδομένων όσο και σε επίπεδο ανταλλαγής πληροφοριών ελέγχου.




Σχήμα 4: Μοντέλο Συστήματος

Η αλληλεπίδραση μεταξύ δύο συστημάτων αναφέρεται ως *Διμερής Συσχετισμός* και αντιστοιχεί σε ένα ζεύγος αλληλεπιδρουσών εργασιών συμπεριλαμβανομένης της αλληλεπίδρασης καθεαυτής, δηλαδή της ακμής που συνδέει τις κατανεμημένες εργασίες. Ο διμερής συσχετισμός αποτελεί το στοιχειώδες δομικό στοιχείο αλληλεπίδρασης και συνιστά ένα κατανεμημένο σύστημα, ενώ μία γενίκευσή του συνιστούν οι *ροές εργασιών*. Θεωρούμε ότι κάθε αλληλεπίδραση έχει έναν ή περισσότερους *εκκινητές* και εξυπηρετεί ένα σύνολο *σκοπών*. Έτσι, στο Σχήμα 4 απεικονίζεται ένα σύνολο αλληλεπιδράσεων, οι οποίες είτε πραγματοποιούνται ανεξάρτητα μεταξύ τους είτε στο πλαίσιο μίας ροής εργασιών, για ένα σύνολο σκοπών και εκκινητών. Επίσης, καθώς μία αλληλεπίδραση είναι πιθανό να λαμβάνει χώρα μόνο κάτω από συγκεκριμένες συνθήκες, θεωρείται ένας μηχανισμός, ο *Δίαυλος Πληροφοριών Πλαισίου*, ο οποίος επιτρέπει στους πράκτορες (υποσυστήματα) να καθίστανται κοινωνοί *πληροφοριών πλαισίου*, ώστε να είναι σε θέση να αποτιμήσουν τις υπό συνθήκη αλληλεπιδράσεις.

Το προτεινόμενο μοντέλο περιλαμβάνει όλες τις απαραίτητες έννοιες και συσχετίσεις για την πραγματοποίηση αποτελεσματικού ελέγχου πρόσβασης και χρήσης όχι μόνο στο επίπεδο μεμονωμένων ενεργειών, αλλά και στο επίπεδο των αλληλεπιδρουσών εργασιών, λαμβάνοντας δηλαδή υπόψη τόσο τη ροή λειτουργίας όσο και τη ροή δεδομένων, με αποτέλεσμα μία ολιστική θεώρηση του ελέγχου πρόσβασης. Οι σχετικές αποφάσεις βάσει των προδιαγεγραμμένων πολιτικών λαμβάνονται από μία *Μηχανή Συμπερασμού*, η οποία αποτελεί το *Σημείο Απόφασης Πολιτικής* (*Policy Decision Point — PDP*) του συστήματος, με τους πράκτορες να αποτελούν τα *Σημεία Εφαρμογής Πολιτικής* (*Policy Enforcement Points — PEPs*) [106].




Σχήμα 5: Διμερής Συσχετισμός

## 3.2 Διμερής Συσχετισμός

Τα θεμελιώδη στοιχεία που απαρτίζουν ένα διμερή συσχετισμό είναι οι *εργασίες* και η μεταξύ τους *ροή*. Οι πρώτες αντιπροσωπεύουν τις ενέργειες που πρόκειται να εκτελεστούν στα πλαίσια της αλληλεπίδρασης μεταξύ δύο συστημάτων, ενώ η ροή εκφράζει εξαρτήσεις και ανταλλαγή πληροφοριών μεταξύ των εν λόγω εργασιών. Επιπλέον, ένας διμερής συσχετισμός συμπληρώνεται από τους επιχειρησιακούς *σκοπούς* που προορίζεται να εξυπηρετήσει και τους εν δυνάμει *εκκινητές*, τις οντότητες, δηλαδή, που δύνανται να εκκινήσουν την εκτέλεση του.

Για τη μοντελοποίηση του διμερούς συσχετισμού υιοθετήθηκε το *σημασιολογικό μοντέλο προδιαγραφής ροών εργασιών* που περιγράφεται στο [107]. Πέρα από την παρατήρηση ότι ένας διμερής συσχετισμός είναι δυνατόν να παραλληλισθεί με μία στοιχειώδη ροή εργασιών, η οποία περιλαμβάνει δύο εργασίες και τη μεταξύ τους αλληλεπίδραση, η επιλογή αυτή έγινε με το κριτήριο ότι η εν λόγω προσέγγιση δύναται να αξιοποιήσει στο έπακρο και να αναδείξει τις δυνατότητες και τα χαρακτηριστικά του προτεινόμενου μοντέλου ελέγχου πρόσβασης και χρήσης, καθώς, σε αντίθεση με άλλες προσεγγίσεις, η εκφραστικότητα που αυτή παρέχει επιτρέπει να αποτυπωθούν στις εμπλεκόμενες οντότητες ενός διμερούς συσχετισμού όλες οι επιταγές ασφάλειας και ιδιωτικότητας που υπαγορεύει ο έλεγχος πρόσβασης.

Στο Σχήμα 5 παρουσιάζεται ο τρόπος προδιαγραφής ενός διμερούς συσχετισμού σύμφωνα με την προαναφερθείσα προσέγγιση, ενώ οι οντότητες που τον απαρτίζουν περιγράφονται αναλυτικά στις ενότητες που ακολουθούν.

### 3.2.1 Εργασίες

Μία *εργασία* (*task*) αντιστοιχεί σε μία αυτοτελή μονάδα έργου και περιγράφει μία *λειτουργία* (*operation*) που εκτελείται από ένα σύνολο *δραστών* (*actors*) πάνω σε ένα σύνολο *πόρων* (*resources*), ενώ μπορεί να συμπληρώνεται και από τον ορισμό παραμέτρων. Αντίθετα με άλλες προσεγγίσεις στις οποίες ο ορισμός των εργασιών είναι μάλλον μονοδιά-

στατος, η προτεινόμενη προσέγγιση, σε συμφωνία με το μοντέλο προδιαγραφής ροών εργασιών [107], εισάγει την έννοια του *προφίλ εκτέλεσης* (*execution profile*). Στην ουσία το προφίλ εκτέλεσης αντανακλά *δηλώσεις εξουσιοδοτήσεων* (*authorisation statements*) και επιτρέπει, μεταξύ άλλων, την προδιαγραφή παραλλαγών στον τρόπο εκτέλεσης των εργασιών. Αυτό αφορά ειδικότερα τους εξής δύο άξονες: αφενός τη διαφοροποιημένη εκτέλεση της εργασίας αναλόγως κάποιων *συνθηκών* (*conditions*) και, αφετέρου, την αποτύπωση εξαρτήσεων μεταξύ δραστών, πόρων και των παραμέτρων της λειτουργίας που αντανακλά η εκάστοτε εργασία, τον ακριβή, με άλλα λόγια, ορισμό έγκυρων συνδυασμών των παραπάνω στοιχείων. Στην περίπτωση του ορισμού πολλαπλών προφίλ, το ποιο μεταξύ αυτών θα εκτελεστεί τελικά καθορίζεται κατά το χρόνο εκτέλεσης και εξαρτάται από τις συνθήκες πραγματικού χρόνου κάτω από τις οποίες οι συγκεκριμένοι δράστες, οι πόροι και οι παράμετροι λειτουργίας μπορούν να συνδυαστούν για την εκτέλεση της τελευταίας, καθώς και από τη διαθεσιμότητα των εν λόγω οντοτήτων.

Εφόσον μία εργασία μπορεί να περιλαμβάνει πολλαπλούς δράστες, εναλλακτικούς ή συμπληρωματικούς μεταξύ τους, αλλά και περισσότερους του ενός πόρους (επίσης εναλλακτικούς ή συμπληρωματικούς), κάθε προφίλ εκτέλεσης συνδέεται με λογικές σχέσεις αντίστοιχων οντοτήτων. Οι εμπλεκόμενες οντότητες (δράστες, λειτουργία, πόροι) είτε ορίζονται σημασιολογικά, με βάση κάποια έννοια του Μοντέλου Πληροφοριών (βλ. Ενότητα 4.1), π.χ., μέσω κάποιου ρόλου, και πιθανώς με τη συνοδεία περιορισμών βασισμένων στις ιδιότητες της υποκείμενης έννοιας, είτε αναφέρονται σε κάποια συγκεκριμένη οντότητα (π.χ., υποδεικνύοντας ένα συγκεκριμένο άτομο μέσω του ονόματός του).

Ο ορισμός ενός προφίλ εκτέλεσης συμπληρώνεται από τις συνθήκες που θα πρέπει να ισχύουν προκειμένου να εκτελεστεί το προφίλ ως έχει. Οι συνθήκες αυτές συνίστανται σε περιορισμούς πραγματικού χρόνου που αφορούν παράγοντες που δεν αποτελούν μέρος της προδιαγραφής του συσχετισμού (π.χ., εξωγενείς παράμετροι περιβάλλοντος) ή που εκτείνονται πέραν των ορίων της εργασίας και που, συνεπώς, δεν μπορούν να εκφραστούν αποκλειστικά στη βάση των ιδιοτήτων των εμπλεκόμενων οντοτήτων. Οι συνθήκες σε μία εργασία διατυπώνονται, όπως και οι υπόλοιποι τύποι περιορισμών, με χρήση εκφράσεων, οι οποίες μπορεί να αναφέρονται σε διάφορα ετερογενή στοιχεία, όπως είναι τα δεδομένα εισόδου της εργασίας, οι παράμετροι πλαισίου, ή ο εκκινητής και ο υποκείμενος σκοπός.

### 3.2.2 Ροές

Οι ροές εκφράζουν εξαρτήσεις μεταξύ εργασιών, συμβολίζονται με κατευθυνόμενες ακμές και διακρίνονται σε δύο τύπους: *ελέγχου (control)* και *δεδομένων (data)*. Μια εξάρτηση ροής ελέγχου $t_A \xrightarrow{f_c} t_B$ μεταξύ δύο εργασιών $t_A$ και $t_B$ εκφράζει ότι η $t_B$ εκτελείται μόνο αφού η εκτέλεση της $t_A$ έχει ολοκληρωθεί˙ αυτό που "μεταφέρει" η ακμή σε αυτή την περίπτωση είναι το νήμα εκτέλεσης, πιθανώς συνοδευόμενο από απαραίτητες παραμέτρους ελέγχου. Αντίθετα, μία εξάρτηση ροής δεδομένων $t_A \xrightarrow{f_d} t_B$ υποδηλώνει ότι και οι

δύο εργασίες βρίσκονται συνεχώς υπό εκτέλεση, με την $t_B$, ωστόσο, να εξαρτάται από το ρεύμα δεδομένων που παράγεται από την $t_A$. Ουσιαστικά, η διάκριση μεταξύ τους προέρχεται από τα σημασιολογικά χαρακτηριστικά των λειτουργιών που επικοινωνούν αναφορικά με τον τρόπο που αυτές λαμβάνουν και καταναλώνουν πληροφορία. Οι δύο αυτοί τρόποι αλληλεπίδρασης αντανακλώνται από τις κατευθυνόμενες ακμές του Σχήματος 4, με τις συνεχόμενες ακμές να δηλώνουν ροή δεδομένων, ενώ οι διακεκομμένες ροή ελέγχου.

Οι ακμές ελέγχου και δεδομένων έχουν πανομοιότυπα χαρακτηριστικά: καθεμία συνδέει δύο εργασίες και υποδηλώνει την κατεύθυνση της ροής, την ανταλλασσόμενη πληροφορία, τις συνθήκες κάτω από τις οποίες η εν λόγω μετάβαση λαμβάνει χώρα, και λοιπές ιδιότητες της ροής. Σε ό,τι αφορά την ανταλλασσόμενη πληροφορία, αυτή μοντελοποιείται μέσω των *οντοτήτων πληροφοριών* (*information entities*), οι οποίες, όπως και στην περίπτωση των οντοτήτων του προφίλ εκτέλεσης, ορίζονται στη βάση κάποιας έννοιας του Μοντέλου Πληροφοριών (στη συγκεκριμένη περίπτωση, κάποιου τύπου δεδομένων) και προσδιορίζονται περαιτέρω με χρήση περιορισμών στις τιμές των σχετικών ιδιοτήτων των δεδομένων. Επιπλέον, οι οντότητες πληροφοριών περιλαμβάνουν πληροφορία σχετική με την *κατάσταση* (*state*) των μεταδιδόμενων δεδομένων, δηλαδή αν είναι π.χ., κρυπτογραφημένα.

Τέλος, ορίζονται *συνθήκες ροής* (*flow conditions*) μέσω κατάλληλων εκφράσεων, ανάλογες των συνθηκών που ορίζονται για τις εργασίες, οι οποίες πρέπει να ισχύουν προκειμένου να πραγματοποιηθεί η υποδηλούμενη μετάβαση μεταξύ των δύο εργασιών, υποστηρίζοντας έτσι όταν είναι αναγκαίο, την υπό συνθήκη διακλάδωση της ροής ελέγχου ή δεδομένων.

## 3.3 Βασικές Αρχές της Προτεινόμενης Λύσης

Κάθε παραβίαση ασφάλειας και ιδιωτικότητας περιλαμβάνει οπωσδήποτε αθέμιτη πρόσβαση σε πόρους, είτε αυτοί είναι συστήματα, δεδομένα ή λειτουργίες. Στο πλαίσιο αυτό, η εξέλιξη των πολιτικών ασφάλειας έχει καταστήσει τον ελέγχο πρόσβασης πυρήνα της ασφάλειας, αλλά και της προστασίας της ιδιωτικότητας. Οι βασικές αρχές που θα πρέπει να διέπουν ένα μοντέλο ελέγχου πρόσβασης και χρήσης γενικού σκοπού απορρέουν τόσο από τις απαιτήσεις που υπαγορεύει η νομοθεσία για την προστασία των προσωπικών δεδομένων, όσο και από τις απαιτήσεις ασφάλειας και ιδιωτικότητας που δημιουργεί το ίδιο το πλαίσιο λειτουργίας του κατανεμημένου περιβάλλοντος και της αλληλεπίδρασης μεταξύ ετερογενών συστημάτων.

Στην Ενότητα 1.2 συνοψίστηκαν οι απαιτήσεις ιδιωτικότητας που θέτουν η νομοθεσία και τα συναφή έγγραφα (γνωμοδοτήσεις, αποφάσεις, κλπ.). Αυτές αφορούν κυρίως τη νομιμότητα της συλλογής και της επεξεργασίας των δεδομένων, τον προσδιορισμό των σκοπών και τη μη απόκλιση από αυτούς, την αναγκαιότητα, την επάρκεια, την αναλογικότητα και την ποιότητα των δεδομένων τα οποία υπόκεινται σε επεξεργασία, την ελάχιστη

χρήση προσωπικών δεδομένων, την εφαρμογή μέτρων ασφάλειας, την εφαρμογή των δικαιωμάτων των υποκειμένων των δεδομένων, το συντονισμό με τις αρμόδιες αρχές, κλπ.. Η ανάλυση των αρχών και των απαιτήσεων που απορρέουν από τη νομοθεσία έχουν αποτελέσει αντικείμενο διαφόρων μελετών και εκτεταμένης έρευνας (π.χ., [108][109][110][111]) και, ιδωμένες υπό το πρίσμα του ελέγχου πρόσβασης, μεταφράζονται σε ένα σύνολο απαιτήσεων για την προδιαγραφή των σχετικών τεχνολογιών.

Επιπρόσθετες απαιτήσεις υπαγορεύονται από τη διασυνεργασία ετερογενών συστημάτων και το διαμοιρασμό πόρων που χαρακτηρίζουν τα κατανεμημένα περιβάλλοντα, εισάγοντας υπολογίσιμη επιπλέον πολυπλοκότητα στην κωδικοποίηση των αναγκαίων εννοιών σε σχέση με ό,τι καλύπτεται από τις υπάρχουσες προσεγγίσεις στο χώρο. Ενδεικτικά, ο έλεγχος της πρόσβασης δεν αφορά μόνο σε προσωπικά δεδομένα των χρηστών της εκάστοτε υπηρεσίας, αλλά και ευαίσθητη εταιρική πληροφορία που περνάει τα σύνορα ενός οργανισμού, καθώς και οποιονδήποτε πόρο που συμμετέχει στη λειτουργία του συστήματος.

Με βάση τα παραπάνω, διαμορφώνονται τελικά οι ακόλουθες απαιτήσεις σε ό,τι αφορά την προστασία της ασφάλειας και της ιδιωτικότητας σε κατανεμημένα περιβάλλοντα:

**Έλεγχος πρόσβασης** Η προστασία των πόρων, συμπεριλαμβανομένων των προσωπικών δεδομένων, προϋποθέτει την εφαρμογή των κατάλληλων μηχανισμών για τον έλεγχο της πρόσβασης σε αυτά. Πέρα από τα χαρακτηριστικά των καθιερωμένων μοντέλων ελέγχου πρόσβασης, οι μηχανισμοί που στοχεύουν στην προστασία της ιδιωτικότητας πρέπει να λαμβάνουν υπόψη επιπλέον παραμέτρους· στην περίπτωση των κατανεμημένων περιβαλλόντων μάλιστα, τα πράγματα καθίστανται ακόμα πιο σύνθετα, καθώς οι έννοιες της *δυναμικότητας* και της *συνεργασίας μεταξύ διαφορετικών φορέων* κατέχουν κεντρική θέση σε αυτά. Ιδιαίτερα σημαντική στο πλαίσιο αυτό κρίνεται η κατά περίπτωση ελαχιστοποίηση των πληροφοριών που υφίστανται επεξεργασία και μεταδίδονται μεταξύ διαφορετικών συστημάτων και οργανισμών.

**Πολυδιάστατος προσδιορισμός δικαιωμάτων πρόσβασης** Λόγω της εγγενούς πολυπλοκότητας της ασφάλειας των σύγχρονων υπολογιστικών και επικοινωνιακών συστημάτων, αλλά και της ιδιωτικότητας και των υποκείμενων επιπτώσεων, οι σχετικές προσεγγίσεις θα πρέπει να περιλαμβάνουν διάφορα κριτήρια όσον αφορά τις αποφάσεις ελέγχου πρόσβασης και χρήσης, και όχι απλώς να προσδιορίζουν *ποιος χρήστης*, ο οποίος κατέχει *κάποιο ρόλο*, μπορεί να εκτελέσει *κάποια ενέργεια σε κάποιον πόρο*.

**Σκοπός συλλογής και επεξεργασίας δεδομένων** Η "αρχή του σκοπού" είναι απαραίτητη για την επίτευξη επίγνωσης της ιδιωτικότητας, καθώς αποτελεί αναπόσπαστο κομμάτι της διασφάλισης της νομιμότητας κατά τη συλλογή και επεξεργασία των δεδομένων

[12]. Ως εκ τούτου, κάθε μοντέλο ελέγχου πρόσβασης για προστασία της ιδιωτικότητας θα πρέπει να προβλέπει τον προσδιορισμό του σκοπού της συλλογής δεδομένων και τη συσχέτισή του με τις εργασίες επεξεργασίας.

**Έλεγχος ροής πληροφορίας** Πέρα από τον "κλασικό" έλεγχο πρόσβασης και χρήσης, ένα μοντέλο ελέγχου πρόσβασης σε κατανεμημένα περιβάλλοντα θα πρέπει να προβλέπει τον προσδιορισμό των αποδεκτών προτύπων όσον αφορά τη ροή των δεδομένων. Αυτό συνεπάγεται, για παράδειγμα, την παρεμπόδιση της κοινοποίησης κάποιων δεδομένων από ένα σύστημα σε κάποιο άλλο, ενώ το τελευταίο μπορεί να επιτρέπεται να λαμβάνει τα ίδια δεδομένα από ένα τρίτο σύστημα.

**Μη διασύνδεση** Ταυτόχρονα, ένα μοντέλο ελέγχου πρόσβασης με επίγνωση ιδιωτικότητας πρέπει να παρέχει τα μέσα για την παρεμπόδιση της διασύνδεσης δεδομένων. Ενώ η απαίτηση για ροή πληροφορίας με επίγνωση ιδιωτικότητας αναφέρεται στην "άμεση" μεταβίβαση δεδομένων μεταξύ συστημάτων, διεργασιών ή ανθρώπων, η ανάγκη για μη διασύνδεση αντανακλά μία γενίκευση προς την κατεύθυνση του αμοιβαίου αποκλεισμού αναφορικά με τη διάθεση ή επεξεργασία των δεδομένων, είτε άμεσα είτε έμμεσα.

**Διαχωρισμός και Σύζευξη Καθηκόντων** Στην ίδια κατεύθυνση, περιορισμοί SoD και BoD πρέπει να είναι δυνατόν να καθοριστούν και να εφαρμοστούν, δεδομένου ότι αυτοί κατέχουν σημαντική θέση μεταξύ των απαιτήσεων εξουσιοδότησης [112], που εξυπηρετούν, μεταξύ άλλων, την αποφυγή συγκρούσεων και τη μη συνδεσιμότητα.

**Συμπληρωματικές ενέργειες** Σε πολλές περιπτώσεις, η πρόσβαση σε πόρους θα πρέπει να συνοδεύεται από κάποιες συμπληρωματικές ενέργειες. Στην περίπτωση προσωπικών δεδομένων, αυτές συχνά αναφέρονται στη βιβλιογραφία ως *υποχρεώσεις ιδιωτικότητας* (*privacy obligations*) [43][113] και αφορούν, για παράδειγμα, την εφαρμογή άμεσων μέτρων προστασίας, όπως είναι η αυτόματη ανωνυμοποίηση των δεδομένων, την αλληλεπίδραση με τα υποκείμενα των δεδομένων (π.χ., όσον αφορά τις πληροφορίες ή το αίτημα για συναίνεση) ή την αρμόδια Αρχή Ιδιωτικότητας, καθώς και την εφαρμογή των διατάξεων για τη διατήρηση δεδομένων.

**Επίγνωση πλαισίου** Έχει καταστεί σαφές ότι οι αποτελεσματικές πολιτικές ασφάλειας και προστασίας της ιδιωτικότητας εξαρτώνται σε μεγάλο βαθμό από παραμέτρους πλαισίου [33][114]. Ως εκ τούτου, ένα μοντέλο ελέγχου πρόσβασης γενικού σκοπού θα πρέπει να ενσωματώνει τα αντίστοιχα στοιχεία, όσον αφορά περιορισμούς σε παραμέτρους πλαισίου και συμβάντα, και να είναι σε θέση να επιβάλλει διαφορετικά δικαιώματα πρόσβασης σύμφωνα με τους ισχύοντες περιορισμούς.

**Ετερογενή περιβάλλοντα** Η προστασία των πόρων και των μεταδιδόμενων πληροφοριών κατά την παροχή υπηρεσιών μέσω κατανεμημένων διαδικασιών επηρεάζεται από την ανάγκη της αλληλεπίδρασης πολλαπλών και ετερογενών οργανισμών, γεγονός που γίνεται πιο πολύπλοκο όταν οι εργασίες και οι ροές δεδομένων ξεφεύγουν από τα διοικητικά και διαχειριστικά σύνορα μίας χώρας. Κατά συνέπεια, οι υποκείμενες διαδικασίες και συστήματα πρέπει όχι μόνο να είναι σε θέση να διαλειτουργούν με ομότιμα συστήματα και υπηρεσίες, αλλά και να ελέγχουν την κυκλοφορία των δεδομένων ούτως ώστε να διασφαλίζεται η ιδιωτικότητα των υποκειμένων των δεδομένων και γενικά η εμπιστευτικότητα της πληροφορίας. Μάλιστα, θα πρέπει να παρέχονται μηχανισμοί για τη διαπραγμάτευση πολιτικών μεταξύ διαφορετικών διαχειριστικών φορέων, κατά την οποία θα πρέπει να επαληθεύεται ότι ο φορέας που πραγματοποιεί επεξεργασία των δεδομένων (Data Processor) έχει συμμορφωθεί με τις πολιτικές που επιβάλλονται από τον φορέα που διαχειρίζεται τα δεδομένα (Data Controller). Το ίδιο ισχύει και για περιπτώσεις όπου παρατηρούνται κανονιστικές διαφορές.

**Μηχανισμοί ασφάλειας** Η στοιχειώδης βάση για την προστασία των πόρων, και ιδιαίτερα των μεταδιδόμενων δεδομένων, είναι ασφαλώς η ασφάλεια των πληροφοριακών και επικοινωνιακών συστημάτων και των καναλιών επικοινωνίας. Στο πλαίσιο αυτό, τα συστήματα θα πρέπει να είναι ασφαλή, ούτως ώστε να είναι σε θέση να εγγυηθούν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, καθώς και να αποτρέπουν την οποιαδήποτε αθέμιτη υποκλοπή ή παρακολούθηση των δεδομένων, ενώ θα πρέπει να εφαρμόζονται οι κατάλληλοι μηχανισμοί προστασίας των επικοινωνιών. Ως εκ τούτου, το προτεινόμενο μοντέλο θα πρέπει να εξασφαλίζει την ενσωμάτωση των κατά περίπτωση αναγκαίων μηχανισμών ασφάλειας στις διαδικασίες σε οποιοδήποτε στάδιο αυτό κρίνεται απαραίτητο.

**Σημασιολογική αναπαράσταση πληροφοριών** Κάθετη σε όλα τα παραπάνω είναι η ανάγκη για ακριβή σημασιολογική αναπαράσταση των υποκείμενων εννοιών˙ ο ιδιαίτερος σημασιολογικός τύπος που χαρακτηρίζει κάθε δεδομένο, η φύση της κάθε λειτουργίας και ο σκοπός για τον οποίο αυτή πραγματοποιείται, καθώς και ο ρόλος της κάθε εμπλεκόμενης οντότητας, μεταξύ άλλων πληροφοριών, αποτελούν σημαντικές παραμέτρους που πρέπει να λαμβάνονται υπόψη κατά τη διαδικασία παροχής πρόσβασης. Ως εκ τούτου, απαιτείται η φορμαλιστική, σημασιολογική μοντελοποίηση, μεταξύ άλλων, των δεδομένων, των δραστών, των ενεργειών, των σκοπών, των συνθηκών πλαισίου, καθώς και των μεταξύ τους σχέσεων, για την προώθηση της διαφάνειας, της απόδοσης ευθυνών (accountability) και της αποτελεσματικότητας σε ό,τι αφορά την προστασία της ιδιωτικότητας.

## 3.4 Απαιτήσεις για Εξαγωγή Γνώσης

Το μέσο για την επαλήθευση της εγκυρότητας τόσο μεμονωμένων όσο και αλληλεπιδρουσών εργασιών, οι οποίες είναι δυνατόν να αποτελούν μέρος μίας ευρύτερης ροής εργασιών, καθώς και για τη λήψη αποφάσεων σχετικών με τις απαραίτητες τροποποιήσεις που καθιστούν έγκυρες τις εργασίες και τη μεταξύ τους αλληλεπίδραση, συνιστούν οι κανόνες ελέγχου πρόσβασης. Αυτοί θα πρέπει να παρέχουν την απαραίτητη γνώση για τη λειτουργία του κατανεμημένου συστήματος και, όπου αυτό κρίνεται αναγκαίο, να υποδεικνύουν την ενσωμάτωση στην υπό εξέταση αλληλεπίδραση χαρακτηριστικών προστασίας της ασφάλειας και της ιδιωτικότητας. Ενδεικτικά, η γνώση που ζητείται στα πλαίσια της επαλήθευσης και μετασχηματισμού ενός διμερούς συσχετισμού αλληλεπιδρουσών εργασιών αφορά ερωτήματα όπως τα ακόλουθα [115]:

(i) Ποιοι είναι οι σκοποί που είναι δυνατόν να εξυπηρετεί ένας διμερής συσχετισμός με βάση τις λειτουργίες που αυτός περιλαμβάνει.

(ii) Εάν ο/οι ρόλος/οι που κατέχει ο εκκινητής ενός διμερούς συσχετισμού δικαιολογεί/ούν την εκτέλεση της εν λόγω αλληλεπίδρασης για την εκπλήρωση κάποιου συγκεκριμένου σκοπού.

(iii) Εάν οι λειτουργίες που περιέχονται σε ένα διμερή συσχετισμό βρίσκονται σε συμφωνία με τους σκοπούς που ο τελευταίος υποτίθεται ότι εξυπηρετεί.

(iv) Εάν μία εργασία είναι *κατ' αρχήν* έγκυρη, δηλαδή αν οι δηλωμένοι δράστες έχουν το δικαίωμα να εκτελέσουν τη λειτουργία στους συγκεκριμένους πόρους, ανεξάρτητα από άλλους παράγοντες, υπό την έννοια ότι, αν και μία εργασία μπορεί να είναι τυπικά έγκυρη, ωστόσο μπορεί τελικά να αποδειχθεί μη έγκυρη, λόγω π.χ., ενδεχόμενης σύγκρουσης με κάποια άλλη εργασία, προαπαιτούμενων τρίτων εργασιών ή περιορισμών πλαισίου.

(v) Σε συνέχεια του προηγούμενου ερωτήματος, εάν μία εργασία είναι έγκυρη όπως ακριβώς αυτή έχει προδιαγραφεί ή αν είναι δυνατόν να καταστεί έγκυρη με "μικρές" τροποποιήσεις οι οποίες όμως δεν αλλοιώνουν το σημασιολογικό της ορισμό, όπως είναι, για παράδειγμα, η αντικατάσταση ενός πόρου, για τον οποίο απαγορεύεται η πρόσβαση, με κάποιον επιτρεπτό σημασιολογικά "συγγενικό" πόρο.

(vi) Ποιες είναι οι εργασίες που θα πρέπει να συμπληρώνουν την εκτέλεση κάποιας εργασίας, δηλαδή να προηγούνται, να έπονται ή να εκτελούνται παράλληλα με την εν λόγω εργασία, ώστε η τελευταία να καθίσταται τελικά έγκυρη. Η απάντηση στο ερώτημα αυτό βρίσκεται σε άμεση συνάρτηση με το εκάστοτε πλαίσιο, τον εκκινητή της αλληλεπίδρασης, τον υποκείμενο σκοπό, κλπ..

(vii) Ποιες είναι οι εργασίες που έρχονται σε σύγκρουση με την εκτέλεση μίας εργασίας και ποια είναι η σχετική ή απόλυτη θέση τους αναφορικά με το χρόνο εκτέλεσης της

εν λόγω εργασίας, ώστε η τελευταία να καθίσταται τελικά έγκυρη. Η απάντηση στο ερώτημα αυτό βρίσκεται σε άμεση συνάρτηση με το εκάστοτε πλαίσιο, τον εκκινητή της αλληλεπίδρασης, τον υποκείμενο σκοπό, κλπ..

(viii) Ποιες είναι οι συνθήκες πλαισίου που θα πρέπει να ισχύουν ώστε να καθίσταται μία εργασία έγκυρη.

(ix) Ποιοι είναι οι επιτρεπόμενοι δυνατοί συνδυασμοί δραστών και πόρων για την εκτέλεση κάποιας λειτουργίας, δεδομένου ότι η τελευταία θα πρέπει να εκτελεστεί σε κάθε περίπτωση. Ένα τέτοιο ερώτημα αποκτά ιδιαίτερη σημασία στην περίπτωση όπου το προφίλ εκτέλεσης μίας εργασίας δεν έχει προδιαγραφεί πλήρως, καθώς οι εξαγόμενοι συνδυασμοί δραστών και πόρων για διαφορετικές συνθήκες πλαισίου ενδέχεται να οδηγήσουν στην ενσωμάτωση *διακλαδώσεων υπό συνθήκη* (*conditional branching*) στη δεδομένη αλληλεπίδραση, όπως διαφορετικά μονοπάτια εκτέλεσης για διαφορετικά προφίλ εκτέλεσης.

(x) Εάν η αλληλεπίδραση δύο εργασιών είναι έγκυρη, όπως αυτή έχει προδιαγραφεί.

(xi) Τον προσδιορισμό των πιθανών ασυμβατοτήτων και συγκρούσεων μεταξύ δύο αλληλεπιδρουσών εργασιών, καθώς και την επίλυσή τους, π.χ., με υπόδειξη της προσθήκης κάποιας άλλης εργασίας ή με τροποποιήσεις στα δεδομένα που ανταλλάσσονται μεταξύ των εργασιών ανάλογες με εκείνες του ερωτήματος (v), λαμβάνοντας υπόψη τις παραμέτρους που σχετίζονται με τους δράστες και τους πόρους των εν λόγω εργασιών, το δηλωμένο εκκινητή, το σκοπό, κλπ..

(xii) Τον προσδιορισμό των πιθανών διαφοροποιήσεων της αλληλεπίδρασης μεταξύ δύο εργασιών με βάση παραμέτρους πλαισίου και συμβάντα, δηλαδή τον προσδιορισμό όλων των πιθανών διακλαδώσεων υπό συνθήκη που μπορεί να περιλαμβάνει η εν λόγω αλληλεπίδραση˙ ακόμα και σε περιπτώσεις όπου τέτοιου είδους διακλαδώσεις έχουν εκ των προτέρων προσδιοριστεί, ενδέχεται ο έλεγχος πρόσβασης να οδηγήσει στην προσθήκη νέων και/ή στην κατάργηση των υπαρχουσών.

Τα ερωτήματα αυτά ουσιαστικά εισάγουν πρόσθετες απαιτήσεις σε ό,τι αφορά τον καθορισμό της μορφής των κανόνων ελέγχου πρόσβασης. Σημειώνεται ότι, ανάλογα με τις απαιτήσεις του υποκείμενου συστήματος, η γνώση που εξάγεται κατά περίπτωση είναι δυνατόν να απαντά κάθε φορά είτε σε ένα από τα παρακάτω ερωτήματα είτε σε συνδυασμούς τους.

## 3.5 Αφηρημένο Μοντέλο για Έλεγχο Πρόσβασης για Προστασία της Ιδιωτικότητας

Πρέπει να σημειωθεί ότι καμία από τις προσεγγίσεις που παρουσιάστηκαν στο Κεφάλαιο 2 δεν επιτυγχάνει να καλύψει όλες τις επισημασμένες απαιτήσεις για την προστασία της ασφάλειας και ιδιωτικότητας στον έλεγχο πρόσβασης για κατανεμήμενα περιβάλλοντα. Στην ενότητα αυτή, σκιαγραφείται ένα αφηρημένο μοντέλο, το οποίο ενσωματώνει όλα τα απαιτούμενα χαρακτηριστικά που παρουσιάστηκαν στην Ενότητα 3.3 και είναι σε θέση να απαντήσει στα ερωτήματα της Ενότητας 3.4 [45]. Ουσιαστικά, το μοντέλο αυτό αποτελεί το σκελετό της προτεινόμενης προσέγγισης, όπως αυτή περιγράφεται αναλυτικά στο Κεφάλαιο 4.

Κατά το γλωσσικό πρότυπο *Υποκείμενο—Ρήμα—Αντικείμενο*, οτιδήποτε λαμβάνει χώρα κατά τη λειτουργία του συστήματος, μπορεί να θεωρηθεί ως η εκτέλεση κάποιας *λειτουργίας* από κάποιο *δράστη* πάνω σε κάποιον *πόρο*. Αυτό ισχύει σε οποιοδήποτε επίπεδο: σε χαμηλό επίπεδο, μία συσκευή ανάγνωσης RFID εκτελεί μία λειτουργία "ανάγνωσης" σε μία ετικέτα RFID, ενώ στο υψηλότερο επίπεδο της επιχειρηματικής διαδικασίας, ένα σύνολο δραστών εκτελεί μία συγκεντρωτική υπερ-λειτουργία, η οποία αποτελείται από στοιχειώδεις λειτουργίες, πάνω από ένα σύνολο πόρων που μπορεί να είναι προσωπικά και ευαίσθητα δεδομένα. Έτσι, οι κανόνες πρόσβασης θεμελιώνονται πάνω σε εννοιολογικές τριάδες ⟨*δράστες*, *λειτουργία*, *πόρος*⟩, που είναι δυνατόν να οριστούν είτε στο *επίπεδο αφαιρέσεων* είτε στο *επίπεδο προσδιορισμού*, δηλαδή, πάνω από αφαιρέσεις που εμπεριέχουν κατηγορίες στοιχείων και προσφέρουν γενικεύσεις ή πάνω από συγκεκριμένες οντότητες.

Ωστόσο, προκειμένου να ρυθμίζουν αποτελεσματικά τη λειτουργία ενός πολύπλοκου συστήματος, οι πολιτικές προστασίας της ιδιωτικότητας και οι κανόνες ελέγχου πρόσβασης πρέπει να ενσωματώνουν επιπρόσθετα χαρακτηριστικά. Πρώτον, υπάρχει η απαίτηση της πλήρους αφαίρεσης, που σημαίνει ότι όλες οι έννοιες περιγράφονται σε στο αφηρημένο επίπεδο. Αυτό επιτρέπει την κοινή διαχείριση οντοτήτων που εμπίπτουν στην ίδια σημασιολογική κατηγορία. Σε αυτό το πλαίσιο,το μοντέλο RBAC πρώτο εισήγαγε την αφαίρεση του ρόλου για τους χρήστες, η οποία αποτελεί το τυπικό πρότυπο που ακολουθείται από τις περισσότερες προσεγγίσεις. Από την άλλη πλευρά, μόνο πολύ λίγες προσεγγίσεις υποστηρίζουν αναπαράσταση με χρήση αφαιρετικών δομών για όλα τα στοιχεία [33][60], ενώ το προτεινόμενο μοντέλο συνιστά μία υβριδική προσέγγιση.

Δεύτερον, οι πολιτικές πρέπει να περιέχουν νόρμες σχετικά με το τι θα έπρεπε να έχει συμβεί πριν και τι θα πρέπει να συμβεί μετά την ενέργεια πρόσβασης, ενώ θα πρέπει επίσης να προσδιορίζουν τις συνθήκες κάτω από τις οποίες επιτρέπεται η πρόσβαση, είτε αυτές αναφέρονται σε παραμέτρους πλαισίου είτε σε συμβάντα. Ενώ σημαντική έρευνα έχει πραγματοποιηθεί στην περιοχή των πολιτικών ασφάλειας και ιδιωτικότητας οι οποίες λαμβάνουν υπόψη τις παραμέτρους ειδικότερου πλαισίου, τα περισσότερα μοντέλα υποστηρίζουν μόνο εν μέρει μερικές απλές παραμέτρους πλαισίου, κυρίως χρονικές, και πα-

ραμέτρους που σχετίζονται με το ιστορικό του συστήματος. Ωστόσο, τα πολύπλοκα συστήματα θα πρέπει να είναι σε θέση όχι μόνο να λειτουργούν λαμβάνοντας υπόψη παραμέτρους πλαισίου, αλλά επίσης και να βασίζουν τη λειτουργία τους σε ενδεχόμενα συμβάντα.

Λαμβάνοντας υπόψη τα παραπάνω, κάθε τριάδα ⟨*δράστες*, *λειτουργία*, *πόρος*⟩ μπορεί να χαρακτηριστεί ως μία *ενέργεια*. Δηλαδή, μία ενέργεια αντιπροσωπεύει οτιδήποτε λαμβάνει χώρα κάποια στιγμή, με τη δομή αυτή να μπορεί να χρησιμοποιηθεί για να μοντελοποιηθούν το παρελθοντικό, παροντικό και μελλοντικό πλαίσιο, καθώς επίσης και συμβάντα. Ως εκ τούτου, ο ορισμός κανόνων που αφορούν πολιτικές προστασίας της ιδιωτικότητας θα πρέπει να βασίζεται σε δομές του τύπου ⟨*σκοπός*, *ενέργεια*, *προ-ενέργεια*, *πλαίσιο*, *μετα-ενέργεια*⟩, με χρήση των κατάλληλων κατηγορημάτων που περιγράφουν άδειες, απαγορεύσεις και υποχρεώσεις. Η προαναφερθείσα δομή περιγράφεται ως εξής:

- Ο *σκοπός* αντανακλά τους στόχους πίσω από τη συλλογή δεδομένων και/ή την επεξεργασία τους. Στην πραγματικότητα, μία απόφαση για την παροχή πρόσβασης δεν μπορεί να ληφθεί ανεξάρτητα από την παράμετρο του σκοπού, η οποία μπορεί να διαφοροποιήσει σημαντικά τη συμπεριφορά της εκάστοτε οντότητας.
- Η *ενέργεια* συνιστά τον πυρήνα του κανόνα, υποδεικνύει, δηλαδή, την ενέργεια που ο εν λόγω κανόνας επιτρέπει, απαγορεύει ή επιβάλει να πραγματοποιηθεί.
- Η *προ-ενέργεια* αντανακλά τις ενέργειες που θα πρέπει να έχουν πραγματοποιηθεί στο παρελθόν, προκειμένου να ενεργοποιηθεί ο εν λόγω κανόνας. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση κατά την οποία ένας ασθενής θα πρέπει να παρέχει τη ρητή συγκατάθεσή του (προ-ενέργεια), προκειμένου το ιατρικό ιστορικό του να υποστεί επεξεργασία για ερευνητικούς σκοπούς.
- Το *πλαίσιο* περιγράφει συνθήκες που ορίζονται στη βάση παραμέτρων περιβάλλοντος και καταστάσεων, καθώς επίσης και συμβάντων.
- Η *μετα-ενέργεια*, στην ίδια λογική με την προ-ενέργεια, υπονοεί οτιδήποτε χρειάζεται να λάβει χώρα μετά την ενεργοποίηση του κανόνα. Για παράδειγμα, ένας κανόνας μπορεί να επιτρέπει την ανάγνωση κάποιων δεδομένων στο πλαίσιο της παροχής μίας υπηρεσίας, υπό τον όρο τα εν λόγω δεδομένα να διαγραφούν αμέσως μετά.

Τα παραπάνω στοιχεία που συμμετέχουν στον ορισμό των κανόνων θα πρέπει να είναι δυνατόν να συνδυαστούν με χρήση λογικών και άλλων τελεστών, έτσι ώστε να ορίζονται πολύπλοκοι και εκφραστικοί κανόνες, καθώς και άλλες δομές.

# Κεφάλαιο 4

# Μοντέλο Ελέγχου Πρόσβασης και Χρήσης

Μετά τον εντοπισμό των περιορισμών που παρουσιάζουν οι σχετικές προσεγγίσεις αναφορικά με τα ιδιαίτερα χαρακτηριστικά των κατανεμημένων περιβαλλόντων, η διδακτορική διατριβή προτείνει ένα καινοτόμο μοντέλο ελέγχου πρόσβασης και χρήσης βασισμένο σε πολιτικές [116], με στόχο την αντιμετώπιση των υποκείμενων ζητημάτων και την εισαγωγή χαρακτηριστικών για προστασία της ασφάλειας και της ιδιωτικότητας στο πλαίσιο εκτέλεσης κατανεμημένων εργασιών.

Ένα σημαντικό χαρακτηριστικό της εν λόγω προσέγγισης αποτελεί το γεγονός ότι βασίζεται σε ένα σημασιολογικά πλούσιο μοντέλο πληροφοριών που παρέχει αφαιρετική αναπαράσταση των βασικών οντοτήτων των κατανεμημένων συστημάτων, καθώς και τις μεταξύ τους συσχετίσεις, συμπεριλαμβανομένων εννοιών και σχεσιακών δομών που δεν έχουν εξετασθεί ακόμα ευρέως. Επιπλέον, θεμελιώνεται στη βάση των απαιτήσεων που προκύπτουν από το πλαίσιο λειτουργίας του κατανεμημένου περιβάλλοντος, καθώς και από την επεξεργασία του νομικού και κανονιστικού πλαισίου που αφορά την προστασία των δεδομένων [111]. Αυτό αντικατοπτρίζεται από τις έννοιες που περιλαμβάνονται στο μοντέλο, καθώς και από τους κανόνες ελέγχου πρόσβασης, ο τρόπος προδιαγραφής των οποίων προωθεί την υλοποίηση των θεμελιωδών αρχών της αναγκαιότητας, της αναλογικότητας, της επάρκειας, της ελαχιστοποίησης και της ελεγχόμενης πρόσβασης.

Κάτι που κυρίως χαρακτηρίζει το προτεινόμενο μοντέλο ελέγχου πρόσβασης και χρήσης είναι το γεγονός ότι θεωρεί για την αναπαράσταση των σχετικών οντοτήτων τόσο ένα επίπεδο *αφαιρέσεων* όσο και ένα *επίπεδο προσδιορισμού*. Ενώ στα παραδοσιακά μοντέλα ελέγχου πρόσβασης οι κανόνες δομούνται αποκλειστικά σε συγκεκριμένες οντότητες και οι υπάρχουσες προσεγγίσεις συνήθως είτε υιοθετούν την αφαίρεση στο επίπεδο του ρόλου, την οποία εισήγαγε το μοντέλο RBAC, είτε χρησιμοποιούν μόνο αφηρημένες οντότητες για τον ορισμό των κανόνων, το παρόν μοντέλο παρέχει την απαραίτητη ευελιξία για την απεικόνιση εννοιών και κανόνων σε όλα τα δυνατά επίπεδα αφαίρεσης: μόνο

επίπεδο αφαιρέσεων, μόνο επίπεδο προσδιορισμού, ή υβριδικό.

Επιπλέον, ο σχεδιασμός του μοντέλου είναι προσανατολισμένος σε αλληλεπιδρώντα συστήματα, προωθώντας έτσι την αποτελεσματική διαχείριση της εκτέλεσης κατανεμημένων δραστηριοτήτων. Στο πλαίσιο αυτό, οι αποφάσεις του ελέγχου πρόσβασης λαμβάνονται και εφαρμόζονται στο επίπεδο του διμερούς συσχετισμού, αντιμετωπίζοντας κατ' αυτόν τον τρόπο τους περιορισμούς που προκύπτουν λόγω της αλληλεπίδρασης μεταξύ ενεργειών. Αυτό σημαίνει ότι οι αποφάσεις δε λαμβάνονται έχοντας σαν γνώμονα μεμονωμένες ενέργειες, αλλά ότι λαμβάνουν υπόψη τόσο τη ροή λειτουργίας όσο και τη ροή δεδομένων, με αποτέλεσμα μία ολιστική θεώρηση του ελέγχου πρόσβασης κατά μήκος του συσχετισμού.

Μία ακόμη συνεισφορά του προτεινόμενου μοντέλου έγκειται στα μέσα που προσφέρει για την προδιαγραφή περιορισμών διαχωρισμού και σύζευξης καθηκόντων. Συγκεκριμένα, η ίδια η δομή των κανόνων επεκτείνει τις έννοιες του αμοιβαίου αποκλεισμού και της σύζευξης, εφαρμόζοντάς τις σε όλα τα στοιχεία που συνθέτουν μία ενέργεια, δηλαδή τους δράστες, τις λειτουργίες, τους πόρους και τους οργανισμούς.

Τέλος, σημειώνεται ότι η προτεινόμενη προσέγγιση επιτυγχάνει να είναι αρκετά γενική και εφαρμόσιμη σε ευρύ φάσμα περιπτώσεων χρήσης, καθώς το μοντέλο ελέγχου πρόσβασης ενσωματώνει όλες τις πτυχές που συναντώνται ήδη στις υπάρχουσες προσεγγίσεις.

Στην Ενότητα 4.1 αναλύεται το υποκείμενο μοντέλο πληροφοριών. Η Ενότητα 4.2 περιγράφει την έννοια της ενέργειας, η οποία κατέχει κεντρική θέση στην προτεινόμενη προσέγγιση, καθώς αποτελεί τη βάση πάνω στην οποία θεμελιώνονται οι κανόνες ελέγχου πρόσβασης και χρήσης, οι οποίοι παρουσιάζονται στην Ενότητα 4.3. Επιπλέον, θέματα κληρονομικότητας των κανόνων διερευνώνται στην Ενότητα 4.4, ενώ το κεφάλαιο κλείνει με την περιγραφή των μηχανισμών για διαχωρισμό και σύζευξη καθηκόντων (Ενότητα 4.5).

## 4.1 Μοντέλο Πληροφοριών

Στο προτεινόμενο Μοντέλο Πληροφοριών έχουν οριστεί σημασιολογικά οι βασικότερες υποκείμενες έννοιες και οι μεταξύ τους σχέσεις, τόσο στο *επίπεδο προσδιορισμού* (*concrete level*) όσο και στο *επίπεδο αφαιρέσεων* (*abstract level*). Το επίπεδο προσδιορισμού αναφέρεται σε σαφώς προσδιορισμένες οντότητες, όπως π.χ. συγκεκριμένα άτομα ή συστήματα, ενώ το επίπεδο αφαιρέσεων χρησιμοποιεί αφαιρετικές δομές για τις υποκείμενες έννοιες, κυρίως το σημασιολογικό τους τύπο ή άλλα ποιοτικά χαρακτηριστικά, επιτρέποντας την αναφορά σε οντότητες που ομαδοποιούνται με βάση κάποια κοινά χαρακτηριστικά που εμφανίζουν, όπως π.χ. το ρόλο ή τον τύπο τους. Η εισαγωγή αφαίρεσης δεν αποτελεί καινοτομία της προτεινόμενης προσέγγισης (ήδη από το μοντέλο RBAC εισάγεται η έννοια του *ρόλου* ως αφαίρεση για τους χρήστες), ωστόσο το παρόν μοντέλο περιλαμβάνει

νέες έννοιες και επιτρέπει τη *συνύπαρξη* των δύο επιπέδων σε κανόνες και άλλες δομές. Οι κύριες έννοιες που απαρτίζουν το Μοντέλο Πληροφοριών παρουσιάζονται στον Πίνακα 2.

Πίνακας 2: Έννοιες του Μοντέλου Πληροφοριών

| **Επίπεδο Αφαιρέσεων** | **Επίπεδο Προσδιορισμού** | **Ορισμός** |
|---|---|---|
| Data Types (*DT*) | Data (*D*) | Δεδομένα που συλλέγονται ή/και υπόκεινται σε επεξεργασία, οργανωμένα σύμφωνα με τους σημασιολογικούς τους τύπους |
| Roles (*R*) | Users (*U*) | Χρήστες στους οποίους ανατίθενται ρόλοι που αντανακλούν τις αρμοδιότητές τους μέσα σε κάποιον οργανισμό |
| Operations (*Op*) | Operation Instances (*OpI*) | Οι λειτουργίες αντικατοπτρίζουν όλες τις ενέργειες που μπορούν να εκτελεστούν στα πλαίσια της λειτουργίας του συστήματος |
| Operation Container Types (*OpCT*) | Operation Containers (*OpC*) | Υποσυστήματα ή άλλες λειτουργικές δομές που συνήθως προσφέρουν ένα σύνολο λειτουργιών |
| Machine Types (*MT*) | Machines (*M*) | Στοιχεία υλικού στα οποία βρίσκονται εγκατεστημένοι περιέκτες λειτουργιών |
| Organisation Types (*OrgT*) | Organisations (*Org*) | Οι διάφοροι τομείς εντός των οποίων εκτελούνται οι ενέργειες |
| Context (*Con*) | Τιμές πλαισίου | Παράμετροι πραγματικού χρόνου και συμβάντα |
| Purposes (*Pu*) | — | Οι σκοποί για τους οποίους ζητείται πρόσβαση σε κάποιον πόρο του συστήματος |
| Attributes (*Att*) | Τιμές ιδιοτήτων | Χαρακτηριστικά που περιγράφουν περαιτέρω μέλη των υπόλοιπων συνόλων |

Έτσι, στο επίπεδο προσδιορισμού, το σύνολο των *Χρηστών* (*Users — U*) συμμετέχει σε *Οργανισμούς* (*Organisations — Org*) χρησιμοποιώντας *Περιέκτες Λειτουργιών* (*Operation Containers — OpC*), οι οποίοι είναι εγκατεστημένοι σε *Μηχανές* (*Machines — M*) και προσφέρουν ένα σύνολο *Στιγμιοτύπων Λειτουργιών* (*Operation Instances — OpI*)[9], ώστε να πραγματοποιήσουν κάποια ενέργεια σε *Αντικείμενα* (*Objects — Obj*), με τα τελευταία να αναφέρονται σε οτιδήποτε επηρεάζεται ή απαιτείται για την εκτέλεση της ενέργειας, όπως π.χ., *Δεδομένα* (*Data — D*) που συλλέγονται ή/και υπόκεινται σε επεξεργασία.

Στο επίπεδο αφαιρέσεων, στους χρήστες ανατίθενται *Ρόλοι* (*Roles — R*), οι ενέργειές τους αφορούν κάποιες *Λειτουργίες* (*Operations — Op*) και πραγματοποιούνται για την ικανοποίηση κάποιων *Σκοπών* (*Purposes — Pu*). Επιπλέον, τα δεδομένα, οι οργανισμοί, οι μηχανές και οι περιέκτες λειτουργιών χαρακτηρίζονται από *τύπους* που αντανακλούν τη σημασιολογική κλάση στην οποία εμπίπτουν˙ έτσι, ορίζονται τα αντίστοιχα σύνολα *Τύποι Δεδομένων* (*Data Types — DT*), *Τύποι Οργανισμών* (*Organisation Types — OrgT*), *Τύποι Μηχανών* (*Machine Types — MT*) και *Τύποι Περιεκτών Λειτουργιών* (*Operation Container Types — OpCT*). Σημειώνεται ότι, στη γενική περίπτωση, έννοιες του επιπέδου προσδιορισμού συσχετίζονται με έννοιες του επιπέδου αφαιρέσεων μέσω κατηγορήματος του τύπου *isOfType*˙ για παράδειγμα, η συσχέτιση κάποιου δεδομένου με τον τύπο του πραγματοποιείται μέσω του

[9]Με όρους Υπηρεσιών Ιστού, οι Περιέκτες Λειτουργιών αντιστοιχούν σε στοιχεία `portType` μίας υπηρεσίας, ενώ τα Στιγμιότυπα Λειτουργιών αναπαριστούν τα στοιχεία `operations`.

λογικού κατηγορήματος *isOfDataType*(*d*, *dt*), όπου $d \in D$ και $dt \in DT$. Ξεχωριστή θέση κατέχουν, τέλος, το *Πλαίσιο Λειτουργίας* (*Context — C*), που επιτρέπει τον προσδιορισμό παραμέτρων πλαισίου, καθώς και οι *Ιδιότητες* (*Attributes — Att*), οι οποίες χρησιμοποιούνται για την περιγραφή ιδιοτήτων και χαρακτηριστικών άλλων στοιχείων.

Αν και οι περισσότερες από αυτές τις έννοιες είτε συμπεριλαμβάνονται ήδη σε υπάρχοντα μοντέλα είτε είναι αυτονόητες, κάποιες επιδέχονται περαιτέρω σχολιασμού. Συγκεκριμένα, οι έννοιες *OpC* και *OpCT* εισάγονται με στόχο τη μοντελοποίηση τμημάτων του συστήματος ή άλλων λειτουργικών δομών που προσφέρουν συνήθως ένα σύνολο λειτουργιών. Για παράδειγμα, ένας περιέκτης λειτουργιών του τύπου `IntrusionDetectionSystem` ομαδοποιεί διάφορες λειτουργίες σχετικές με την ανίχνευση εισβολών. Εκτός από την ευκολία που εισάγουν σχετικά με διάφορες πτυχές της μοντελοποίησης (όπως η κληρονομικότητα των ιδιοτήτων), οι δομές αυτές είναι επίσης χρήσιμες για την περιγραφή εννοιών που σχετίζονται με *οριζόντιες* εξαρτήσεις και μεταφορά χαρακτηριστικών. Επιπλέον, οι μηχανές διαδραματίζουν θεμελιώδη ρόλο στα κατανεμημένα περιβάλλοντα· σε κάθε περίπτωση, μία λειτουργία παρέχεται από κάποια μηχανή, η οποία, από τη μία πλευρά, χαρακτηρίζεται από ιδιότητες που μπορούν να κληρονομούνται στην παρεχόμενη λειτουργία (π.χ., τοπολογικές ιδιότητες) και, αφετέρου, από τη δημιουργία εγγενών εξαρτήσεων μεταξύ των λειτουργιών που προσφέρει. Τέλος, οι οργανισμοί μοντελοποιούνται ρητά τόσο στο επίπεδο αφαιρέσεων όσο και στο επίπεδο προσδιορισμού, καθώς στο πλαίσιο ενός ενοποιημένου μοντέλου, παρόμοιοι κανόνες μπορεί να οριστούν διαφορετικά για ετερογενείς τύπους οργανισμών. Για παράδειγμα, στο πλαίσιο ενός οργανισμού του τύπου `BillingServiceProvider`, οι άδειες για πρόσβαση στα δεδομένα των πελατών δε θα είναι οι ίδιες με εκείνες που καθορίζονται για τα ίδια δεδομένα μέσα σε έναν οργανισμό του τύπου `TelecomOperator`, ο οποίος αποτελεί την οντότητα που είναι υπεύθυνη για τα δεδομένα (Data Controller). Επιπλέον, ένας οργανισμός που συμμετέχει σε συνεργασίες με τρίτους οργανισμούς θα εφαρμόσει πιθανότατα διαφορετικές πολιτικές πρόσβασης για τους οργανισμούς αυτούς με βάση τον τύπο τους.

Οι έννοιες που παρουσιάστηκαν στον Πίνακα 2 σχηματίζουν γράφους στοιχείων που χαρακτηρίζονται εγγενώς από πολύπλοκες συσχετίσεις μεταξύ τους· οι τελευταίες υλοποιούνται μέσω λογικών κατηγορημάτων, τα οποία δημιουργούν ιεραρχίες τύπου AND και OR και επιτρέπουν την κληρονομικότητα των ιδιοτήτων και των κανόνων, καθώς και τον προσδιορισμό εξαρτήσεων. Για παράδειγμα, και σε σχέση με το γράφο *DT*, έχουν οριστεί τρεις σχέσεις μερικής διάταξης: *isA*($dt_i$, $dt_j$), *lessDetailedThan*($dt_i$, $dt_j$) και *isPartOf* ($dt_i$, $dt_j$), όπου $dt_i$ και $dt_j \in DT$, οι οποίες αντικατοπτρίζουν τη συγκεκριμενοποίηση μίας έννοιας, το επίπεδο λεπτομέρειας, και τη συμπερίληψη ορισμένων τύπων δεδομένων σε κάποιον άλλο, αντίστοιχα. Μερικές ενδεικτικές σχέσεις που σχηματίζουν ιεραρχίες μεταξύ των μελών ενός συνόλου παρουσιάζονται στον Πίνακα 3. Θα πρέπει επίσης να σημειωθεί ότι το κατηγόρημα *inheritsFrom*($m_i$, $m_j$) που υποδηλώνει την κληρονομικότητα των χαρακτηριστικών, όπως ιδιοτήτων και κανόνων, υπονοείται από τα άλλα κατηγορήματα και επιτρέπει τον ορισμό των κανόνων σε υψηλά επίπεδα αφαίρεσης, με αποτέλεσμα τη μείωση του αριθ-

μού των πολιτικών. Έτσι, οι πολιτικές που ρυθμίζουν την πρόσβαση στα δεδομένα είναι δυνατόν να ορίζονται για γενικότερους τύπους δεδομένων και στη συνέχεια να μεταβιβάζονται σε πιο συγκεκριμένους, ή σύνθετοι τύποι δεδομένων να κληρονομούν πολιτικές, οι οποίες έχουν ρητά ορισθεί για τους τύπους δεδομένων που τους αποτελούν. Ο τρόπος με τον οποίο η σχέση *inheritsFrom* συνάγεται από τις υπόλοιπες παρουσιάζεται πιο αναλυτικά στην Ενότητα 4.4.

Επιπλέον, στο μοντέλο προβλέπονται τα απαραίτητα κατηγορήματα για το συσχετισμό εννοιών που ανήκουν σε διαφορετικούς γράφους˙ για παράδειγμα, το κατηγόρημα $mayActForPurposes(r, \langle pu \rangle^k)$, όπου $r \in R$ και $\langle pu \rangle^k \subseteq \mathcal{P}(Pu)$, υποδεικνύει τους συμβατούς σκοπούς $\langle pu \rangle^k$ για τους οποίους μπορούν να ενεργούν οι χρήστες στους οποίους έχει ανατεθεί ο ρόλος $r$.

Πίνακας 3: Βασικές σχέσεις μεταξύ των $m_i$, $m_j$ μελών ενός συνόλου

| **Κατηγόρημα** | **Περιγραφή** | **Ισχύει για Σύνολα** | **Παράδειγμα** |
|---|---|---|---|
| $isA(m_i, m_j)$ | Εκφράζει τη σχέση εξειδίκευσης | *DT*, *R*, *Op*, *OpCT*, *MT*, *Pu* | $isA$(`ChiefSecurityOfficer`, `SecurityOfficer`), $m_i, m_j \in R$ |
| $isPartOf(m_i, m_j)$ | Εκφράζει τη σχέση συμπερίληψης | *DT*, *R*, *Op* | $isPartOf$(`IPHeader`, `IPPacket`), $m_i, m_j \in DT$ |
| $lessDetailedThan(m_i, m_j)$ | Εκφράζει το βαθμό λεπτομέρειας | *DT* | $lessDetailedThan$(`IPv4AddressNetworkID`, `IPv4Address`), $m_i, m_j \in DT$ |

Στη συνέχεια, οι κυριότερες από τις παραπάνω έννοιες περιγράφονται σε μεγαλύτερο βάθος, προκειμένου να αναδειχθούν οι κύριες πτυχές της προσέγγισης σε ό,τι αφορά την προστασία της ασφάλειας και της ιδιωτικότητας.

### 4.1.1 Δεδομένα και Τύποι Δεδομένων

Τα δεδομένα που συλλέγονται και υπόκεινται σε επεξεργασία κατέχουν κεντρική θέση στη λειτουργία των κατανεμημένων περιβαλλόντων. Χαρακτηρίζονται από έναν *τύπο δεδομένων*, δηλαδή τη σημασιολογική κατηγορία στην οποία ανήκουν. Πράγματι, η σημασιολογία των δεδομένων παίζει σημαντικό ρόλο στον τρόπο επεξεργασίας τους, καθώς και στην εφαρμογή των απαιτήσεων που σχετίζονται με την προστασία της ιδιωτικότητας. Στο πλαίσιο αυτό και όπως έχει προαναφερθεί, ορίστηκαν δύο σύνολα: το σύνολο *Data* (*D*), το οποίο αντιπροσωπεύει τα δεδομένα στο επίπεδο προσδιορισμού, και το σύνολο *Data Types* (*DT*), το οποίο αντανακλά τους σημασιολογικούς τύπους δεδομένων στο επίπεδο αφαιρέσεων.

Η οργάνωση των διαφόρων τύπων δεδομένων πραγματοποιείται μέσω των κατηγορημάτων $isA(dt_i, dt_j)$, $lessDetailedThan(dt_i, dt_j)$ και $isPartOf(dt_i, dt_j)$ του Πίνακα 3, τα οποία καθορίζουν μεταβατικές και αντισυμμετρικές μερικές διατάξεις τύπων δεδομένων και αντανακλούν, αντίστοιχα, τη συγκεκριμενοποίηση μίας έννοιας, το επίπεδο λεπτομέρειας και

τη συμπερίληψη ενός τύπου δεδομένων σε κάποιον άλλο. Όσον αφορά το κατηγόρημα *lessDetailedThan*($dt_i$, $dt_j$), αυτό επιτρέπει την αποτελεσματική ρύθμιση της ακρίβειας των δεδομένων που υπόκεινται σε συλλογή/επεξεργασία/μετάδοση, με στόχο να ικανοποιηθεί η λεγόμενη "αρχή της αναλογικότητας", η οποία απαιτεί ότι τα προσωπικά και εταιρικά δεδομένα μπορούν να συλλέγονται και να υφίστανται επεξεργασία μόνο στο βαθμό που είναι κατάλληλα, συναφή και όχι υπερβολικά σε σύγκριση με τη λειτουργία για την οποία συλλέγονται από το σύστημα.

Όσον αφορά την κληρονομικότητα ιδιοτήτων, κάθε πιο συγκεκριμένος τύπος δεδομένων έχει όλα τα χαρακτηριστικά του γενικού τύπου δεδομένων, καθώς και επιπλέον χαρακτηριστικά που τον διαφοροποιούν. Για παράδειγμα, σε έναν τύπο δεδομένων είναι δυνατόν να αποδοθεί μία ιδιότητα που υποδηλώνει τον ιδιοκτήτη του ή την περίοδο διατήρησης· αυτή η ιδιότητα κληρονομείται σε όλους τους πιο συγκεκριμένους από αυτόν τύπους δεδομένων. Κληρονομικότητα των ιδιοτήτων είναι δυνατόν να συναχθεί και για τύπους δεδομένων που συνδέονται μέσω των σχέσεων *isPartOf* και *lessDetailedThan*, ανάλογα πάντα με τη φύση της αντίστοιχης ιδιότητας.

### 4.1.2 Χρήστες και Ρόλοι

Στους χρήστες ανατίθενται ρόλοι, οι οποίοι αντανακλούν τις αρμοδιότητές τους μέσα σε κάποιον οργανισμό, μέσω του ακόλουθου κατηγορήματος που δηλώνει ότι στον χρήστη $u$ ανατίθενται οι ρόλοι $\langle r \rangle^k$:

- *assignedWithRoles*($u$, $\langle r \rangle^k$), όπου $u \in U$ και $\langle r \rangle^k \subseteq \mathcal{P}(R)$.

Όπως φαίνεται στον Πίνακα 3, και οι ρόλοι οργανώνονται σύμφωνα με τις σχέσεις *isA* και *isPartOf*, οι οποίες υποδηλώνουν συγκεκριμενοποίηση ενός ρόλου και συμπερίληψή του σε κάποιο σύνθετο, αντίστοιχα. Η δεύτερη σχέση μάλιστα μοντελοποιεί περιπτώσεις όπως είναι η συμμετοχή ενός ρόλου `NetworkAdministrator` στο σύνθετο ρόλο Computer Security Incident Response Team (CSIRT) [117], ο οποίος ορίζεται σημασιολογικά ως `CSIRT`.

Η κληρονομικότητα των εξουσιοδοτήσεων μέσω της σχέσης *inheritsFrom* εξετάζεται στην Ενότητα 4.4. Επιπλέον, εκτός από τις ρητά ορισμένες ιδιότητες, οι ρόλοι αποκτούν και όλα τα χαρακτηριστικά των προγόνων τους στην εκάστοτε ιεραρχία ρόλων. Για παράδειγμα, η ιδιότητα `att_Schedule` που φέρει ο ρόλος `Employee` κληρονομείται από το ρόλο `NetworkAdministrator`, ο οποίος συνδέεται με τον πρώτο μέσω της σχέσης *isA*. Στην περίπτωση της σχέσης *isPartOf*, οι ιδιότητες του σύνθετου ρόλου συνάγονται με βάση τις αντίστοιχες ιδιότητες των ρόλων που τον απαρτίζουν.

### 4.1.3 Λειτουργίες

Οι λειτουργίες αντανακλούν όλες τις ενέργειες που είναι δυνατόν να εκτελεστούν στα πλαίσια της λειτουργίας του συστήματος, συνιστώντας τον πυρήνα της δομής της *ενέργειας*, όπως θα περιγραφεί αναλυτικότερα στην Ενότητα 4.2. Υπάρχουν επίσης περιπτώσεις όπου οι λειτουργίες παίζουν το ρόλο του δράστη σε μία ενέργεια, ειδικά σε ιδιαίτερα αυτοματοποιημένα συστήματα όπου λειτουργίες είναι δυνατόν να προκαλέσουν την εκτέλεση άλλων λειτουργιών.

Οι λειτουργίες απαρτίζουν ένα σύνολο σημασιολογικά ορισμένων στοιχείων (*Operations — Op*) και εμφανίζουν διάφορα επίπεδα ανάλυσης. Ξεκινώντας από πολύ στοιχειώδεις λειτουργίες, οι οποίες χαρακτηρίζονται ως *ατομικές*, φτάνουμε σε λειτουργίες που είναι δυνατόν να οργανωθούν σε διάφορες δομές και να σχηματίσουν πολύπλοκες συνθέσεις, οι οποίες μπορούν να φτάσουν σε πολύ υψηλό επίπεδο και να αναπαραστήσουν πολύ γενικές εργασίες, διευκολύνοντας με αυτόν τον τρόπο την αναπαράσταση πολύπλοκων συνθέσεων με αφαιρετικές δομές. Συγκεκριμένα, οι λειτουργίες σχηματίζουν ιεραρχίες που υποδηλώνουν τα διαφορετικά επίπεδα ανάλυσης, με βάση το σημασιολογικό ορισμό των ίδιων των λειτουργιών. Το κατηγόρημα *isA* εκφράζει τη λογική σχέση OR υποδεικνύοντας εναλλακτικές λειτουργίες, οι οποίες υλοποιούν την ίδια λειτουργία, ενώ το κατηγόρημα *isPartOf* συνιστά τη λογική σχέση AND, καθιστώντας υποχρεωτική την εκτέλεση όλων των πιο στοιχειωδών λειτουργιών ούτως ώστε να ολοκληρωθεί η σύνθετη λειτουργία.

Παρ' όλα αυτά, για να περιγραφούν λεπτομερώς πιο σύνθετες λειτουργίες, όπως για παράδειγμα μία καλά ορισμένη αλληλουχία λειτουργιών, οι AND και OR σχέσεις δεν επαρκούν· κρίνεται απαραίτητος ο ορισμός επιπρόσθετων σχέσεων, καθώς και περιορισμών που αφορούν τη σειρά εκτέλεσης των συμπεριλαμβανόμενων λειτουργιών. Τελικά, μία δομή αυτού του είδους χαρακτηρίζεται από ένα σύνολο λειτουργιών και ένα σύνολο κατευθυνόμενων ακμών (σύνολο *Legs*), οι οποίες συνδέουν γειτονικές λειτουργίες και μοντελοποιούν τη ροή ελέγχου και δεδομένων μεταξύ τους. Αυτές οι αλληλουχίες λειτουργιών με καλά ορισμένες ροές ελέγχου και δεδομένων ονομάζονται *worklets* [118] και περιγράφουν λεπτομερώς την υλοποίηση κάποιας σύνθετης λειτουργίας. Κατά συνέπεια, ορίζεται το ακόλουθο σύνολο, καθώς και το αντίστοιχο κατηγόρημα:

- *Worklets* (*Wl*), το σύνολο των προκαθορισμένων αυτόνομων υπο-διαδικασιών που περιγράφουν την υλοποίηση μίας λειτουργίας από λειτουργίες χαμηλότερου επιπέδου.
- *implementsOperation*(*wl*, *op*), όπου $wl \in Wl$, $op \in Op$.

Με άλλα λόγια, ένα worklet αποτελεί το ίδιο μία λειτουργία —ικανοποιώντας έτσι την αρχή της επαναχρησιμοποίησης— και είναι δυνατόν να οδηγήσει σε διαφορετικές εκτελέσεις σύμφωνα με τις υποκείμενες εξουσιοδοτήσεις που αφορούν τις συμπεριλαμβανόμενες λειτουργίες.

Οι λειτουργίες είναι δυνατόν να παίρνουν σαν είσοδο δεδομένα και παραμέτρους, ενώ μπορούν να εξάγουν δεδομένα ή να προκαλούν την εκτέλεση κάποιας άλλης λειτουργίας. Για τη συσχέτιση μίας λειτουργίας με τους τύπους δεδομένων που μπορεί να λάβει σαν είσοδο και να δίνει στην έξοδο, ορίζονται τα ακόλουθα κατηγορήματα:

- *hasInput*(*op*, $\langle dt \rangle^k$), όπου $op \in Op$, $\langle dt \rangle^k \subseteq \mathcal{P}(DT)$.
- *hasOutput*(*op*, $\langle dt \rangle^k$), όπου $op \in Op$, $\langle dt \rangle^k \subseteq \mathcal{P}(DT)$.

Οι απαιτούμενες παράμετροι για την εκτέλεση μίας λειτουργίας αντιμετωπίζονται σαν ιδιότητες. Για παράδειγμα, η ιδιότητα `att_AcceptsHumanActor` δηλώνει αν μία λειτουργία θα πρέπει να εκτελεστεί από κάποιον χρήστη ή αν είναι αυτοματοποιημένη.

Επιπλέον, οι λειτουργίες οργανώνονται με βάση το μηχανισμό που αντιπροσωπεύει η έννοια των *περιεκτών λειτουργιών* (*operations' containers*). Όπως ειπώθηκε παραπάνω, η έννοια αυτή αναφέρεται σε υποσυστήματα ή άλλες λειτουργικές δομές που συνήθως προσφέρουν ένα σύνολο λειτουργιών. Το κατηγόρημα που συσχετίζει λειτουργίες με ένα τύπο περιεκτών είναι το ακόλουθο:

- *providesOperations*(*opct*, $\langle op \rangle^k$), όπου $opct \in OpCT$, $\langle op \rangle^k \subseteq \mathcal{P}(Op)$.

Οι λειτουργίες αναπαριστώνται και στο επίπεδο προσδιορισμού, μέσω των *Στιγμιοτύπων Λειτουργίας* (*Operation Instances*). Τα Στιγμιότυπα Λειτουργίας αντιστοιχούν σε *υλοποιήσεις* των λειτουργιών από συγκεκριμένα συστήματα. Με όρους Υπηρεσιών Ιστού [6], ένα στιγμιότυπο λειτουργίας είναι ισοδύναμο με την αφηρημένη περιγραφή μίας *λειτουργίας* (*operation*), σε συνδυασμό με την πληροφορία για σύνδεση με το επίπεδο προσδιορισμού, όπως αυτό προκύπτει από το συσχετισμένο περιέκτη λειτουργιών και τη μηχανή που παρέχει τη λειτουργία.

Για τη διαχείριση των στιγμιοτύπων λειτουργίας ορίζονται διάφορα κατηγορήματα, μεταξύ των οποίων αυτά που συσχετίζουν ένα στιγμιότυπο λειτουργίας με τη λειτουργία που υλοποιεί και διάφορα στιγμιότυπα με έναν περιέκτη λειτουργιών:

- *instantiatesOperation*(*opi*, *op*), όπου $opi \in OpI$, $op \in Op$.
- *containsOperationInstances*(*opc*, $\langle opi \rangle^k$), όπου $opc \in OpC$, $\langle opi \rangle^k \subseteq \mathcal{P}(OpI)$.

Παρ' όλα αυτά, δεν είναι δυνατόν να οριστούν στιγμιότυπα για όλες τις λειτουργίες. Για παράδειγμα, λειτουργίες όπως οι `execute`, `read` και `invoke` βρίσκουν αναπαράσταση μόνο στο επίπεδο αφαιρέσεων.

Τέλος, σημειώνεται ότι, καθώς οι περιέκτες λειτουργιών φιλοξενούνται από μηχανές, ορίζεται το αντίστοιχο κατηγόρημα, δηλαδή το *hostsContainers*(*mt*, $\langle opct \rangle^k$), όπου $mt \in$

$MT$, $\langle opct \rangle^k \subseteq \mathcal{P}(OpCT)$, το οποίο επιτρέπει την αντανάκλαση των συνεπειών της εκτέλεσης μίας λειτουργίας μέσα σε μία μηχανή στους περιέκτες λειτουργιών που φιλοξενούνται από τη μηχανή και ενδεχομένως στις λειτουργίες που αυτοί προσφέρουν.

### 4.1.4 Πληροφορίες Πλαισίου

Στην πράξη, οι κανόνες ελέγχου πρόσβασης παραμένουν ανενεργοί μέχρις ότου να πληρούνται μία σειρά από προϋποθέσεις, δηλαδή, έως ότου οι προϋποθέσεις αξιολογηθούν και αντιστοιχηθούν σε μία τιμή αλήθειας. Ως εκ τούτου, ορίζουμε ως *πολιτικές με επίγνωση πληροφορίας πλαισίου* τις πολιτικές εκείνες που βασίζουν την εξουσιοδότηση σε δυναμικά διαμορφούμενη πληροφορία. Κατά συνέπεια, οι κανόνες εξουσιοδότησης μπορεί να εξαρτώνται από χρονικές παραμέτρους (π.χ., άδειες χορηγούνται μόνο κατά τις ώρες εργασίας), γεωγραφικές παραμέτρους (π.χ., άδεια εντός των φυσικών ορίων μίας εταιρείας), ή τις λεγόμενες *a priori* παραμέτρους, όπου η άδεια για την εκτέλεση ενός συνόλου ενεργειών μπορεί να χορηγηθεί μόνο ως αποτέλεσμα της ολοκλήρωσης προηγούμενων ενεργειών. Επομένως, είναι σημαντικό οι συνθήκες πλαισίου όχι μόνο να αποτυπώνονται στο μοντέλο, αλλά και να λαμβάνονται υπόψη κατά τη διαδικασία ελέγχου και μετασχηματισμού, επιτρέποντας τον προσδιορισμό διαφορετικών εκδοχών του ίδιου διμερούς συσχετισμού ανάλογα με την τιμή κάποιας παραμέτρου πλαισίου.

Με βάση τα παραπάνω, ορίζεται στο Μοντέλο Πληροφοριών το σύνολο *Context* (*Con*) για τον ορισμό παραμέτρων πλαισίου, οι οποίες αφορούν είτε σε παραμέτρους πραγματικού χρόνου, όπως είναι η γεωγραφική θέση ή ο χρόνος, είτε σε συμβάντα (events). Για τον ορισμό παραμέτρων πλαισίου χρησιμοποιούνται αποτιμήσιμες συνθήκες, οι οποίες πρέπει να ισχύουν για να ενεργοποιηθεί κάποιος κανόνας. Μερικές κατηγορίες τέτοιων συνθηκών πλαισίου είναι οι εξής: *Χρονικές* συνθήκες πλαισίου (*Temporal* context), οι οποίες εξαρτώνται από τη χρονική στιγμή κατά την οποία ζητείται πρόσβαση σε κάποιον πόρο, *Χωρικές* συνθήκες πλαισίου (*Spatial* context), οι οποίες εξαρτώνται από τη θέση του δράστη ή/και του πόρου, και συνθήκες που καθίστανται αληθείς με την πραγματοποίηση κάποιου συμβάντος (*Event* context). Επιπλέον, είναι δυνατόν να οριστούν λογικές δομές αποτελούμενες από τέτοιες συνθήκες μέσω δύο σχέσεων, οι οποίες έχουν σαν αποτέλεσμα τη δημιουργία OR και AND δέντρων, αντίστοιχα. Με αυτόν τον τρόπο, μία πληροφορία πλαισίου $cont \in Con$ μπορεί να οριστεί σαν το λογικό OR/λογικό AND ενός συνόλου επιμέρους πληροφοριών πλαισίου, ενώ επίσης είναι δυνατός ο ορισμός αρνητικών συνθηκών. Οι συνθήκες που αποτελούν συνδυασμό επιμέρους συνθηκών ονομάζονται *σύνθετες*, σε αντιδιαστολή με τις *ατομικές* συνθήκες.

### 4.1.5 Σκοποί

Η έννοια του σκοπού για τον οποίο ζητείται πρόσβαση σε πόρους αποτελεί θεμελιώδη έννοια για την προστασία της ιδιωτικότητας, η οποία θα πρέπει να λαμβάνεται σε

κάθε περίπτωση υπόψη. Μολονότι θα μπορούσε να μοντελοποιηθεί σαν μία ακόμα περίπτωση πληροφορίας πλαισίου (όπως στην προσέγγιση [39]), στο Μοντέλο Πληροφοριών ο σκοπός περιλαμβάνεται σαν μία αυτόνομη έννοια, με κύριο στόχο να τονιστεί η σημασία του σε ό,τι αφορά την προστασία της ιδιωτικότητας, καθώς και να διαχωριστεί από παραμέτρους πραγματικού χρόνου και συμβάντα. Έτσι, ορίζεται το σύνολο των σκοπών *Purposes* (*Pu*), με τα μέλη του να σχηματίζουν ιεραρχίες λόγω της ύπαρξης της OR σχέσης *isA*, η οποία μοντελοποιεί τη συγκεκριμενοποίηση ενός σκοπού υψηλού επιπέδου σε πιο ειδικούς σκοπούς.

Σε ό,τι αφορά τις λειτουργίες, δεν μπορούν όλες να εκτελεστούν για την εκπλήρωση κάποιου σκοπού, υπό την έννοια ότι δεν είναι συμβατές και συνεπείς με το σκοπό αυτό, γεγονός που εκφράζεται μέσω του ακόλουθου κατηγορήματος:

- *mayServePurposes*$(op, \langle pu \rangle^k)$, όπου $op \in Op$, $\langle pu \rangle^k \subseteq \mathcal{P}(Pu)$.

Συνδυάζοντας το κατηγόρημα αυτό με την προαναφερθείσα σχέση *isA*, συνάγεται ότι, εκτός από τους ρητά ορισμένους σκοπούς, μία λειτουργία μπορεί ακόμη να εξυπηρετεί πιο συγκεκριμένους ή πιο γενικούς σκοπούς. Επιπροσθέτως, συνεπάγεται μέσω των σχέσεων συγκεκριμενοποίησης *isA* ή συμπερίληψης *isPartOf* ότι όλες οι λειτουργίες που σχετίζονται με αυτήν εξυπηρετούν αυτούς τους σκοπούς.

Ομοίως, η παρατήρηση ότι δεν μπορούν όλοι οι ρόλοι να ενεργούν για όλους τους σκοπούς οδηγεί στον ορισμό του κατηγορήματος:

- *mayActForPurposes*$(r, \langle pu \rangle^k)$, όπου $r \in R$, $\langle pu \rangle^k \subseteq \mathcal{P}(Pu)$.

Θα πρέπει να σημειωθεί ότι τα δύο αυτά κατηγορήματα ορίζονται ρητά —ενώ θα μπορούσαν απλώς να συναχθούν μέσω διαδικασίας συλλογιστικής στη βάση των κανόνων ελέγχου πρόσβασης (βλ. Ενότητα 4.3)— με στόχο την υποστήριξη του βήματος επαλήθευσης του σκοπού της Διαδικασίας Επαλήθευσης Διμερούς Συσχετισμού (βλ. Ενότητα 7.2)· αυτή η σχεδιαστική επιλογή επιτρέπει έναν "γρήγορο" έλεγχο της συμμόρφωσης του εκάστοτε σκοπού. Σε αυτό το πλαίσιο, το κατηγόρημα *mayServePurposes* επιτρέπει τον έλεγχο σχετικά με το αν οι λειτουργίες που συμπεριλαμβάνονται σε ένα συσχετισμό συμμορφώνονται με το σκοπό τον οποίο αυτός υποτίθεται πως εξυπηρετεί. Από την άλλη πλευρά, το κατηγόρημα *mayActForPurposes* χρησιμοποιείται για να ελεγχθεί το αν οι ρόλοι που κατέχει ο εκκινητής δικαιολογούν την πραγματοποίηση της αλληλεπίδρασης, προκειμένου να ικανοποιηθεί κάποιος συγκεκριμένος σκοπός.

Όσον αφορά τον έλεγχο της συμμόρφωσης μεταξύ του σκοπού για τον οποίο ενεργεί ένας ρόλος και εκείνου τον οποίο εξυπηρετεί μία λειτουργία, χρησιμοποιείται το ακόλουθο κατηγόρημα:

- *compliantWithPurpose*$(pu_r, pu_{op})$, όπου $pu_r, pu_{op} \in Pu$.

### 4.1.6 Ιδιότητες

Οι ιδιότητες αποτελούν μία σημαντική πλευρά του μοντέλου πληροφοριών, συμπληρώνοντας και περιγράφοντας περαιτέρω τα μέλη των υπόλοιπων συνόλων τόσο στο επίπεδο αφαιρέσεων όσο και στο επίπεδο προσδιορισμού. Ως εκ τούτου, ορίζεται το αντίστοιχο σύνολο *Attributes* (*Att*) και τα μέλη του περιγράφονται φορμαλιστικά μέσω του διατεταγμένου ζεύγους ⟨AttributeName, AttributeType⟩, χαρακτηρίζονται δηλαδή από ένα όνομα και έναν τύπο. Σημειώνεται ότι για το όνομα των ιδιοτήτων, το πρόθεμα `att_` χρησιμοποιείται κατά σύμβαση, προκειμένου να αποφευχθεί η σύγχυση με τα μέλη των άλλων συνόλων. Σε ό,τι αφορά τον τύπο μίας ιδιότητας, αυτός μπορεί να είναι κάποιος απλός τύπος, π.χ., boolean, integer, κλπ., ή μέλος ενός άλλου συνόλου. Τα παρακάτω αποτελούν παραδείγματα ορισμού ιδιοτήτων:

- ⟨`att_Raw`, `boolean`⟩, που δηλώνει αν κάποιο δεδομένο δεν έχει υποστεί επεξεργασία ή έχει προκύψει ως αποτέλεσμα κάποιας λειτουργίας επεξεργασίας.
  Εδώ ο τύπος της ιδιότητας ορίζεται ως `boolean`.
- ⟨`att_NetworkAddress`, `IPv4Address`⟩, όπου `IPv4Address` $\in DT$, ιδιότητα η οποία χαρακτηρίζει κάποια οντότητα, π.χ., μία διεπαφή δικτύου, χρησιμοποιώντας τη διεύθυνση δικτύου της.
  Σε αυτήν την περίπτωση, το στοιχείο `IPv4Address` του συνόλου *DT* ορίζεται ως ο τύπος της ιδιότητας.

Οι αντιστοιχήσεις μεταξύ οντοτήτων και ιδιοτήτων επιτυγχάνεται μέσω των ακόλουθων κατηγορημάτων:

- *hasAttribute*(*entity*, $\langle at \rangle^k$), όπου $entity \in DT \cup Op \cup OpCT \cup R \cup MT \cup OrgT \cup D \cup OpC \cup U \cup M \cup Org$ και $\langle at \rangle^k \subseteq \mathcal{P}(Att)$, ή
- *hasAttributeValue*(*entity*, *at*, *value*), το οποίο περιλαμβάνει και την τιμή της ιδιότητας, η οποία πρέπει να συμμορφώνεται με τον καθορισμένο τύπο.

Η τιμή μίας ιδιότητας είναι δυνατόν να οριστεί τόσο στο επίπεδο αφαιρέσεων όσο και στο επίπεδο προσδιορισμού. Για παράδειγμα, η τιμή της ιδιότητας `att_Raw` μπορεί να οριστεί για τον τύπο δεδομένων `NetworkData` και στη συνέχεια να ισχύει για όλους τους τύπους δεδομένων που κληρονομούν χαρακτηριστικά από αυτόν. Υπάρχουν επίσης περιπτώσεις στις οποίες η τιμή πρέπει να καθορίζεται ρητά στο επίπεδο προσδιορισμού· μπορεί η ιδιότητα `att_NetworkAddress` να ορίζεται για τον τύπο μηχανών `NetworkInterface`, όμως η τιμή είναι μοναδική για κάθε μηχανή αυτού του τύπου. Έτσι, οι ιδιότητες διακρίνονται σε δύο κατηγορίες, ανάλογα με το επίπεδο στο οποίο ορίζονται οι τιμές τους. Οι ιδιότητες των οποίων οι τιμές ορίζονται ήδη από το επίπεδο αφαιρέσεων ονομάζονται *αμετάβλητες*

(*immutable attributes*), σε αντιδιαστολή με τις *μεταβλητές* ιδιότητες (*mutable attributes*), των οποίων οι τιμές μπορούν να οριστούν μόνο στο επίπεδο προσδιορισμού.

Τέλος, οι ιδιότητες είναι δυνατόν να κληρονομούνται από κάποια οντότητα προς άλλες, μέσω διαφόρων τύπων σχέσεων. Παρ' όλα αυτά, για την περίπτωση ιδιοτήτων που δεν θα πρέπει να μεταβιβάζονται, προβλέπεται μία σχετική boolean ιδιότητα που ορίζεται πάνω στην ίδια την ιδιότητα.

## 4.2 Ενέργειες και Οντότητες

Όλες οι προαναφερθείσες οντότητες συμμετέχουν αφενός στον προσδιορισμό διμερών συσχετισμών και, αφετέρου, στον ορισμό κανόνων ελέγχου πρόσβασης, οι οποίοι διέπουν την εκτέλεση και τους απαραίτητους μετασχηματισμούς του εκάστοτε συσχετισμού. Ως εκ τούτου, κεντρική θέση στην προτεινόμενη προσέγγιση κατέχει η έννοια της *Ενέργειας* (*Action*). Οι ενέργειες, εκτός του ότι αντανακλώνται στις εργασίες ενός διμερούς συσχετισμού, συνιστούν επίσης τον πυρήνα του ελέγχου πρόσβασης, καθώς στη βάση τους δομούνται οι κανόνες ελέγχου πρόσβασης, όπως θα περιγραφεί στη συνέχεια.

### 4.2.1 Ενέργεια

Έχει ήδη αναφερθεί ότι μία *ενέργεια* αντανακλά τη *λειτουργία* που εκτελείται από έναν *δράστη* σε κάποιον *πόρο*. Διαφορετικοί τύποι οντοτήτων μπορούν να αποτελέσουν δράστες, συμπεριλαμβανομένων ανθρώπων χρηστών και λειτουργικών υποσυστημάτων, ενώ παρομοίως, οι πόροι είναι δυνατόν να αναφέρονται σε διάφορες οντότητες, όπως είναι τα δεδομένα και οι περιέκτες λειτουργιών. Θεωρώντας τόσο το επίπεδο αφαιρέσεων όσο και το επίπεδο προσδιορισμού, οι δράστες και οι πόροι απαρτίζουν τα ακόλουθα αντίστοιχα σύνολα:

- *Actors* (*A*) = $R \cup Op \cup OpCT \cup U \cup OpI \cup OpC$
- *Resources* (*Res*) = $DT \cup Op \cup OpCT \cup R \cup MT \cup U \cup OpI \cup OpC \cup M \cup D$

Σε ό,τι αφορά τις οντότητες του επιπέδου προσδιορισμού, όταν αυτές παίζουν το ρόλο του δράστη ή του πόρου σε μία ενέργεια, αναφερόμαστε σε αυτές ως *υποκείμενα* και *αντικείμενα*, ορίζοντας έτσι τα αντίστοιχα σύνολα *Subjects* (*Subj*) και *Objects* (*Obj*).

Μία ενέργεια $act_i$ ορίζεται ως εξής:

**Ορισμός 1** Μία *ενέργεια* (*action*) $act_i \in Act$ είναι μία πλειάδα $\langle a_i, op_i, res_i, org \rangle$, όπου $act_i \in A$ ο δράστης, $op_i \in Op$ η λειτουργία, $res_i \in Res$ ο πόρος, και $org \in Org$ ο οργανισμός μέσα στον οποίο πραγματοποιείται μία ενέργεια.

Η έννοια του οργανισμού είναι ιδιαίτερης σημασίας στο πεδίο των κατανεμημένων περιβαλλόντων, καθώς οι διμερείς συσχετισμοί είναι δυνατόν να περιλαμβάνουν εργασίες που λαμβάνουν χώρα σε διαφορετικούς οργανισμούς και επομένως, κάθε ενέργεια πρέπει να συσχετίζεται με τον οργανισμό μέσα στον οποίο εκτελείται.

Σύμφωνα με τις ιεραρχικές σχέσεις των λειτουργιών *Op*, μία ενέργεια μπορεί να είναι είτε *ατομική*, είτε *σύνθετη*, ανάλογα με το αν η λειτουργία που περιλαμβάνεται στην ενέργεια μπορεί να αναλυθεί σε πιο στοιχειώδεις λειτουργίες ή όχι. Σε αυτό το σημείο θα πρέπει να τονιστεί ότι μία ενέργεια μπορεί να περιέχει οντότητες ορισμένες αποκλειστικά στο επίπεδο αφαιρέσεων ή στο επίπεδο προσδιορισμού. Ειδικά σε ό,τι αφορά τον ορισμό των κανόνων ελέγχου πρόσβασης και χρήσης στη βάση των ενεργειών, αυτό αποτελεί ένα καινοτόμο χαρακτηριστικό της παρούσας προσέγγισης, δεδομένου ότι οι υπάρχουσες προσεγγίσεις είτε χρησιμοποιούν αφαιρετικές δομές μόνο για το υποκείμενο, ακολουθώντας το παράδειγμα του RBAC [28], είτε επικεντρώνονται στην προδιαγραφή πολιτικών κάνοντας χρήση αποκλειστικά αφαιρετικών δομών. Η υβριδική προοπτική που προτείνει η εν λόγω προσέγγιση παρέχει ένα πλεονέκτημα έναντι των άλλων μοντέλων· αν και η χρήση αφαιρετικών δομών προσδίδει υψηλότερο βαθμό γενικότητας και επιτρέπει κοινή διαχείριση οντοτήτων που υπάγονται στον ίδιο σημασιολογικό τύπο, θα πρέπει να είναι δυνατόν οι περιορισμοί πρόσβασης να ορίζονται και πάνω σε οντότητες του επιπέδου προσδιορισμού. Θα πρέπει δηλαδή να υπάρχει η δυνατότητα οι ενέργειες και οι κανόνες να ανταποκρίνονται σε αιτήματα πρόσβασης που αφορούν τόσο το επίπεδο αφαιρέσεων όσο και το επίπεδο προσδιορισμού, καθώς η προδιαγραφή ενός διμερούς συσχετισμού μπορεί να αναφέρεται και στα δύο.

Ανάλογα με το επίπεδο αφαίρεσης, δηλαδή αφαιρέσεων ή προσδιορισμού, στο οποίο καθένα από τα τέσσερα στοιχεία της ενέργειας ορίζεται, υπάρχουν τελικά δεκαέξι διαφορετικοί δυνατοί συνδυασμοί για τον ορισμό μίας ενέργειας. Οι ενέργειες των οποίων όλα τα στοιχεία είναι ορισμένα στο επίπεδο αφαιρέσεων ονομάζονται *Αφηρημένες* (*Abstract Actions*), ενώ στην αντίθετη περίπτωση, όπου όλες οι οντότητες είναι ορισμένες στο επίπεδο προσδιορισμού, ονομάζονται *Συγκεκριμένες* (*Concrete Actions*). Οι υβριδικές ενέργειες που περιέχουν οντότητες και των δύο επιπέδων καλούνται *Ημι-Αφηρημένες* (*Semi-Abstract Actions*). Για παράδειγμα, μία ενέργεια μπορεί να αφορά στην εκτέλεση μίας λειτουργίας *op* από έναν συγκεκριμένο χρήστη *u* πάνω σε κάποιο δεδομένο του τύπου *dt* μέσα σε έναν οργανισμό *org*, δηλαδή, $act_i = \langle u, op, dt, org \rangle$, όπου $u \in U$, $op \in Op$, $dt \in DT$, $org \in Org$. Μία ακόμη περίπτωση που αναδεικνύει τη χρησιμότητα του συνδυασμού οντοτήτων ορισμένων σε διαφορετικά επίπεδα αφαίρεσης αφορά ενέργειες που αντιστοιχίζονται ρητά σε ένα συγκεκριμένο οργανισμό. Για παράδειγμα, οι εξουσιοδοτήσεις που ορίζονται για ένα ρόλο που εκτελεί μια λειτουργία σε κάποιο πόρο μπορεί να διαφέρουν ανάλογα με τον οργανισμό εντός του οποίου αυτή η ενέργεια λαμβάνει χώρα.

Επιπλέον, δεν είναι απαραίτητο να είναι σαφώς ορισμένα όλα τα πεδία μίας ενέργειας. Αυτό σημαίνει ότι μία ενέργεια μπορεί να ορίζεται μόνο μέσω μίας λειτουργίας,

ανεξάρτητα από τους δυνατούς δράστες και πόρους, ή μπορεί να περιλαμβάνει μόνο ένα δράστη και μία λειτουργία. Στην πραγματικότητα, για τον ορισμό μίας ενέργειας είναι αρκετή η συσχέτισή της με μία λειτουργία, αφήνοντας στο σύστημα τη συμπλήρωση των υπόλοιπων πεδίων, π.χ., συνδυασμών δραστών και πόρων που να έχουν νόημα για την εν λόγω λειτουργία. Αυτό αποδίδεται μέσω της πλειάδας $\langle *, op, *, * \rangle$, με το σύμβολο '$*$' να υποδεικνύει τα πεδία που θα συναχθούν μέσω συλλογιστικής με βάση τις προδιαγεγραμμένες εξουσιοδοτήσεις για την αντίστοιχη λειτουργία *op*. Σε κάθε περίπτωση, οι αμιγώς συγκεκριμένες ενέργειες προκύπτουν από αφηρημένες ή ημι-αφηρημένες σαν αποτέλεσμα μίας διαδικασίας τεχνικής βελτίωσης (refinement).

Στο επίπεδο του διμερούς συσχετισμού, μία εργασία αντανακλά μία ή περισσότερες ενέργειες. Λόγω των διαφορών που παρουσιάζουν οι εργασίες και οι ενέργειες στον ορισμό τους, στη γενική περίπτωση δεν είναι δυνατόν να υπάρξει ένα προς ένα αντιστοίχιση. Πρώτον, κάθε εργασία είναι δυνατόν να συσχετίζεται με περισσότερα του ενός προφίλ εκτέλεσης, τα οποία προσδιορίζουν τη λειτουργία στην οποία αναφέρεται η εργασία, τους δυνητικούς δράστες και τους δυνητικούς πόρους. Ακριβώς σε αυτήν τη δομή του προφίλ εκτέλεσης διαφαίνονται οι βασικές διαφορές που εμφανίζει η δομή της εργασίας σε σχέση με εκείνη της ενέργειας. Σε μία ενέργεια προβλέπεται μόνο ένας δράστης ή δράστες λογικά συσχετισμένοι μεταξύ τους με σχέση AND, ενώ στο προφίλ εκτέλεσης μίας εργασίας είναι δυνατόν να περιλαμβάνονται πολλαπλοί δράστες, εναλλακτικοί ή συμπληρωματικοί μεταξύ τους, με χρήση των αντίστοιχων λογικών σχέσεων. Ομοίως, λογικά συσχετισμένοι σε μία εργασία μπορεί να είναι και οι πόροι, ενώ σε μία ενέργεια ο πόρος είναι πάντα ένας, καθώς στα πλαίσια του ελέγχου πρόσβασης η πρόσβαση εξετάζεται πάντα αναφορικά με κάποιο συγκεκριμένο πόρο[10].

Τέλος, αντίστοιχα με τα worklets που παρουσιάστηκαν στην Ενότητα 4.1, σημειώνεται ότι και οι ενέργειες είναι δυνατόν να αποτελούν τμήματα άλλων δομών, οι οποίες περιγράφονται στην Ενότητα 4.3, όπου θα διαφανεί καλύτερα η σημασία τους για την προδιαγραφή περιορισμών στους κανόνες ελέγχου πρόσβασης.

### 4.2.2 Οντότητες Ενέργειας

Η δομή της ενέργειας ενσωματώνει περιορισμούς με βάση είτε τις ιδιότητες των οντοτήτων που την απαρτίζουν είτε τα υπο-στοιχεία αυτών των οντοτήτων (δηλαδή στοιχεία που σχετίζονται με την εκάστοτε οντότητα μέσω της σχέσης συμπερίληψης *isPartOf*), με χρήση εκφράσεων που περιγράφουν περαιτέρω το δράστη, τη λειτουργία, τον πόρο και τον οργανισμό. Σημειώνεται ότι οι περιορισμοί αυτοί είναι δυνατόν να ορίζονται ως λογικές εκφράσεις, κάνοντας χρήση των λογικών τελεστών AND, OR, NOT και XOR. Η ενσωμά-

[10]Εξαίρεση αποτελούν οι ενέργειες πρόσβασης και χρήσης που είναι συσχετισμένες με υποχρεώσεις που προέκυψαν από άλλες υποχρεώσεις μέσω κληρονομικότητας της σχέσης γενίκευσης-εξειδίκευσης (βλ. Ενότητα 4.4). Σε αυτήν την περίπτωση ενδέχεται οι οντότητες της ενέργειας να αναφέρονται σε λογικές δομές που αντανακλούν τη σχέση OR.

τωση των περιορισμών αυτού του είδους στις ενέργειες είναι ιδιαίτερης σημασίας, καθώς προσφέρουν τα μέσα για την επίτευξη ελέγχου πρόσβασης βάσει ιδιοτήτων [30]. Αν και θα μπορούσαν να μοντελοποιηθούν σαν περιορισμοί πλαισίου, θεωρήθηκε αναγκαίος ο διαχωρισμός των παραμέτρων πραγματικού χρόνου από περιορισμούς που αναφέρονται σε ιδιότητες. Οι συνθήκες πλαισίου εξάλλου αφορούν παράγοντες που δεν αποτελούν μέρος της προδιαγραφής μίας ενέργειας (π.χ., εξωγενείς παράμετροι περιβάλλοντος) ή που εκτείνονται πέραν των ορίων της ενέργειας και που, συνεπώς, δεν μπορούν να εκφραστούν αποκλειστικά στη βάση των ιδιοτήτων των εμπλεκόμενων οντοτήτων.

Έτσι, τα στοιχεία που συμμετέχουν σε μία ενέργεια και αναφέρονται στο επίπεδο αφαιρέσεων ορίζονται τελικά σαν *Διευρυμένες Οντότητες* (*Enhanced Entities*), οι οποίες περιλαμβάνουν, εκτός από το σημασιολογικό τύπο της οντότητας, εκφράσεις που περιορίζουν την εν λόγω οντότητα με βάση τις ιδιότητες που την χαρακτηρίζουν ή με βάση τα υποστοιχεία της. Ο μηχανισμός των διευρυμένων οντοτήτων βελτιώνει έτσι τον ορισμό μίας έννοιας, οδηγώντας στην περιγραφή περιορισμών βάσει ιδιοτήτων και στην προδιαγραφή ιδιαίτερα εκφραστικών κανόνων ελέγχου πρόσβασης. Ο τρόπος ορισμού των εν λόγω περιορισμών είναι παρεμφερής με την προσέγγιση που παρουσιάζεται στο [119].

**Ορισμός 2** Μία *διευρυμένη οντότητα* (*enhanced entity*) ορίζεται ως ένα ζεύγος ⟨*concept*, *constraint*⟩, όπου *concept* είναι ένα στοιχείο του Μοντέλου Πληροφοριών, και *constraint* είναι μια έκφραση που θέτει τιμές στις παραμέτρους του *concept* ή/και περιγράφει επιθυμητές ιδιότητες.

Σημειώνεται επίσης ότι ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί για να οριστεί ρητά ο πληθάριθμος (cardinality) των δηλωμένων δραστών, δηλαδή ο ακριβής αριθμός δραστών του ίδιου σημασιολογικού τύπου που πρόκειται να εκτελέσουν μία λειτουργία σε κάποιο πόρο. Για παράδειγμα, η έκφραση `Administrator(att_cardinality == 2)` υποδηλώνει ότι οι δράστες θα πρέπει να είναι δύο και να κατέχουν το ρόλο `Administrator`.

Για τις οντότητες που συμμετέχουν σε μία ενέργεια και αναφέρονται στο επίπεδο προσδιορισμού δεν έχει νόημα να οριστούν περιορισμοί˙ οι οντότητες αυτές αναφέρονται ως *Συγκεκριμένες Οντότητες* (*Concrete Entities*).

## 4.3 Κανόνες Ελέγχου Πρόσβασης και Χρήσης

Στην προτεινόμενη προσέγγιση, οι κανόνες χρησιμοποιούνται για τον ορισμό *Αδειών* (*Permissions*), *Απαγορεύσεων* (*Prohibitions*) και *Υποχρεώσεων* (*Obligations*). Καθώς οι κανόνες δομούνται με κεντρικό άξονα τις ενέργειες, ορίζονται και αυτοί με τη σειρά τους στα τρία επίπεδα αφαίρεσης (αφαιρέσεων, προσδιορισμού, συνδυασμός επιπέδων). Ο ορισμός των κανόνων στο υψηλότερο δυνατό επίπεδο αφαίρεσης επιτρέπει σημαντική μείωση του αριθμού των πολιτικών˙ ωστόσο, η αναπαράσταση των κανόνων στο επίπεδο προσδιορι-

σμού, όχι μόνο επιτρέπει τον ορισμό εξαιρέσεων, αλλά και διευκολύνει την εξαγωγή συμπερασμάτων όταν τα υπό εξέταση αιτήματα πρόσβασης αναφέρονται σε οντότητες και των δύο επιπέδων ή αποκλειστικά ορισμένες στο επίπεδο προσδιορισμού.

**Ορισμός 3** Ένας *κανόνας ελέγχου πρόσβασης* ορίζεται ως μία δομή:

$$\left.\begin{array}{l} Permission \\ Prohibition \\ Obligation \end{array}\right\} (pu, act, preAct, cont, postAct)$$

όπου, $act \in Act$ είναι η ενέργεια για την οποία ισχύει ο κανόνας, $pu \in Pu$ είναι ο σκοπός για τον οποίο η ενέργεια *act* επιτρέπεται/απαγορεύεται/επιβάλλεται να εκτελεστεί και $cont \in \mathcal{P}(Con)$ είναι μία δομή από παραμέτρους πλαισίου. Η ενέργεια $preAct \in Act$ αποτελεί μία δομή από ενέργειες που θα πρέπει να έχουν προηγηθεί (*προ-ενέργειες — preActions*) ώστε να εφαρμοστεί ο κανόνας ελέγχου πρόσβασης, ενώ το πεδίο $postAct \in Act$ αναφέρεται σε μία ή περισσότερες ενέργειες που θα πρέπει να εκτελεστούν μετά την εφαρμογή του κανόνα (*μετα-ενέργειες — postActions*).

Στη συνέχεια, παρουσιάζεται ενδεικτικά ένας κανόνας αυτής της μορφής, όπου μία ενέργεια η οποία αφορά την εκτέλεση μίας λειτουργίας *op* σε κάποιον πόρο *res* από έναν ρόλο $r_i$ αποκλείει την εκτέλεση της ίδιας λειτουργίας στον ίδιο πόρο από έναν δεύτερο ρόλο $r_j$, για κάποιο σκοπό *pu* και στα πλαίσια του ίδιου οργανισμού *org*, ανεξάρτητα από το τρέχον πλαίσιο και τις πιθανές μετα-ενέργειες:

- $Prohibition(pu, \langle r_j, op, res, org\rangle, \langle r_i, op, res, org\rangle, *, *)$

Σε αυτό το σημείο θα πρέπει να τονιστεί ότι η έννοια του οργανισμού δεν συμπεριλαμβάνεται στο σώμα του κανόνα, όπως π.χ. στην περίπτωση των OrBAC κανόνων [32]· αντ' αυτού, προσδιορίζεται −άμεσα ή έμμεσα− για την κάθε ενέργεια χωριστά. Έτσι, αν και ένας κανόνας αφορά την εκτέλεση κάποιας ενέργειας μέσα σε έναν οργανισμό, οι καθορισμένες προ- και μετα- ενέργειες μπορεί να λαμβάνουν χώρα στα πλαίσια της λειτουργίας άλλων οργανισμών. Με αυτόν τον τρόπο, αντιμετωπίζεται η ανάγκη για προσδιορισμό ενός ιδεατού δυναμικού οργανισμού (π.χ., [120]), κάθε φορά που ένας κανόνας αναφέρεται σε ενέργειες που εκτείνονται σε διαφορετικούς οργανισμούς. Επίσης, η ρητή συσχέτιση των κανόνων με τους σκοπούς αναδεικνύει την πολύ σημαντική για την ιδιωτικότητα έννοια του σκοπού.

Όπως αναφέρθηκε νωρίτερα, εκτός από μεμονωμένες ενέργειες, οι προ- και μετα-ενέργειες ενδέχεται να αναφέρονται σε δομές από ενέργειες. Έτσι, είναι δυνατόν να αποτελούνται από ενέργειες συνδεδεμένες μέσω λογικών τελεστών, συμπεριλαμβανομένης της άρνησης, δηλαδή $\neg preAct$, $\neg postAct$. Για παράδειγμα:

- $Permission(pu, act_n, act_1 \vee act_2 \vee ... \wedge act_{n-1}, *, act_{n+1} \wedge act_{n+2} \vee ... \wedge act_m)$,

εννοώντας ότι η ενέργεια $act_n$ επιτρέπεται εφόσον η σύνθετη ενέργεια $act_1 \vee act_2 \vee ... \wedge act_{n-1}$ έχει ήδη πραγματοποιηθεί, ενώ η εφαρμογή του κανόνα θα οδηγήσει στην εκτέλεση της σύνθετης ενέργειας $act_{n+1} \wedge act_{n+2} \vee ... \wedge act_m$.

Τέτοιου είδους λογικές δομές ενεργειών για τον προσδιορισμό των προ- και μετα-ενεργειών δεν περιλαμβάνουν περιορισμούς σχετικά με την αλληλουχία ή τον χρονισμό των εμπλεκόμενων ενεργειών, δηλαδή με αυτόν τον φορμαλισμό οι ενέργειες είναι δυνατόν να εκτελούνται με οποιαδήποτε σειρά. Ωστόσο, υπάρχουν περιπτώσεις όπου οι ενέργειες που συναπαρτίζουν κάποια προ-/μετα- ενέργεια θα πρέπει να εκτελούνται με συγκεκριμένη σειρά, ή να εκτελούνται ακολουθώντας κάποιο συγκεκριμένο πρότυπο. Συνεπώς, κρίνεται απαραίτητος ο ορισμός συμπληρωματικών τύπων δομικών προτύπων. Σε αυτήν την κατεύθυνση, χαρακτηρίζεται ως *Σκελετός* (*Skeleton*) κάθε δομή ενεργειών που θα πρέπει να εκτελούνται με συγκεκριμένη σειρά, ανεξάρτητα από το αν μεσολαβούν άλλες ενέργειες ανάμεσα στις ενέργειες του σκελετού. Μία τέτοια δομή δύναται να περιλαμβάνει κάθε πρότυπο ροής ελέγχου [121], όπως AND-split/AND-join ή XOR-split/XOR-join, ενώ όταν το μοναδικό πρότυπο ροής ελέγχου που χρησιμοποιείται είναι το *Πρότυπο Αλληλουχίας* (*Sequence Pattern*) [121], ο σκελετός χαρακτηρίζεται ως *Μονοπάτι* (*Path*). Επιπλέον, όταν οι ενέργειες που αποτελούν το σκελετό πρέπει να εκτελούνται χωρίς να παρεμβάλλονται άλλες ενέργειες, ο σκελετός χαρακτηρίζεται ως *κρίσιμος* (*critical*), σε αντίθεση με το *μη-κρίσιμο* (*non-critical*) σκελετό.

Από την άλλη πλευρά, είναι δυνατόν να υπάρχουν περιορισμοί σχετικά με το *πότε* εκτελείται κάποια προ-/μετα- ενέργεια σε σχέση με την ενέργεια για την οποία εφαρμόζεται ο κανόνας˙ μία προ-/μετα- ενέργεια χαρακτηρίζεται ως *αυστηρή* (*tight*), όταν πρέπει να εκτελείται αμέσως πριν ή μετά την ενέργεια πρόσβασης, δηλαδή χωρίς τη μεσολάβηση άλλων ενεργειών, και ως *χαλαρή* (*loose*), όταν δεν υφίστανται τέτοιοι περιορισμοί. Το ίδιο ισχύει και για τις ενέργειες που εκτελούνται παράλληλα. Οι απαιτήσεις αυτές καλύπτονται με την εισαγωγή του κατηγορήματος *isConstrainedToAct*, το οποίο επιτρέπει τον προσδιορισμό χρονικών περιορισμών και περιορισμών που αφορούν τη σειρά εκτέλεσης για τις προ- και μετα- ενέργειες έχοντας σαν σημείο αναφοράς την κύρια ενέργεια του κανόνα ελέγχου πρόσβασης. Πιο συγκεκριμένα, το εν λόγω κατηγόρημα ορίζεται ως εξής:

- *isConstrainedToAct*(*act*, *value*), όπου $act \in Act$ και αναφέρεται σε μία προ-ενέργεια ή σε μία μετα-ενέργεια, και το όρισμα *value* αντιστοιχεί στην τιμή του περιορισμού.

Ειδικά για τις προ-ενέργειες η τιμή μπορεί να είναι μία από τις `tight`, `before` ή `meet`. Η πρώτη αντιστοιχεί στον περιορισμό να μην παρεμβάλλεται άλλη ενέργεια ανάμεσα στην προ-ενέργεια και την ενέργεια πρόσβασης, η τιμή `before` δηλώνει ότι προ-ενέργεια θα πρέπει να έχει εκτελεστεί οποιαδήποτε στιγμή πριν από την εκτέλεση της κύριας ενέργειας, ενώ τέλος η τιμή `meet` σημαίνει ότι η λήξη της εκτέλεσης της προ-ενέργειας συμπίπτει με την έναρξη της κύριας ενέργειας και αποτελεί έναν αυστηρό χρονικό περιορισμό. Οι τιμές `tight`, `after` και `meet`, οι οποίες χρησιμοποιούνται στην περίπτωση των

μετα-ενεργειών, είναι σημασιολογικά αντίστοιχες των τιμών για τις προ-ενέργειες και θέτουν περιορισμούς στην εκτέλεση της εκάστοτε μετα-ενέργειας σε σχέση με την ενέργεια πρόσβασης. Υπάρχει επίσης η περίπτωση οι προ- και μετα- ενέργειες να πρέπει να εκτελούνται παράλληλα με την ενέργεια πρόσβασης. Σε αυτό το πλαίσιο, τόσο για τις προ- όσο και για τις μετα- ενέργειες, χρησιμοποιείται κάποια από τις τιμές `during`, `overlaps`, `begins` (οι ενέργειες ξεκινούν ταυτόχρονα), `finishes` (οι ενέργειες τελειώνουν ταυτόχρονα) και `equals` (η έναρξη και η λήξη των εν λόγω ενεργειών συμπίπτουν), ενώ ορίζονται επίσης και οι πιο γενικές τιμές `parallel` και `tightParallel`.

Τέλος, οι συγκεκριμένες εξουσιοδοτήσεις προκύπτουν από αφηρημένες ή ημι-αφηρημένες, ενώ μπορούν να οριστούν επίσης εξουσιοδοτήσεις κατευθείαν στο επίπεδο προσδιορισμού, π.χ., σαν εξαιρέσεις γενικών κανόνων. Μοντελοποιούνται μέσω των ακόλουθων κατηγορημάτων, όπου $subj \in Subj$ το συγκεκριμένο υποκείμενο, $op \in Op \cup OpI$ η συγκεκριμένη ή αφηρημένη λειτουργία[11] και $obj \in Obj$ το συγκεκριμένο αντικείμενο:

$$\left.\begin{array}{c} isPermitted \\ isProhibited \\ isObliged \end{array}\right\} (subj, op, obj)$$

## 4.4 Κληρονομικότητα των Εξουσιοδοτήσεων

Όπως έχει ήδη περιγραφεί, το μοντέλο πληροφοριών θεωρεί ιεραρχίες τύπων δεδομένων, ρόλων, λειτουργιών και σκοπών, μεταξύ άλλων, οι οποίες δημιουργούνται κυρίως λόγω της συσχέτισης εννοιών μέσω των σχέσεων *isA* και *isPartOf* (Πίνακας 3). Λόγω της κοινής σημασιολογίας που εμφανίζουν οι σχέσεις αυτές για όλους τους γράφους, εξετάζονται στη συνέχεια τα γενικά πρότυπα κληρονομικότητας αδειών, απαγορεύσεων και υποχρεώσεων που προκύπτουν για τις διαφορετικές ιεραρχίες των τύπων δεδομένων, ώστε να παρουσιαστεί επίσης το πρότυπο κληρονομικότητας που ισχύει για τη σχέση *lessDetailedThan*, η οποία συνδέει μόνο μέλη του συνόλου *DT*. Σημειώνεται ότι, καθώς το μοντέλο ελέγχου πρόσβασης περιλαμβάνει τόσο άδειες όσο και απαγορεύσεις, ενδέχεται οι εξουσιοδοτήσεις που κληρονομούνται κατά μήκος των ιεραρχιών να συγκρούονται με εκείνες που έχουν προσδιοριστεί με ρητό τρόπο και κατά συνέπεια να ακυρώνονται˙ σε κάθε περίπτωση, οι ρητά ορισμένες εξουσιοδοτήσεις έχουν υψηλότερη προτεραιότητα από εκείνες που προκύπτουν εμμέσως λόγω σχέσεων κληρονομικότητας (ενδέχεται, π.χ., να αποτελούν εξαιρέσεις), ενώ επίσης οι απαγορεύσεις υπερισχύουν των αδειών, όταν οι τελευταίες δεν αποτελούν εξαιρέσεις .

Η σχέση *inheritsFrom* συνάγεται από τις υπόλοιπες σχέσεις και αντανακλά την κληρονομικότητα των κανόνων. Συγκεκριμένα, οι σχέσεις *isA*, *isPartOf* και *lessDetailedThan* υπονοούν τη σχέση *inheritsFrom* ως ακολούθως, λαμβάνοντας υπόψη και τον τύπο της αντίστοι-

[11] Υπό την έννοια ότι λειτουργίες όπως οι `read` και `execute` δε συγκεκριμενοποιούνται περαιτέρω.

χης εξουσιοδότησης (αν πρόκειται, δηλαδή, για θετική ή αρνητική εξουσιοδότηση):

- $isA(dt_i, dt_j) \longrightarrow inheritsFrom(dt_i, dt_j)$: ισχύει τόσο για θετικές όσο και για αρνητικές εξουσιοδοτήσεις, δηλαδή, μία άδεια (αντίστοιχα, μία απαγόρευση) κληρονομείται από έναν πιο γενικό τύπο δεδομένων σε κάποιον πιο συγκεκριμένο.
- $isPartOf(dt_i, dt_j) \longrightarrow inheritsFrom(dt_i, dt_j)$: ισχύει για θετικές εξουσιοδοτήσεις, δηλαδή, εάν επιτρέπεται η πρόσβαση σε κάποιο σύνθετο τύπο δεδομένων, η άδεια μεταβιβάζεται σε όλους τους τύπους δεδομένων που τον απαρτίζουν.
- $isPartOf(dt_i, dt_j) \longrightarrow inheritsFrom(dt_j, dt_i)$: ισχύει για αρνητικές εξουσιοδοτήσεις, δηλαδή, εάν απαγορεύεται η πρόσβαση σε έστω έναν τύπο δεδομένων που περιέχεται σε κάποιο σύνθετο τύπο δεδομένων, η απαγόρευση ισχύει και για τον εν λόγω σύνθετο τύπο.
- $lessDetailedThan(dt_i, dt_j) \longrightarrow inheritsFrom(dt_i, dt_j)$: ισχύει για θετικές εξουσιοδοτήσεις, δηλαδή, μία άδεια για κάποιον πιο λεπτομερή τύπο δεδομένων υπονοεί τις αντίστοιχες άδειες για τους λιγότερο λεπτομερείς τύπους.
- $lessDetailedThan(dt_i, dt_j) \longrightarrow inheritsFrom(dt_j, dt_i)$: ισχύει για αρνητικές εξουσιοδοτήσεις, δηλαδή, εάν απαγορεύεται η πρόσβαση σε κάποιον τύπο δεδομένων ο οποίος είναι λιγότερο λεπτομερής από κάποιον άλλο, τότε απαγορεύεται η πρόσβαση και στον τελευταίο.

Πιο συγκεκριμένα, $\forall\ pu \in Pu, dt_i, dt_j \in DT, a \in A, op \in Op, orgt \in OrgT, cont \in Con, preAct, postAct \in Act$:

- $Permission(pu, \langle a, op, dt_i, orgt\rangle, preAct, cont, postAct) \wedge isA(dt_j, dt_i) \longrightarrow$
  $Permission(pu, \langle a, op, dt_j, orgt\rangle, preAct, cont, postAct)$
- $Prohibition(pu, \langle a, op, dt_i, orgt\rangle, preAct, cont, postAct) \wedge isA(dt_j, dt_i) \longrightarrow$
  $Prohibition(pu, \langle a, op, dt_j, orgt\rangle, preAct, cont, postAct)$
- $Permission(pu, \langle a, op, dt_i, orgt\rangle, preAct, cont, postAct) \wedge isPartOf(dt_j, dt_i) \longrightarrow$
  $Permission(pu, \langle a, op, dt_j, orgt\rangle, preAct, cont, postAct)$
- $Prohibition(pu, \langle a, op, dt_j, orgt\rangle, preAct, cont, postAct) \wedge isPartOf(dt_j, dt_i) \longrightarrow$
  $Prohibition(pu, \langle a, op, dt_i, orgt\rangle, preAct, cont, postAct)$
- $Permission(pu, \langle a, op, dt_i, orgt\rangle, preAct, cont, postAct) \wedge lessDetailedThan(dt_j, dt_i) \longrightarrow$
  $Permission(pu, \langle a, op, dt_j, orgt\rangle, preAct, cont, postAct)$
- $Prohibition(pu, \langle a, op, dt_j, orgt\rangle, preAct, cont, postAct) \wedge lessDetailedThan(dt_j, dt_i) \longrightarrow$
  $Prohibition(pu, \langle a, op, dt_i, orgt\rangle, preAct, cont, postAct)$

Σημειώνεται ότι οι υποχρεώσεις ακολουθούν τα ίδια πρότυπα κληρονομικότητας με τις άδειες. Ωστόσο, ειδικά σε ό,τι αφορά την κληρονομικότητα μέσω της σχέσης γενίκευσης-ειδίκευσης *isA*, μία υποχρέωση ορισμένη για κάποια γενική έννοια, στην οποία αναφέρεται κάποια από τις οντότητες της ενέργειας πρόσβασης/χρήσης, οδηγεί στη δημιουργία μίας μοναδικής μετα-υποχρέωσης, όπου η γενική έννοια αντικαθίσταται από τις εναλλακτικές μεταξύ τους πιο εξειδικευμένες έννοιες, δηλαδή από τις εν λόγω έννοιες λογικά συσχετισμένες μεταξύ τους με σχέση OR. Δηλαδή:

- $Obligation(pu, \langle a, op, dt_i, orgt\rangle, preAct, cont, postAct) \wedge isA(dt_j, dt_i) \wedge isA(dt_k, dt_i) \longrightarrow$
  $Obligation(pu, \langle a, op, dt_j \vee dt_k, orgt\rangle, preAct, cont, postAct)$

Η εξαγωγή *n* υποχρεώσεων για *n* πιο εξειδικευμένες έννοιες θα σήμαινε ότι θα έπρεπε να εκτελεστούν όλες οι πιο εξειδικευμένες ενέργειες πρόσβασης/χρήσης κάτω από τις ίδιες συνθήκες, ενώ η αρχική υποχρέωση υπαγορεύει την εκτέλεση τουλάχιστον μίας από τις εναλλακτικές ενέργειες για την ικανοποίηση του κανόνα. Το συγκεκριμένο πρότυπο κληρονομικότητας για την περίπτωση των υποχρεώσεων οδηγεί στη συμπερίληψη στη δομή της ενέργειας λογικά συσχετισμένων δραστών, λειτουργιών ή/και πόρων που όμως είναι πάντα εναλλακτικοί μεταξύ τους. Τέτοιες ενέργειες είναι δυνατόν να προκύψουν μόνο μέσω κληρονομικότητας και είναι πάντα συσχετισμένες με κάποια μετα-υποχρέωση. Οι ενέργειες που ορίζονται ρητά σε κάθε περίπτωση περιλαμβάνουν έναν ή περισσότερους συμπληρωματικούς μεταξύ τους δράστες, ακριβώς μία λειτουργία και ακριβώς έναν πόρο. Σημειώνεται ότι για την περίπτωση της κληρονομικότητας μέσω της σχέσης συμπερίληψης, κάθε τέτοια σχέση οδηγεί στη δημιουργία μίας μετα-υποχρέωσης.

Κληρονομικότητα των εξουσιοδοτήσεων θεωρείται επίσης μεταξύ των διαφόρων γράφων του Μοντέλου Πληροφοριών. Για παράδειγμα, οι άδειες που αφορούν τύπους περιεκτών λειτουργιών επηρεάζουν επίσης τις προσφερόμενες λειτουργίες, ενώ το ίδιο ισχύει και στην περίπτωση των εξουσιοδοτήσεων που προσδιορίζονται για έναν τύπο μηχανής, οι οποίες, κατά συνέπεια, μεταβιβάζονται σε λειτουργίες μέσω των περιεκτών λειτουργιών που τις προσφέρουν. Έτσι, $\forall\, pu \in Pu, a \in A, op, op_i, op_j, op_k, op_l \in Op, opct \in OpCT, orgt \in OrgT, cont \in Con, preAct, postAct \in Act$:

- $Permission(pu, \langle a, op, opct, orgt\rangle, preAct, cont, postAct) \wedge$
  $providesOperations(opct, \{op_i, op_j\}) \wedge$
  $isPartOf(op_k, op_i) \wedge$
  $isPartOf(op_l, op_i) \longrightarrow$
  $Permission(pu, \langle a, op, op_i, orgt\rangle, preAct, cont, postAct) \wedge$
  $Permission(pu, \langle a, op, op_j, orgt\rangle, preAct, cont, postAct) \wedge$
  $Permission(pu, \langle a, op, op_k, orgt\rangle, preAct, cont, postAct) \wedge$
  $Permission(pu, \langle a, op, op_l, orgt\rangle, preAct, cont, postAct)$

Στο ίδιο πλαίσιο, $\forall\ pu \in Pu$, $a \in A$, $op, \in Op$, $mt \in MT$, $opct_i$, $opct_j \in OpCT$, $orgt \in OrgT$, $cont \in Con$, $preAct$, $postAct \in Act$:

- $Permission(pu, \langle a, op, mt, orgt\rangle, preAct, cont, postAct) \wedge$
  $hostsContainers(mt, \{opct_i, opct_j\}) \longrightarrow$
  $Permission(pu, \langle a, op, opct_i, orgt\rangle, preAct, cont, postAct) \wedge$
  $Permission(pu, \langle a, op, opct_j, orgt\rangle, preAct, cont, postAct)$

Ο τρόπος με τον οποίο μεταβιβάζονται οι εξουσιοδοτήσεις από τους τύπους μηχανών στις λειτουργίες προκύπτει από το συνδυασμό των δύο προηγούμενων κανόνων.

## 4.5 Διαχωρισμός και Σύζευξη Καθηκόντων

Αναφορικά με τους περιορισμούς διαχωρισμού καθηκόντων, πρέπει να σημειωθεί ότι η προτεινόμενη προσέγγιση εισάγει σημαντική ευελιξία και εκφραστικότητα στον ορισμό τους, καθώς δεν εστιάζει σε περιορισμούς που σχετίζονται μόνο με το ρόλο ή το χρήστη, αλλά επεκτείνει την έννοια του διαχωρισμού σε όλα τα στοιχεία που συνθέτουν μία ενέργεια, δηλαδή τους δράστες, τις λειτουργίες, τους πόρους και τους οργανισμούς. Σαν αποτέλεσμα, οι περιορισμοί διαχωρισμού καθηκόντων στο προτεινόμενο μοντέλο ουσιαστικά αφορούν αμοιβαίως αποκλειόμενες ενέργειες. Το ίδιο ισχύει και για τους περιορισμούς σύζευξης καθηκόντων.

Η χρήση της έννοιας της ενέργειας για την προδιαγραφή SoD και BoD περιορισμών αποτελεί στην ουσία ένα συνδυασμό των προσεγγίσεων διαχωρισμού και σύζευξης *Βασισμένων σε Εργασίες* (*Task-Based*) [122] και *Βασισμένων στο Ιστορικό Πρόσβασης* (*History-Based*) [123]. Επίσης, οι περιορισμοί μπορεί είτε να ορίζονται στα πλαίσια ενός διμερούς συσχετισμού είτε να είναι τελείως ανεξάρτητοι από αυτόν. Τέλος, ο ορισμός τους ευνοείται ιδιαίτερα από τη δομή των κανόνων˙ οι ίδιοι οι κανόνες χρησιμοποιούνται για να εκφραστούν τέτοιου είδους περιορισμοί, μέσω των πεδίων *act*, *preAct* και *postAct*, ενώ και οι παράμετροι πλαισίου προσδίδουν δυναμικότητα.

Για παράδειγμα, ένας περιορισμός δυναμικού διαχωρισμού καθηκόντων είναι δυνατόν να οριστεί μέσω της ακόλουθης απαγόρευσης, όπου οι ενέργειες *act* και *preAct* περιέχουν τα αμοιβαίως αποκλειόμενα στοιχεία υπό τη συνθήκη πλαισίου *cont*:

- $Prohibition(*, act, preAct, cont, *)$

Από την άλλη πλευρά, ένας περιορισμός BoD ορίζεται ως μία άδεια που λειτουργεί σαν θετική εξαίρεση κάποιας προκαθορισμένης απαγόρευσης, περιορίζοντας την άδεια μέσω μίας προ-ενέργειας. Δηλαδή, για τη σύζευξη των στοιχείων δύο ενεργειών *act* και *preAct*, ο κανόνας που χρησιμοποιείται είναι ο εξής:

- *Permission*($*$, *act*, *preAct*, $*$, $*$)

Σημειώνεται ότι οι προηγούμενοι κανόνες δεν αποτελούν το μοναδικό τρόπο για την προδιαγραφή κάποιου BoD ή SoD περιορισμού˙ στην πραγματικότητα, υπάρχουν διάφοροι εναλλακτικοί τρόποι ώστε να εκφραστούν τέτοιοι περιορισμοί.

Ο επόμενος κανόνας περιορίζει έναν χρήστη σε ό,τι αφορά την εκτέλεση της λειτουργίας $op_i$ πάνω σε κάποιον πόρο *res*, εάν ο ίδιο χρήστης έχει εκτελέσει οποιαδήποτε λειτουργία (δηλαδή, ακόμα και την ίδια) πάνω στον ίδιο πόρο στο ιστορικό του συστήματος:

- *Prohibition*($*$, $\langle u, op_i, res\rangle$, $\langle u, *, res\rangle$, $*$, $*$)

Ένας SoD ή BoD περιορισμός είναι δυνατόν να υπόκειται σε όλες τις πιθανές παραμέτρους πλαισίου. Για παράδειγμα, ένας SoD ή BoD περιορισμός μπορεί να ισχύει "για 24 ώρες", ενώ επίσης σημειώνεται ότι οι ενέργειες που συμμετέχουν στον ορισμό τέτοιων περιορισμών μπορεί να σχηματίζουν δομές ενεργειών, όπως *σκελετούς* (βλ. Ενότητα 4.3).

Τέλος, SSoD περιορισμοί προσδιορίζονται μέσω του κατηγορήματος *disjointWith*, το οποίο για την περίπτωση των ρόλων εκφράζεται ως εξής:

- *disjointWith*($r_i$, $r_j$), το οποίο μεταφράζεται ως
  *assignedWithRoles*($u$, $r_i$) $\longrightarrow$ $\neg$*assignedWithRoles*($u$, $r_j$), όπου $r_i$, $r_j \in R$ και $u \in R$.

Παρ' όλα αυτά, εκτός από αυτήν την τυπική περίπτωση στατικού διαχωρισμού των ρόλων, το ίδιο κατηγόρημα μπορεί να χρησιμοποιηθεί για όλες τις έννοιες του επιπέδου αφαιρέσεων του μοντέλου πληροφοριών. Για παράδειγμα, το ακόλουθο κατηγόρημα αποκλείει μια μηχανή από το να έχει δύο τύπους $mt_i$ και $mt_j$ ταυτόχρονα:

- *disjointWith*($mt_i$, $mt_j$), το οποίο μεταφράζεται ως
  *isOfMachineType*($m$, $mt_i$) $\longrightarrow$ $\neg$*isOfMachineType*($m$, $mt_j$), όπου $mt_i$, $mt_j \in MT$ και $m \in M$.

# Κεφάλαιο 5

# Οντολογική Υλοποίηση του Μοντέλου Ελέγχου Πρόσβασης και Χρήσης

Το Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης και Χρήσης [124] αποτελεί ένα ενιαίο σύστημα για το φορμαλιστικό ορισμό των κανόνων που διέπουν τη λειτουργία του υποκείμενου συστήματος και αποτελεί τη γνωσιακή βάση για την εξαγωγή συμπερασμάτων και τη λήψη αποφάσεων. Για την υλοποίηση του μοντέλου, όπως αυτό προδιαγράφηκε στο προηγούμενο κεφάλαιο, η προσέγγιση που υιοθετήθηκε είναι η χρήση οντολογιών, λόγω της υψηλής πολυπλοκότητας και της εκφραστικότητας του υποκείμενου μοντέλου. Πράγματι, η χρήση οντολογιών επιτρέπει τον ορισμό πολύπλοκων δομών και κανόνων, ενώ παρουσιάζει διάφορα πλεονεκτήματα, όπως οι δυνατότητες εξαγωγής λογικών συμπερασμάτων, συμπεριλαμβανομένης γνώσης που δεν περιέχεται ρητά στην οντολογία, η δυνατότητα αξιολόγησης των κανόνων ως προς τη συνέπειά τους και η δυνατότητα ολοκλήρωσης με άλλα σημασιολογικά μοντέλα τα οποία περιγράφουν συμπληρωματικές έννοιες. Σημειώνεται ότι καθώς και το μοντέλο προδιαγραφής ροών εργασιών στη βάση του οποίου ορίζεται ο διμερής συσχετισμός υλοποιείται με χρήση οντολογίας, η οντολογική υλοποίηση του μοντέλου ελέγχου πρόσβασης επιτρέπει την αποτελεσματική ολοκλήρωσή τους.

Για την υλοποίηση της οντολογίας χρησιμοποιήθηκε η διαδεδομένη γλώσσα Web Ontology Language (OWL) [63]. Οι έννοιες του επιπέδου αφαιρέσεων συνιστούν οντολογικές κλάσεις, ενώ τα στοιχεία τους ορίζονται ως οντολογικά στιγμιότυπα (instances). Όλες οι συσχετίσεις μεταξύ των οντολογικών στιγμιοτύπων εκφράζονται ως αντικειμενικές ιδιότητες (object properties) της γλώσσας OWL, ενώ χρησιμοποιούνται επίσης ιδιότητες τύπου δεδομένων (datatype properties) για τον ορισμό άλλων ιδιοτήτων.

Το Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης και Χρήσης αποτελείται από το

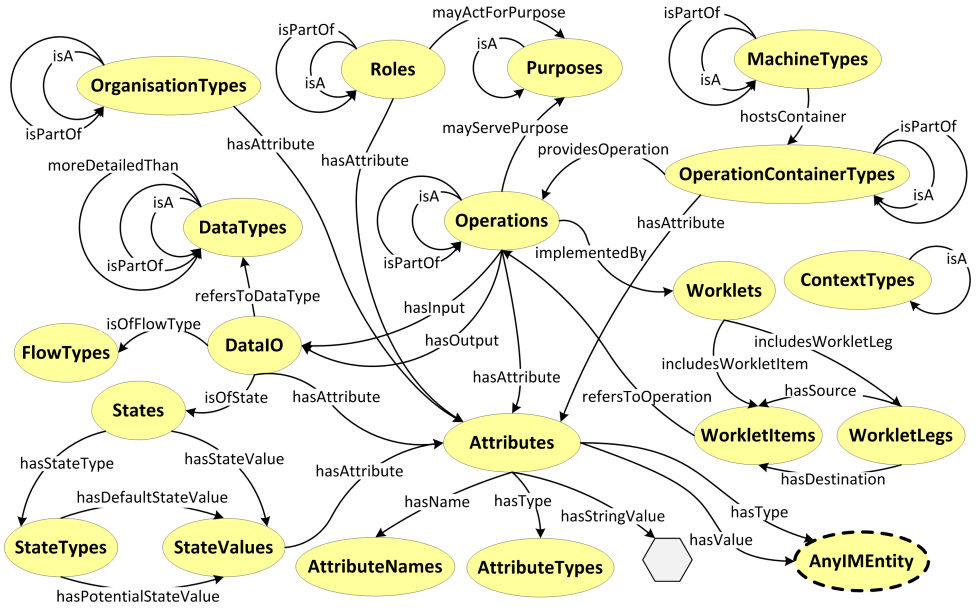
Σημασιολογικό Μοντέλο Πληροφοριών, το οποίο περιγράφεται στην Ενότητα 5.1, και το Σημασιολογικό Μοντέλο Πολιτικών, το οποίο χρησιμοποιείται για τη φορμαλιστική περιγραφή των κανόνων και παρουσιάζεται στην Ενότητα 5.2.

## 5.1 Σημασιολογικό Μοντέλο Πληροφοριών

Το Σχήμα 6 προσφέρει μία επισκόπηση του Σημασιολογικού Μοντέλου Πληροφοριών (Information Model Ontology — IMO). Όπως φαίνεται, όλες οι έννοιες του επιπέδου αφαιρέσεων που παρουσιάστηκαν στην Ενότητα 4.1 και συνοψίστηκαν στον Πίνακα 2 συνιστούν οντολογικές κλάσεις, οι οποίες χαρακτηρίζονται από ενδοσυσχετίσεις (intra-class relations) και συσχετίσεις με άλλες κλάσεις (inter-class relations), υλοποιημένες σαν αντικειμενικές ιδιότητες της γλώσσας OWL. Οι ενδοσυσχετίσεις υλοποιούν σχέσεις μεταξύ μελών της ίδιας κλάσης, με βασικότερες τις `isA`, `isPartOf` και `moreDetailedThan` (όπως παρουσιάστηκαν στον Πίνακα 3), οι οποίες μαζί με τις αντίστροφές[12] τους ουσιαστικά σχηματίζουν AND και OR ιεραρχίες, καθιστώντας έτσι δυνατή τη μεταβίβαση κανόνων και ιδιοτήτων, καθώς και τον προσδιορισμό εξαρτήσεων. Όπως έχει ήδη αναφερθεί, οι αντικειμενικές ιδιότητες `isA` και `isPartOf` περιγράφουν, αντίστοιχα, την εξειδίκευση μίας έννοιας και τη συμπερίληψη μίας οντότητας σε κάποια άλλη, ενώ η κλάση `DataTypes` χαρακτηρίζεται επιπλέον από την ιδιότητα `moreDetailedThan`, η οποία αντανακλά μία μερική διάταξη των τύπων δεδομένων ανάλογα με το βαθμό λεπτομέρειας. Από την άλλη πλευρά, οι συσχετίσεις μεταξύ στιγμιοτύπων που ανήκουν σε διαφορετικές κλάσεις χρησιμεύουν σε περιπτώσεις όπως αυτή της συσχέτισης μεταξύ ενός ρόλου κι ενός σκοπού μέσω της ιδιότητας `mayActForPurpose`, η οποία υποδεικνύει τους σκοπούς για τους οποίους μπορεί να δράσει ένας ρόλος, της συσχέτισης μεταξύ στιγμιοτύπων και ιδιοτήτων (`hasAttribute`), ή για τον προσδιορισμό των δεδομένων εισόδου και εξόδου μίας λειτουργίας (`hasInput` και `hasOutput`, αντίστοιχα).

Οι περισσότερες από τις κλάσεις και τις σχέσεις που περιλαμβάνονται στο Σημασιολογικό Μοντέλο Πληροφοριών περιγράφονται επαρκώς από το Σχήμα 6 σε συνδυασμό με την ανάλυση που πραγματοποιήθηκε στην Ενότητα 4.1, ωστόσο για κάποιες κρίνεται απαραίτητη περαιτέρω επεξήγηση. Έτσι, για τον πλήρη ορισμό ενός στιγμιότυπου της κλάσης `Attributes`, το εν λόγω στιγμιότυπο συσχετίζεται με ένα αναγνωριστικό (στιγμιότυπο της βοηθητικής κλάσης `AttributeNames`), με έναν τύπο, ο οποίος μπορεί να είναι κάποιος συνήθης τύπος, όπως, π.χ., `Integer`, και να αποτελεί στιγμιότυπο της κλάσης `AttributeTypes`, ή κάποια άλλη οντότητα του Σημασιολογικού Μοντέλου Πληροφοριών, και τέλος, προαιρετικά με μία τιμή, η οποία μπορεί να είναι ένα οντολογικό στοιχείο, ή μία αυθαίρετη συμβολοσειρά. Για αυτήν την τελευταία προαιρετική συσχέτιση, χρησιμοποιούνται η αντικειμενική ιδιότητα `hasValue` ή η ιδιότητα τύπου δεδομένων `hasStringValue`,

[12]Οι αντίστροφες ιδιότητες ορίζονται ρητά για όλες τις αντικειμενικές ιδιότητες της οντολογίας, με σκοπό να διευκολύνουν την πλοήγηση από ένα οντολογικό στοιχείο προς κάποιο άλλο.




Σχήμα 6: Σημασιολογικό Μοντέλο Πληροφοριών (Information Model Ontology — IMO).

αντίστοιχα. Σημειώνεται ότι μία ιδιότητα με προσδιορισμένη τιμή θεωρείται αμετάβλητη (immutable), σε αντίθεση με τις μεταβλητές (mutable) ιδιότητες οι οποίες είναι δυνατόν να καθοριστούν κατά την εκτέλεση. Τέλος, για την ανάθεση ιδιοτήτων σε κάποιο στιγμιότυπο γίνεται χρήση της αντικειμενικής ιδιότητας `hasAttribute`.

Η κλάση `DataIO` ορίζεται με τα στιγμιότυπά της να αποτελούν δυνητικές εισόδους και εξόδους λειτουργιών. Σημειώνεται ότι η σύνδεση των λειτουργιών με τους τύπους δεδομένων που μπορούν να λάβουν σαν είσοδο ή να δώσουν σαν έξοδο δε γίνεται απευθείας (με την έννοια ότι δεν ορίζεται κάποια αντικειμενική ιδιότητα που να συνδέει τις λειτουργίες με τους τύπους δεδομένων), αλλά επιλέχθηκε η σύνδεση μέσω της βοηθητικής κλάσης `DataIO`, η οποία, εκτός από τις ιδιότητες που χαρακτηρίζουν την είσοδο/έξοδο, επιπλέον εμπεριέχει πληροφορία σχετική με τον *τύπο ροής* (*flow type*), δηλαδή αν η λειτουργία λαμβάνει δεδομένα με ασύγχρονο τρόπο (control flow), όπως δεδομένα ελέγχου, ή συνεχή ροή δεδομένων (data flow), και την *κατάσταση* (*state*) των δεδομένων, π.χ., εάν τα δεδομένα εξόδου μίας λειτουργίας είναι κρυπτογραφημένα. Έτσι, τα στιγμιότυπα της κλάσης `States` αντανακλούν ουσιαστικά το αποτέλεσμα που έχει η εκτέλεση μίας λειτουργίας πάνω στα δεδομένα που λαμβάνει και χαρακτηρίζονται από έναν τύπο (στιγμιότυπο της κλάσης `StateTypes`) και μία τιμή (στιγμιότυπο της κλάσης `StateValues`). Η πληροφορία που αφορά την κατάσταση των δεδομένων είναι πολύ σημαντική για την εφαρμογή ελέγχου πρόσβασης στο πλαίσιο της επαλήθευσης ενός διμερούς συσχετισμού, καθώς ενδέχεται να οδηγήσει σε μετασχηματισμό της προκαθορισμένης ροής δεδομένων (βλ. Ενότητα 7.5.2).

Τα στιγμιότυπα της κλάσης `Worklet` περιγράφουν αναλυτικά πώς υλοποιείται μία σύνθετη λειτουργία από πιο στοιχειώδεις λειτουργίες. Οι τελευταίες συνδέονται με ένα worklet έμμεσα, μέσω της κλάσης `WorkletItems`, ενώ οι συσχετίσεις μεταξύ των λειτουρ-

γιών (με κύρια την ακριβή σειρά εκτέλεσης) περιγράφονται από στιγμιότυπα της κλάσης `WorkletLegs`. Η συσχέτιση μίας λειτουργίας με κάποιο worklet που την υλοποιεί πραγματοποιείται με χρήση της αντικειμενικής ιδιότητας `implementedBy`.

Τέλος, σημειώνεται ότι η ρίζα του κάθε γράφου της οντολογίας αντανακλά την οντότητα από την οποία κληρονομούν χαρακτηριστικά και εξουσιοδοτήσεις όλα τα υπόλοιπα στοιχεία του γράφου, δηλαδή την πιο στοιχειώδη οντότητα, π.χ., `anyUser` στην περίπτωση της κλάσης `Roles`, `anyData` στην περίπτωση της κλάσης `DataTypes`, κ.ο.κ.. Επίσης, κάθε φορά που κάποια οντότητα συνδέεται με κάποια άλλη μέσω κάποιας από τις αντικειμενικές ιδιότητες `isA`, `isPartOf`, `moreDetailedThan` και τις αντίστροφές τους, συνεπάγεται ότι η πρώτη συνδέεται τελικά και με τις οντότητες που έχουν συσχετιστεί με τη δεύτερη.

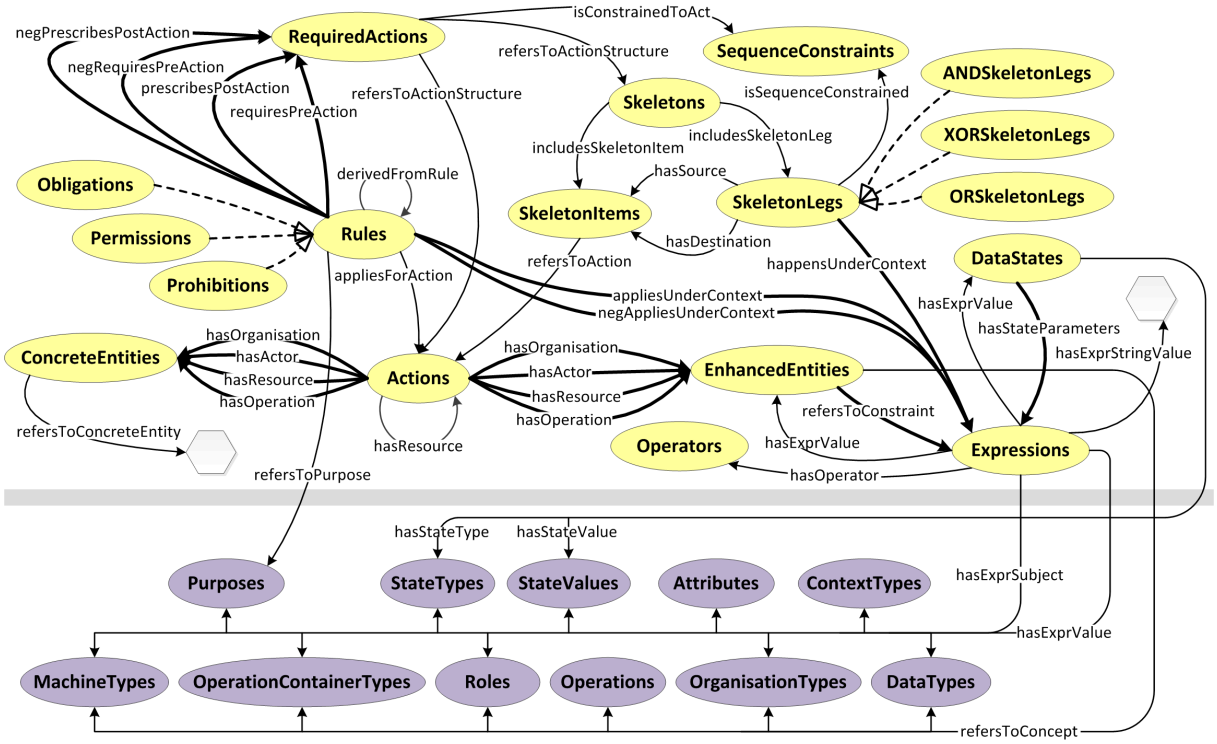
## 5.2 Σημασιολογικό Μοντέλο Πολιτικών

Το Σχήμα 7 παρουσιάζει το Σημασιολογικό Μοντέλο Πολιτικών (Policy Model Ontology — PMO), μέσω του οποίου προδιαγράφονται οι κανόνες ελέγχου πρόσβασης. Οι κύριες πτυχές του αναλύονται στις ενότητες που ακολουθούν. Επιπλέον, το Σχήμα 8 απεικονίζει την οντολογική αναπαράσταση ενός κανόνα εμπνευσμένου από τις κατευθυντήριες οδηγίες για τον τομέα της υγείας [125]: *"Για το σκοπό της ιατρικής έρευνας και στο πλαίσιο ενός εν εξελίξει R&D έργου, ένας στατιστικολόγος επιτρέπεται να πραγματοποιήσει στατιστική ανάλυση σε ταυτοποιήσιμα ιατρικά αρχεία του ασθενούς, αν ο εν λόγω ασθενής έχει συναινέσει σχετικά. Για να καθίσταται δυνατή η απόδοση ευθυνών, η ενέργεια πρόσβασης θα πρέπει αμέσως να καταγράφεται"*. Το παράδειγμα αυτό θα χρησιμοποιηθεί στο παρόν κεφάλαιο για την επεξήγηση των κύριων χαρακτηριστικών της προτεινόμενης προσέγγισης.

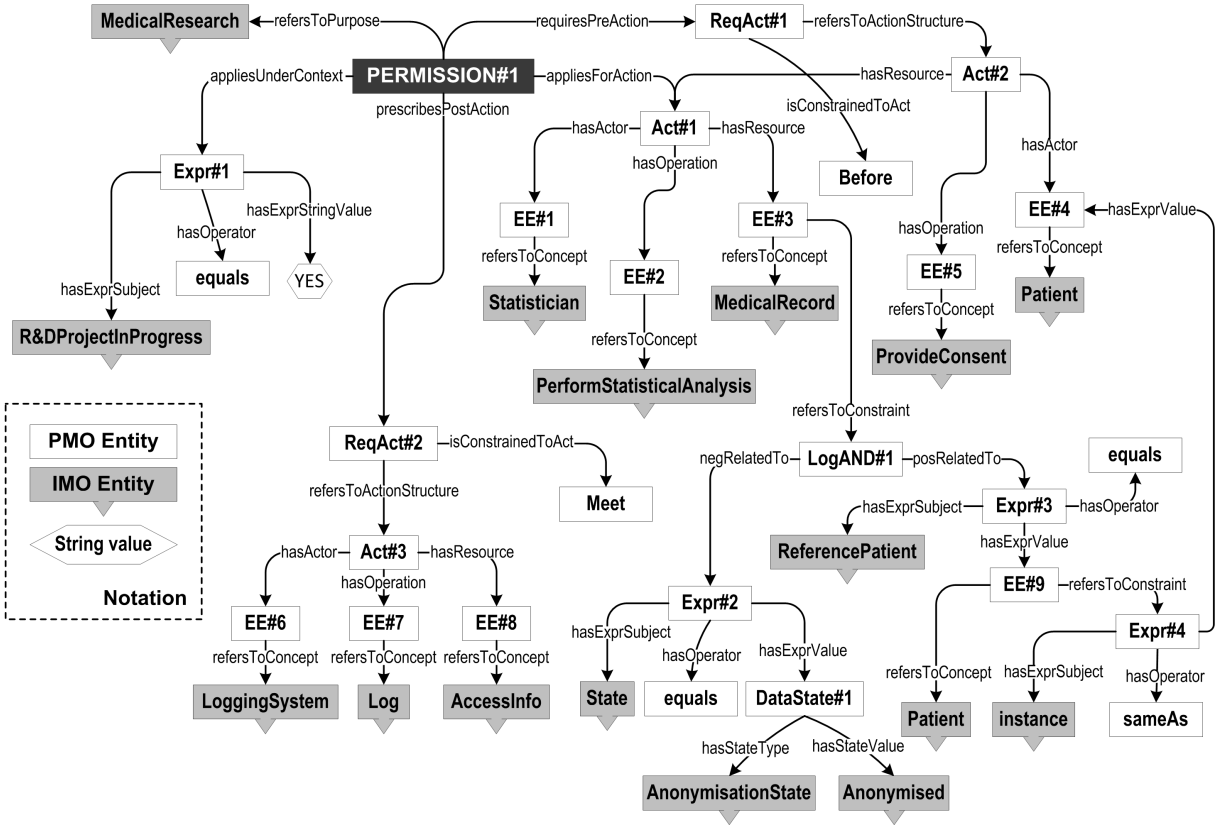
### 5.2.1 Εκφράσεις και Λογικές Σχέσεις

Ένα από τα κύρια χαρακτηριστικά της προτεινόμενης προσέγγισης αποτελεί η υψηλή εκφραστικότητα που προσφέρει. Στο πλαίσιο αυτό, δύο σημαντικά εργαλεία για τη λεπτομερή σημασιολογική περιγραφή των εμπλεκόμενων εννοιών είναι οι *εκφράσεις* (*expressions*) και οι *λογικές σχέσεις* (*logical relations*).

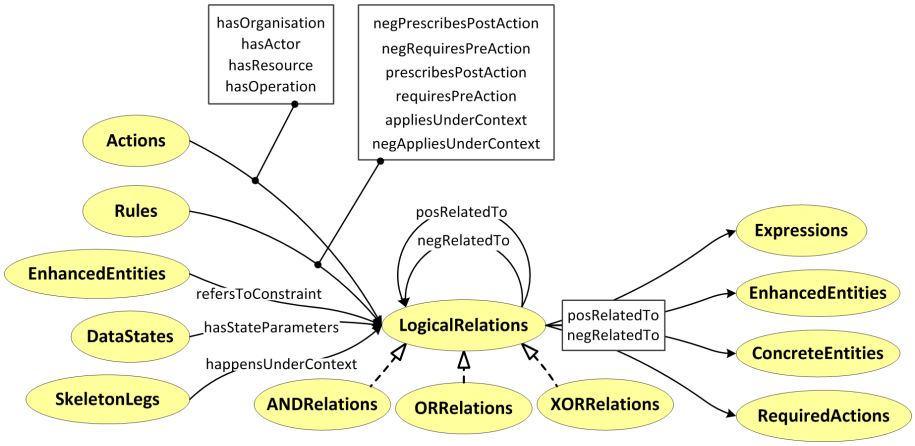
Οι λογικές σχέσεις επιτρέπουν τον ορισμό λογικών δομών εννοιών μεταξύ ομοειδών εννοιών. Για παράδειγμα, ένας κανόνας είναι δυνατόν να απαιτεί την από κοινού εκτέλεση διαφορετικών μετα-ενεργειών (σχέση σύζευξης — AND) , την εκτέλεση τουλάχιστον μίας προ-ενέργειας μεταξύ διάφορων εναλλακτικών (σχέση περιεκτικής διάζευξης — OR), ή την εκτέλεση το πολύ μίας από ένα σύνολο αμοιβαίως αποκλειόμενων προ-ενεργειών (σχέση αποκλειστικής διάζευξης — XOR). Οι τελεστές αυτοί είναι δυνατόν να συνδυάζονται ώστε να σχηματίζουν πολύπλοκες λογικές εκφράσεις. Μία λογική σχέση ορίζεται ως εξής:




Σχήμα 7: Σημασιολογικό Μοντέλο Πολιτικών (Policy Model Ontology — PMO).




Σχήμα 8: Παράδειγμα Οντολογικού Κανόνα Ελέγχου Πρόσβασης και Χρήσης




Σχήμα 9: Λογικές Σχέσεις

**Ορισμός 4** Έστω ότι $\mathcal{F}$ είναι η κλάση όλων των λειτουργιών σε ένα σύνολο $S$, έτσι ώστε κάθε $\phi_i(V) \in \mathcal{F}$ να είναι μία καλά σχηματισμένη δομή, η οποία είναι δυνατόν να περιλαμβάνει έναν ή περισσότερους από τους $n$-αδικούς τελεστές AND, OR και XOR, το μοναδιαίο τελεστή NOT, και ένα σύνολο μεταβλητών $V$. Μία *λογική σχέση* είναι μία λογική δομή $\phi(S')$, έτσι ώστε $\phi \in \mathcal{F}$ και $S' \subseteq S$.

Οι τονισμένες γραμμές στο Σχήμα 7 υπονοούν τη χρήση λογικών σχέσεων για τη δόμηση στοιχείων της οντολογίας PMO και υλοποιούνται μέσω της κλάσης `LogicalRelations` (Σχήμα 9). Τα στιγμιότυπα των υποκλάσεών της `ANDRelations`, `ORRelations`, `XORRelations` εκφράζουν τους λογικούς τελεστές AND, OR και XOR, αντίστοιχα. Αναφορά στα οντολογικά στιγμιότυπα που συμμετέχουν σε λογικές σχέσεις, συμπεριλαμβανομένων και άλλων λογικών σχέσεων, γίνεται μέσω των αντικειμενικών ιδιοτήτων `posRelatedTo` και `negRelatedTo`, με την τελευταία να μοντελοποιεί τη χρήση του λογικού τελεστή NOT.

Οι εκφράσεις, από την άλλη πλευρά, επιτρέπουν τον ορισμό των συνθηκών πλαισίου και των περιορισμών που αφορούν οντότητες (π.χ., περιορισμοί σχετικοί με τις ιδιότητες ενός ρόλου). Συνιστούν τριαδικές συσχετίσεις, θέτοντας μία τιμή σε κάποια υποκείμενη οντότητα μέσω ενός τελεστή, ή λογικές δομές αποτελούμενες από τέτοιες συσχετίσεις.

**Ορισμός 5** Μία *ατομική έκφραση* (*atomic expression*) είναι μία πλειάδα $\langle$*exprSubject*, *operator*, *exprValue*$\rangle$, τέτοια ώστε: το υποκείμενο της έκφρασης *exprSubject* αντανακλά το στοιχείο αναφοράς, ο τελεστής *operator* $\in$ *Operators*, όπου *Operators* ένα σύνολο τελεστών, όπως π.χ., `equals`, `greaterThan`, κλπ., και η τιμή της έκφρασης *exprValue* αντιπροσωπεύει την τιμή που ανατίθεται στο υποκείμενο *exprSubject*. Μία *έκφραση* είναι είτε ατομική είτε μία λογική δομή από ατομικές εκφράσεις.

Οντολογικά, οι εκφράσεις μοντελοποιούνται με χρήση των κλάσεων `Expressions` και `LogicalRelations`. Τα στιγμιότυπα της πρώτης κλάσης ουσιαστικά μοντελοποιούν τις ατομικές εκφράσεις, ενώ τα στιγμιότυπα της δεύτερης επιτρέπουν τη δόμηση σύνθετων

εκφράσεων χρησιμοποιώντας ατομικές. Σύμφωνα με τον Ορισμό 5, ορίζονται οι κατάλληλες ιδιότητες για τα στιγμιότυπα της κλάσης `Expressions`, οι οποίες υποδεικνύουν το υποκείμενο (`hasExprSubject`), τον τελεστή (`hasOperator`) και την τιμή (`hasExprValue`). Οι τελεστές ορίζονται οντολογικά ως στιγμιότυπα της κλάσης `Operators`, ενώ το υποκείμενο και η τιμή μίας έκφρασης μπορεί να είναι στιγμιότυπα είτε της PMO οντολογίας είτε της IMO. Ωστόσο, η τιμή είναι δυνατόν να είναι κάποια αυθαίρετη συμβολοσειρά, δηλαδή όχι κάποιο σημασιολογικά ορισμένο στοιχείο. Στην τελευταία αυτή περίπτωση, χρησιμοποιείται η ιδιότητα τύπου δεδομένων `hasExprStringValue` αντί της αντικειμενικής ιδιότητας `hasExprValue`, ώστε να οριστεί μία τιμή τύπου String.

### 5.2.2 Ενέργειες και Οντότητες

Όπως τονίστηκε στην Ενότητα 4.2, οι ενέργειες αποτελούν τον πυρήνα των κανόνων ελέγχου πρόσβασης· οι κανόνες όχι μόνο βρίσκουν εφαρμογή για συγκεκριμένες ενέργειες, αλλά επιπλέον ορίζουν προ- και μετα- ενέργειες που πρέπει (ή όχι) να εκτελεστούν πριν και μετά την επιβολή ενός κανόνα. Οντολογικά οι ενέργειες υλοποιούνται σαν στιγμιότυπα της κλάσης `Actions`. Σύμφωνα με τον Ορισμό 1, η πλειάδα $\langle a_i, op_i, res_i, org \rangle$ αναπαράγεται μέσω των αντικειμενικών ιδιοτήτων που υποδεικνύουν το δράστη (`hasActor`), τη λειτουργία (`hasOperation`), τον πόρο (`hasResource`) και τον οργανισμό (`hasOrganisation`) της ενέργειας (Σχήμα 7). Από τις ιδιότητες αυτές, μόνο η `hasActor` δεν είναι λειτουργική (functional), καθώς περισσότεροι του ενός δράστες είναι δυνατόν να είναι απαραίτητοι για την εκτέλεση κάποιας ενέργειας· η συσχετισμένη λειτουργία είναι πάντα μία, ενώ στα πλαίσια του ελέγχου πρόσβασης, η πρόσβαση εξετάζεται πάντα αναφορικά με κάποιο συγκεκριμένο πόρο[13]. Δράστες συσχετισμένοι μεταξύ τους με σχέση AND υπονοούνται από την ύπαρξη πολλαπλών ιδιοτήτων `hasActor`. Η παράλειψη κάποιας από τις προαναφερθείσες ιδιότητες δηλώνει ότι η αντίστοιχη οντότητα μπορεί να είναι *οποιαδήποτε*, ανεξάρτητα από το επίπεδο αφαίρεσης, μοντελοποιώντας έτσι την περίπτωση $*$.

Εντούτοις, οι προαναφερθείσες ιδιότητες δε δείχνουν απευθείας στο στοιχείο αναφοράς, όπως σε κάποιο ρόλο ο οποίος δηλώνεται σαν δράστης. Αντ' αυτού, η προτεινόμενη προσέγγιση κάνει χρήση ενδιάμεσων αντικειμένων, τα οποία αποτελούν στιγμιότυπα της κλάσης `EnhancedEntities`. Μία διευρυμένη οντότητα υποδεικνύει όχι μόνο την αφηρημένη οντότητα αναφοράς που περιλαμβάνεται στην οντολογία IMO, αλλά επιπλέον προσδιορίζει περιορισμούς για αυτή την οντότητα, επιτρέποντας έτσι την εφαρμογή ελέγχου πρόσβασης βάσει ιδιοτήτων, καθώς και την προδιαγραφή προηγμένων ένθετων περιορισμών. Οι αντίστοιχες αντικειμενικές ιδιότητες είναι οι `refersToConcept` και `refersToConstraint`, με την τελευταία να δείχνει σε κάποιο στιγμιότυπο είτε της κλάσης `Expressions` είτε της

[13]Εξαίρεση αποτελούν οι ενέργειες που είναι συσχετισμένες με μετα-υποχρεώσεις που προέκυψαν μέσω κληρονομικότητας της σχέσης *isA* (βλ. Ενότητα 4.4). Οι ενέργειες αυτές είναι δυνατόν να περιλαμβάνουν περισσότερους του ενός δράστες, λειτουργίες ή πόρους, οι οποίοι είναι εναλλακτικοί μεταξύ τους. Αυτό δηλώνεται με χρήση στιγμιοτύπων της κλάσης `ORRelations`, όπως υπονοούν οι τονισμένες γραμμές που συνδέουν στιγμιότυπα της κλάσης `Actions` με στιγμιότυπα των κλάσεων `EnhancedEntities` και `ConcreteEntities`.

κλάσης LogicalRelations, ενώ οι περιορισμοί ορίζονται στη βάση είτε των χαρακτηριστικών της εν λόγω οντότητας, είτε των στοιχείων που την απαρτίζουν, δηλαδή των στοιχείων που συνδέονται (άμεσα ή έμμεσα) μέσω της αντικειμενικής ιδιότητας isPartOf. Σημειώνεται ότι αν η ιδιότητα refersToConcept παραλείπεται, η οντότητα η οποία υπόκειται σε περιορισμό μπορεί να αναφέρεται σε οποιαδήποτε έννοια του Μοντέλου Πληροφοριών, σε συνάρτηση ωστόσο με άλλες παραμέτρους (π.χ., αν η εν λόγω οντότητα αφορά στο δράστη, τη λειτουργία, τον πόρο ή τον οργανισμό της ενέργειας).

Όπως επίσης αναφέρθηκε στην Ενότητα 4.2, οι ενέργειες είναι δυνατόν να περιέχουν στοιχεία που ορίζονται στο επίπεδο προσδιορισμού. Για το λόγο αυτό, ορίζεται επιπλέον η κλάση ConcreteEntities για την αναπαράσταση τέτοιων οντοτήτων, όπως είναι π.χ., κάποιος συγκεκριμένος χρήστης, αντί κάποιας οντότητας του επιπέδου αφαιρέσεων. Στην περίπτωση αυτή, η ενέργεια συσχετίζεται με την οντότητα του επιπέδου προσδιορισμού μέσω της ιδιότητας τύπου δεδομένων refersToConcreteEntity. Προφανώς, οι οντότητες του επιπέδου προσδιορισμού δεν είναι δυνατόν να περιοριστούν περαιτέρω.

Το Σχήμα 8 απεικονίζει τρεις ενέργειες, οι οποίες αντιστοιχούν στη στατιστική ανάλυση (Act#1), την προ-ενέργεια της παροχής συγκατάθεσης (Act#2), και τη μετα-ενέργεια της καταγραφής (Act#3) της ενέργειας πρόσβασης, δηλαδή της πραγματοποίησης στατιστικής ανάλυσης. Αυτές περιλαμβάνουν διάφορες διευρυμένες οντότητες, για τις περισσότερες εκ των οποίων δεν ορίζονται περιορισμοί, όπως στην περίπτωση της οντότητας EE#1, η οποία αντιστοιχεί στο δράστη με το ρόλο του στατιστικολόγου (Statistician), ή της EE#2, η οποία αντανακλά τη λειτουργία της στατιστικής ανάλυσης. Από την άλλη πλευρά, η διευρυμένη οντότητα EE#3, με το σχετικό πόρο να αφορά σε κάποιο ιατρικό αρχείο (Medical-Record), προσδιορίζεται περαιτέρω μέσω δύο περιορισμών, οι οποίοι περιγράφονται από τις εκφράσεις Expr#2 και Expr#3 και συνδέονται με λογική σχέση AND (LogAND#1).

Συγκεκριμένα, η έκφραση Expr#3 αποτελεί παράδειγμα σύζευξης εννοιών, το οποίο παρουσιάζεται εκτενέστερα στην Ενότητα 5.2.5, ενώ η έκφραση Expr#2 υπονοεί ταυτοποιήσιμα δεδομένα, μέσω άρνησης της κατάστασης στην οποία το ιατρικό αρχείο είναι ανώνυμο. Έτσι, η τιμή της ιδιότητας State που χαρακτηρίζει τα δεδομένα τύπου MedicalRecord αναφέρεται σε ένα στιγμιότυπο της κλάσης DataStates, με τύπο AnonymisationState και τιμή Anonymised. Ο κανόνας δεν υπαγορεύει κάποιο συγκεκριμένο τρόπο με τον οποίο θα επιτευχθεί η ανωνυμία˙ σε περίπτωση που θα έπρεπε να προσδιοριστεί επιπλέον, π.χ., ο αλγόριθμος ανωνυμοποίησης, το στιγμιότυπο DataState#1 θα συσχετιζόταν με την κατάλληλη έκφραση ή λογική σχέση μέσω της ιδιότητας hasStateParameters.

Τέλος, είναι σημαντικό να σημειωθεί ότι οι ίδιες οι ενέργειες είναι δυνατόν να αποτελούν πόρους άλλων ενεργειών. Τέτοια είναι η περίπτωση της ενέργειας Act#1, η οποία αποτελεί τον πόρο της ενέργειας Act#2, υπό την έννοια ότι ο ασθενής θα πρέπει να έχει προηγουμένως συναινέσει για την εκτέλεση της Act#1.

### 5.2.3 Οντολογικοί Κανόνες Ελέγχου Πρόσβασης

Οι κανόνες ελέγχου πρόσβασης υλοποιούνται στην οντολογία PMO μέσω της κλάσης `Rules` (Σχήμα 7). Ουσιαστικά, η κλάση αυτή ενσωματώνει όλες τις υπόλοιπες κλάσεις της οντολογίας, προσφέροντας έτσι την υλοποίηση των κανόνων ελέγχου πρόσβασης, όπως αυτοί προδιαγράφηκαν στην Ενότητα 4.3.

Καθώς οι κανόνες είναι δυνατόν να περιγράφουν άδειες, απαγορεύσεις και υποχρεώσεις, ορίζονται οι αντίστοιχες υπο-κλάσεις της κλάσης `Rules`, δηλαδή `Permissions`, `Prohibitions` and `Obligations`, αντίστοιχα. Κάθε κανόνας περιγράφεται σαν ένα στιγμιότυπο της κατάλληλης υπο-κλάσης, ενώ προσδιορίζονται και τα πεδία του, δηλαδή η ενέργεια για την οποία βρίσκει εφαρμογή ο κανόνας, οι προ- και μετα- ενέργειες, οι συνθήκες πλαισίου και ο υποκείμενος σκοπός πρόσβασης και χρήσης.

Σε αυτό το πλαίσιο, η αντικειμενική ιδιότητα `refersToPurpose` αντιστοιχίζει έναν κανόνα με ένα στιγμιότυπο της κλάσης `Purposes` της IMO οντολογίας, ενώ η ιδιότητα `appliesUnderContext` και η αρνητική της ισοδύναμη `negAppliesUnderContext` δείχνουν σε κάποιο στιγμιότυπο είτε της κλάσης `Expressions` είτε της κλάσης `LogicalRelations` (με στιγμιότυπα της κλάσης `Expressions` να αποτελούν φύλλα της λογικής δομής), για να δηλωθούν οι παράμετροι πλαισίου κάτω από τις οποίες ο εν λόγω κανόνας ισχύει. Στην περίπτωση αυτή, σαν υποκείμενο της εκάστοτε έκφρασης δηλώνεται κάποιο στιγμιότυπο της κλάσης `ContextTypes` της IMO οντολογίας. Για παράδειγμα, η άδεια του Σχήματος 8 ισχύει για το σκοπό της ιατρικής έρευνας `MedicalResearch`, υπό την προϋπόθεση ότι ένα R&D έργο βρίσκεται σε εξέλιξη (`R&DProjectInProgress`).

Η κύρια ενέργεια του κανόνα είναι ένα στιγμιότυπο της κλάσης `Actions` και ορίζεται άμεσα μέσω της ιδιότητας `appliesForAction`. Σε ό,τι αφορά τις προ- και μετα- ενέργειες, αυτές αποτελούν επίσης στιγμιότυπα της κλάσης `Actions`· ωστόσο, ο κανόνας τελικά συσχετίζεται με στιγμιότυπα της κλάσης `RequiredActions` (είτε άμεσα, είτε έμμεσα με χρήση στιγμιοτύπων της κλάσης `LogicalRelations` για λογικά συσχετισμένες συμπληρωματικές ενέργειες), η οποία παρεμβάλλεται μεταξύ των κανόνων και των ενεργειών, μέσω των ιδιοτήτων `requiresPreAction`, `prescribesPostAction`, καθώς και των αρνητικών τους παραλλαγών. Η επιλογή αυτή υπαγορεύεται από δύο κυρίως χαρακτηριστικά: πρώτον, επιτρέπει την περιγραφή πολύπλοκων δομών ενεργειών, δηλαδή την περιγραφή σκελετών (βλ. Ενότητα 5.2.4), και δεύτερον, επιτρέπει τον προσδιορισμό περιορισμών σχετικών με το *πότε* μία προ-/μετα-ενέργεια εκτελείται σε σχέση με την κύρια ενέργεια του κανόνα. Έτσι, η ιδιότητα `isConstrainedToAct` χρησιμοποιείται ώστε να εκφραστούν περιορισμοί τόσο χρονικοί όσο και σχετικοί με την αλληλουχία εκτέλεσης, οι οποίοι αντανακλώνται από τα στιγμιότυπα της κλάσης `SequenceConstraints`. Η τελευταία περιλαμβάνει στιγμιότυπα όπως τα ακόλουθα [126]:

- `Meet`, μέσω του οποίου εκφράζεται ένας αυστηρός χρονικός περιορισμός που περιγράφει ότι το τέλος της προ-ενέργειας συμπίπτει με την έναρξη της ενέργειας πρόσβασης

(αντίστροφα για την περίπτωση των μετα-ενεργειών).

- `Tight`, ένας περιορισμός αλληλουχίας που δηλώνει ότι δεν μπορεί να παρεμβάλλεται άλλη ενέργεια μεταξύ της προ-/μετα- ενέργειας και της ενέργειας πρόσβασης.
- `Before`, ένας χαλαρός περιορισμός αλληλουχίας που εκφράζει ότι η προ-ενέργεια θα πρέπει να έχει εκτελεστεί κάποια στιγμή πριν την ενέργεια πρόσβασης. Αν δεν υπάρχει κάποιο στιγμιότυπο της κλάσης `SequenceConstraints` συσχετισμένο με το στιγμιότυπο της κλάσης `RequiredActions` που αντιπροσωπεύει την προ-ενέργεια, υπονοείται το εν λόγω στιγμιότυπο.
- `After`, που επιβάλλει έναν χαλαρό περιορισμό αλληλουχίας, σύμφωνα με τον οποίο η μετα-ενέργεια θα πρέπει να εκτελεστεί κάποια στιγμή μετά την ενέργεια πρόσβασης. Αν δεν υπάρχει κάποιο στιγμιότυπο της κλάσης `SequenceConstraints` συσχετισμένο με το στιγμιότυπο της κλάσης `RequiredActions` που αντιπροσωπεύει τη μετα-ενέργεια, υπονοείται το εν λόγω στιγμιότυπο.
- `During`, ένας χρονικός περιορισμός που δηλώνει ότι η ενέργεια πρόσβασης θα εκτελεστεί μετά την έναρξη και πριν τη λήξη της προ-ενέργειας (αντίστροφα για την περίπτωση των μετα-ενεργειών).
- `Overlapping`, μέσω του οποίου εκφράζεται ένας χρονικός περιορισμός που δηλώνει ότι η ενέργεια πρόσβασης θα αρχίσει να εκτελείται μετά την έναρξη της προ-ενέργειας και θα ολοκληρωθεί μετά το τέλος της προ-ενέργειας (αντίστροφα για την περίπτωση των μετα-ενεργειών).
- `Parallel`, που εισάγει έναν πιο χαλαρό περιορισμό αλληλουχίας σε σύγκριση με τους δύο προηγούμενους.
- `TightParallel`, που επιβάλλει έναν περιορισμό αλληλουχίας, ο οποίος συνδυάζει τους περιορισμούς που εκφράζουν τα στιγμιότυπα `Tight` και `Parallel`.

Στο παράδειγμα, η χρήση του στιγμιότυπου `Meet` επιβάλλει έναν αυστηρό χρονικό περιορισμό, υπαγορεύοντας ότι το τέλος της ενέργειας πρόσβασης θα πρέπει να συμπίπτει με την έναρξη της μετα-ενέργειας (`Act#3`), ενώ ο πιο χαλαρός περιορισμός αλληλουχίας `Before` εκφράζει ότι η προ-ενέργεια `Act#2` θα πρέπει να έχει εκτελεστεί κάποια στιγμή πριν την κύρια ενέργεια.

Τέλος, σημειώνεται ότι αν κάποια από τις προδιαγεγραμμένες ιδιότητες του κανόνα παραλείπεται, αυτό μεταφράζεται σε, π.χ., *οποιονδήποτε* σκοπό, *οποιαδήποτε* προ-ενέργεια, κ.ο.κ.. Ενδεικτικά, στην περίπτωση του σκοπού, το σύστημα θα συμπεράνει ότι ο σκοπός σε αυτήν την περίπτωση θα είναι η ρίζα του γράφου των σκοπών, δηλαδή το στιγμιότυπο `anyPurpose`.

### 5.2.4 Σκελετοί

Προκειμένου να καταστεί δυνατός ο συνδυασμός ενεργειών έτσι ώστε οι τελευταίες να σχηματίζουν πολύπλοκες δομές εισάγεται η έννοια των σκελετών, η οποία είναι ιδιαίτερα σημαντική για περιπτώσεις όπως, π.χ., η μοντελοποίηση των σύνθετων ενεργειών πριν ή μετά την εκτέλεση ενός κανόνα, όπου περιορισμοί σχετικοί με την αλληλουχία και γενικά με τη ροή είναι απαραίτητο να καθορίζονται, όταν οι λογικές συσχετίσεις ενεργειών δεν αρκούν.

Υλοποιημένοι σαν στιγμιότυπα της κλάσης `Skeletons`, οι σκελετοί παρέχουν τα μέσα για τον προσδιορισμό δομών ενεργειών, οι οποίες περιλαμβάνουν και τις συσχετίσεις αλληλουχίας των ενεργειών αυτών. Οι σκελετοί είναι δυνατόν να αποτελέσουν προ- και μετα- ενέργειες, με στιγμιότυπα της κλάσης `RequiredActions` να δείχνουν σε αυτούς μέσω της ιδιότητας `refersToActionStructure`.

Οι υποκείμενες ενέργειες υποδεικνύονται από στιγμιότυπα της κλάσης `SkeletonItems` μέσω της ιδιότητας `refersToAction`, ενώ τα στιγμιότυπα της κλάσης `SkeletonLegs` περιγράφουν τα πρότυπα αλληλεπίδρασης μεταξύ των εκάστοτε αντικειμένων σκελετού (skeleton items). Κάθε στιγμιότυπο της τελευταίας κλάσης αποτελεί ουσιαστικά μία *ακμή* (edge) που συνδέει δύο ενέργειες· έχει ένα αρχικό και ένα τελικό αντικείμενο σκελετού, στα οποία γίνεται αναφορά με χρήση των ιδιοτήτων `hasSource` και `hasDestination`, αντίστοιχα, ενώ είναι δυνατόν να υπόκειται σε συνθήκες πλαισίου, καθώς και σε περιορισμούς αλληλουχίας. Οι τελευταίοι υλοποιούνται μέσω της κλάσης `SequenceConstraints`, οι οποίοι παράλληλα δηλώνουν (εμμέσως) εάν μία ακμή είναι *κρίσιμη* ή *μη κρίσιμη* όσον αφορά την πιθανή παρεμβολή άλλων ενεργειών μεταξύ του αρχικού και του τελικού αντικειμένου σκελετού. Τέλος, για να δηλωθεί εάν η μετάβαση που υπονοείται από μία ακμή θα συμβεί σε κάθε περίπτωση ή όχι, ορίζονται για μεγαλύτερη ευελιξία τρεις υπο-κλάσεις της `SkeletonLegs`, οι οποίες αντανακλούν, αντίστοιχα, τις AND, OR και XOR συσχετίσεις μεταξύ των εξερχόμενων ακμών μίας ενέργειας.

### 5.2.5 Διαχωρισμός και Σύζευξη Καθηκόντων

Η υψηλή εκφραστικότητα της προτεινόμενης προσέγγισης επιτρέπει την προδιαγραφή προηγμένων περιορισμών διαχωρισμού και σύζευξης καθηκόντων. Αντί να βασίζεται μόνο σε περιορισμούς σχετικούς με τους χρήστες ή τους ρόλους, επιτρέπει την εφαρμογή διαχωρισμού και σύζευξης σε όλα τα στοιχεία που περιλαμβάνει μία ενέργεια, δηλαδή το δράστη, τη λειτουργία, τον πόρο και τον οργανισμό. Αυτό επιτυγχάνεται μέσω εξαρτήσεων μεταξύ των οντοτήτων που περιλαμβάνουν οι ενέργειες ενός κανόνα.

Για παράδειγμα, θεωρούμε ότι ο πόρος `MedicalRecord` της στατιστικής ανάλυσης (`Act#1`) του Σχήματος 8 περιέχει ένα πεδίο που υποδεικνύει τον ασθενή τον οποίο αφορά (`ReferencePatient`), δηλαδή $\texttt{ReferencePatient} \xrightarrow{\texttt{isPartOf}} \texttt{MedicalRecord}$. Καθώς ο ασθενής

`Patient` αποτελεί στιγμιότυπο της κλάσης `Roles` της IMO, θα πρέπει να δηλωθεί ρητά ότι δεν πρόκειται για έναν οποιοδήποτε ασθενή που έχει δώσει τη συγκατάθεσή του, αλλά για το συγκεκριμένο ασθενή που είναι το υποκείμενο των δεδομένων της ιατρικής εγγραφής. Στο πλαίσιο αυτό, η διευρυμένη οντότητα `EE#9` περιορίζεται από την έκφραση `Expr#4`, η οποία προσδιορίζει ότι το στιγμιότυπο (`instance`) του ασθενούς αναφοράς θα πρέπει να αναφέρεται στον ίδιο (`sameAs`) ασθενή που υπονοείται από την οντότητα `EE#4`.

# Κεφάλαιο 6

# Εξαγωγή Γνώσης

Οι οντολογίες που περιγράφηκαν στο Κεφάλαιο 5, δηλαδή το Σημασιολογικό Μοντέλο Πληροφοριών και το Σημασιολογικό Μοντέλο Πολιτικών, αποτελούν τη Βάση Γνώσης του συστήματος και τη βάση για την εξαγωγή συμπερασμάτων σχετικών με την πρόσβαση σε πόρους του συστήματος. Η *Διαδικασία Εξαγωγής Συμπερασμάτων* είναι ιδιαίτερα πολύπλοκη και μπορεί να αποβεί αρκετά χρονοβόρα, λαμβάνοντας υπόψη την εκφραστικότητα —και την πολυπλοκότητα που αυτή εισάγει— των υποκείμενων οντολογιών. Συνεπώς, κρίνεται απαραίτητο να υπάρχει όσο το δυνατόν περισσότερη πληροφορία διαθέσιμη πριν αυτή ζητηθεί κατά τη διαδικασία επαλήθευσης ενός διμερούς συσχετισμού, ώστε να μειωθεί ο αριθμός των αιτημάτων προς τις οντολογίες IMO και PMO, πετυχαίνοντας έτσι καλύτερες επιδόσεις. Με άλλα λόγια, όλες οι απαιτητικές εργασίες επεξεργασίας της υπάρχουσας γνώσης εκτελούνται *σε μη πραγματικό χρόνο* (*offline*)[14] και μόνο κάθε φορά που ενημερώνονται οι οντολογίες IMO και PMO, για παράδειγμα, όταν προστίθενται νέοι κανόνες ελέγχου πρόσβασης ή καταργούνται ήδη υπάρχοντες.

Η *Offline Εξαγωγή Γνώσης* από το Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης και Χρήσης συνίσταται σε δύο διακριτές διαδικασίες: την *εξαγωγή των μετακανόνων*, η οποία ακολουθεί πρότυπα κληρονομικότητας που βασίζονται στις ιδιότητες του Σημασιολογικού Μοντέλου Πληροφοριών, και τη *διαδικασία συλλογιστικής στη βάση των κανόνων ελέγχου πρόσβασης*, κατά την οποία εξάγονται όλες οι ενέργειες που επιτρέπεται τελικά να εκτελεστούν στα πλαίσια της λειτουργίας του συστήματος, σε συνδυασμό με τις προϋποθέσεις που τις καθιστούν έγκυρες, δηλαδή κάποιον έγκυρο σκοπό, τις συνθήκες πλαισίου, καθώς και τις απαιτούμενες και απαγορευμένες δομές προ- και μετα- ενεργειών.

Το πρώτο σκέλος της διαδικασίας εξαγωγής γνώσης, δηλαδή η εξαγωγή των μετακανόνων, περιγράφεται στην Ενότητα 6.1, ενώ στην Ενότητα 6.2 αρχικά παρουσιάζεται η επέκταση του Σημασιολογικού Μοντέλου Πολιτικών ώστε να υποστηρίζει την εκ των προτέρων εξαγωγή γνώσης που περιέχεται στους κανόνες ελέγχου πρόσβασης, καθώς και η αντίστοιχη διαδικασία συλλογιστικής.

[14]Στο εξής, για λόγους συντομίας θα χρησιμοποιείται ο αγγλικός όρος offline.

## 6.1 Εξαγωγή Μετακανόνων

Το Μοντέλο Ελέγχου Πρόσβασης και Χρήσης θεωρεί διάφορες ιεραρχίες˙ στη γενική περίπτωση, και προκειμένου να μειωθεί ο αριθμός των πολιτικών, οι κανόνες ορίζονται στο υψηλότερο δυνατό επίπεδο αφαίρεσης και στη συνέχεια διαδίδονται κατά μήκος των αντίστοιχων γράφων του Σημασιολογικού Μοντέλου Πληροφοριών. Έτσι, ξεκινώντας από τους ρητά ορισμένους κανόνες, που αρχικά συνιστούν το σύνολο *Rules* (*RU*), οι μετακανόνες εξάγονται μέσω μίας offline διαδικασίας, η οποία περιγράφεται σε υψηλό επίπεδο από τον Αλγόριθμο 1.

Το πρώτο βήμα της διαδικασίας αφορά στην *πλήρη ανάπτυξη* των καθορισμένων προ- και μετα- ενεργειών του δεδομένου κανόνα (γραμμές 3—5). Σε αυτό το βήμα δεν εξάγονται νέοι κανόνες με βάση τις σχέσεις κληρονομικότητας που αφορούν τα στοιχεία που συμμετέχουν στις προ- και μετα- ενέργειες. Αντ' αυτού, νέες ενέργειες κατασκευάζονται αντικαθιστώντας τα αρχικά στοιχεία της προ-/μετα- ενέργειας με τα συσχετισμένα με αυτά στοιχεία, ενώ τα υπόλοιπα στοιχεία του κανόνα παραμένουν αμετάβλητα. Συγκεκριμένα, οι *ισοδύναμες*[15] της αρχικής ενέργειες περιλαμβάνουν οντότητες που αναφέρονται σε στοιχεία-φύλλα των *isA* γράφων, δηλαδή οντότητες που δεν μπορούν να εξειδικευθούν περαιτέρω˙ στα πλαίσια της διαδικασίας επαλήθευσης ενός διμερούς συσχετισμού και της προδιαγραφής της τελικής εκτελέσιμης εκδοχής του, το ζητούμενο είναι κάθε εργασία να έχει αντικατασταθεί (εάν δε βρίσκεται ήδη σε αυτήν τη μορφή) από την πιο εξειδικευμένη ισοδύναμή της, ώστε να μη χρειάζεται περαιτέρω αλληλεπίδραση με την οντολογία IMO σε μετέπειτα στάδια συλλογιστικής. Οι εξειδικευμένες ισοδύναμες της αρχικής ενέργειες συνδέονται λογικά μεταξύ τους μέσα στον κανόνα με σχέση OR, η οποία δηλώνει ότι αυτές αποτελούν εναλλακτικές μεταξύ τους ενέργειες. Σε περίπτωση που η αρχικά ορισμένη δομή προ-/μετα- ενεργειών περιελάμβανε λογικά συνδεδεμένες μεταξύ τους ενέργειες, καθεμία από αυτές αναπτύσσεται με τον τρόπο που περιγράφηκε και στη συνέχεια οι αναπτυγμένες δομές αντικαθιστούν τις αρχικές ενέργειες στην αυθεντική λογική σχέση. Στο τέλος αυτού του βήματος, το σύνολο *Rules* παραμένει αμετάβλητο. Σημειώνεται ότι έγινε η παραδοχή ότι αν η προ-/μετα- ενέργεια (ή κάποια από τις ενέργειες που τη συνιστούν) αναφέρεται σε σκελετό, αυτός παραμένει ως έχει και δεν αναπτύσσεται περαιτέρω, θεωρώντας ότι θα πρέπει να εκτελεστεί ακριβώς όπως προσδιορίστηκε κατά τη συγγραφή πολιτικών.

Στα επόμενα βήματα εξάγονται ουσιαστικά οι μετακανόνες. Η εξαγωγή των μετακανόνων ακολουθεί τα πρότυπα που παρουσιάστηκαν στην Ενότητα 4.4, και αφορούν την κληρονομικότητα με βάση το δηλωμένο σκοπό και καθένα από τα στοιχεία που συμμετέχουν στην ενέργεια πρόσβασης, δηλαδή τον/τους δράστη/ες, τη λειτουργία, τον πόρο και τον οργανισμό. Υπενθυμίζεται ότι τα πρότυπα αυτά εξαρτώνται από τον τύπο του κανόνα, δηλαδή αν αυτός αποτελεί άδεια, απαγόρευση ή υποχρέωση. Όπως φαίνεται στα

[15]Η *ισοδυναμία* αναφέρεται στο γεγονός ότι οι πιο εξειδικευμένες ενέργειες περιγράφουν τελικά με μεγαλύτερη λεπτομέρεια την αρχική ενέργεια από την οποία προήλθαν.

αντίστοιχα βήματα του Αλγόριθμου 1, καθεμία από τις μεθόδους εκτελείται πάνω στο σύνολο των κανόνων, όπως αυτό διαμορφώνεται από το κάθε προηγούμενο βήμα, με τους μετακανόνες που προκύπτουν να συνιστούν αρχικά το σύνολο *InferredRules* (*IRU*), το οποίο προστίθεται στο τέλος του κάθε βήματος στο σύνολο των κανόνων. Σημειώνεται ότι κάθε μετακανόνας συσχετίζεται με τον κανόνα (ή μετακανόνα) από τον οποίο συνάγεται, με παράλληλη αναφορά στη σχέση μέσω της οποίας προέκυψε, ενώ επίσης οι κανόνες επισημειώνονται κατάλληλα για να οριστεί αν μπορούν να κληρονομηθούν με βάση κάποιο στοιχείο της ενέργειας πρόσβασης[16]. Οι ιδιότητες αυτές παίζουν σημαντικό ρόλο στη διαχείριση και τη συντήρηση του συνόλου των κανόνων.

Έτσι, αρχικά πραγματοποιείται η εξαγωγή των μετακανόνων με βάση το σκοπό που είναι συσχετισμένος με τον εκάστοτε κανόνα (γραμμές 6—9). Η διαδικασία περιγράφεται πιο αναλυτικά από τον Αλγόριθμο 2. Ξεκινώντας από το ρητά συσχετισμένο σκοπό, οι μετακανόνες εξάγονται ακολουθώντας τη σχέση *isA* στο γράφο των σκοπών. Συγκεκριμένα, βρίσκονται οι ρητά πιο εξειδικευμένοι σκοποί (απόσταση 1 στο γράφο) που συνιστούν το σύνολο *eXplicitlyMoreSpecificPurposes* (*XMSP*) και για καθέναν από αυτούς κατασκευάζεται ένας νέος κανόνας, με όλα τα υπόλοιπα στοιχεία του νέου κανόνα (ενέργεια πρόσβασης, προ-/μετα- ενέργειες, συνθήκες πλαισίου) να αντιγράφονται από τον αρχικό κανόνα. Η διαδικασία αυτή επαναλαμβάνεται αναδρομικά για καθέναν από τους εξαχθέντες μετακανόνες, μέχρι να καταλήξουμε στα φύλλα του γράφου. Υπενθυμίζεται ότι, λόγω της σχέσης *isA*, το ίδιο πρότυπο κληρονομικότητας ισχύει για όλους τους τύπους κανόνων, δηλαδή τα πιο γενικά στοιχεία ενός γράφου κληροδοτούν εξουσιοδοτήσεις στα πιο εξειδικευμένα.

Στη συνέχεια εξάγονται οι μετακανόνες που αφορούν την ενέργεια πρόσβασης, σύμφωνα με τα πρότυπα κληρονομικότητας που ακολουθούν τα διάφορα στοιχεία της (γραμμές 10—44). Τα βήματα αυτά έχουν νόημα μόνο όταν η αντίστοιχη οντότητα είναι εκφρασμένη στο επίπεδο αφαιρέσεων. Αρχικά, εξάγονται οι μετακανόνες με βάση τη σχέση *isA*, ώστε τελικά να υπάρχουν κανόνες για όλες τις ενέργειες που είναι ισοδύναμες με τις αρχικές ενέργειες των ρητά καθορισμένων κανόνων (γραμμές 10—24), και ακολούθως εκείνοι με βάση τις σχέσεις *isPartOf* και *moreDetailedThan* (η τελευταία έχει νόημα μόνο για τύπους δεδομένων που παίζουν το ρόλο του πόρου). Συνοπτικά, για κάθε στοιχείο που είναι πιο εξειδικευμένο από το εκάστοτε στοιχείο της ενέργειας πρόσβασης (π.χ., ένας ρόλος), δημιουργείται μία νέα ενέργεια όπου το πιο εξειδικευμένο στοιχείο αντικαθιστά το αρχικό και συνδέεται με το νέο μετακανόνα, σε πλήρη αντιστοιχία με το προηγούμενο βήμα, με τα υπόλοιπα στοιχεία του κανόνα να παραμένουν αμετάβλητα και στον εν λόγω μετακανόνα.

Η ίδια διαδικασία διεξάγεται και στην περίπτωση των άλλων δύο σχέσεων, δηλαδή των σχέσεων *isPartOf* και *moreDetailedThan*, με μόνη εξαίρεση τη διάσχιση των αντίστοιχων

[16]Έχουν οριστεί οι αντίστοιχες ιδιότητες στην οντολογία PMO, οι οποίες όμως παραλείπονται στο Σχήμα 7 για λόγους οικονομίας χώρου.

γράφων προς διαφορετική κατεύθυνση ανάλογα με το εάν ο εν λόγω κανόνας συνιστά θετική ή αρνητική εξουσιοδότηση. Ο Αλγόριθμος 3 περιγράφει τη διαδικασία εξαγωγής μετακανόνων σύμφωνα με τη σχέση συμπερίληψης, για την περίπτωση των πόρων. Το σύνολο *RelatedResourses* (*RELRES*) περιλαμβάνει τις έννοιες που συσχετίζονται με την έννοια πάνω στην οποία ορίζεται ο πόρος της ενέργειας (*ruActResCon*) —υπό την έννοια ότι ο πόρος περιλαμβάνει και περιορισμούς πάνω στην έννοια— και είναι διαφορετικό ανάλογα με τον τύπο του κανόνα. Η μέθοδος CreateResourceEnhancedEntity(*relRes*, *ruActRes*)) δημιουργεί τη νέα διευρυμένη οντότητα, χρησιμοποιώντας τη συγγενική έννοια *relRes* και τους περιορισμούς που είχαν οριστεί για τον πόρο *ruActRes* της αρχικής ενέργειας πρόσβασης *ruAct*, η οποία συνδέεται με την εξαχθείσα ενέργεια *infAct* και αυτή με τη σειρά της με το μετακανόνα *iru*.

Τέλος, ειδικά για την περίπτωση που κάποιος ρόλος που συνιστά δράστη στην ενέργεια πρόσβασης αποτελείται από περισσότερους ρόλους συσχετισμένους μεταξύ τους με σχέση AND (περίπτωση *isPartOf* σχέσης), δε δημιουργείται μία ξεχωριστή ενέργεια —και κατ' επέκταση, ένας ξεχωριστός μετακανόνας— για κάθε συνιστώσα του ρόλου αυτού, αλλά μία μόνο ενέργεια με τους λογικά συσχετισμένους ρόλους να αντικαθιστούν τον αρχικό.

Τα βήματα που περιγράφηκαν παραπάνω είναι δυνατόν να οδηγήσουν σε *περιττούς* κανόνες, υπό την έννοια ότι μπορεί να υπάρχουν πολλαπλά αντίγραφα του ίδιου κανόνα ή κανόνες διαφορετικού τύπου που συγκρούονται μεταξύ τους. Έτσι, οι γραμμές 45—51 του Αλγόριθμου 1 αφορούν στην αφαίρεση των περιττών και των αντικρουόμενων κανόνων, ενώ ο Αλγόριθμος 4 περιγράφει τη διαδικασία εύρεσης των κανόνων αυτών. Στο πλαίσιο αυτό, αναζητούνται οι κανόνες με πανομοιότυπο σώμα, δηλαδή με ίδιο σκοπό, ενέργεια πρόσβασης, προ- και μετα- ενέργειες και συνθήκες πλαισίου[17], και τελικά αφαιρούνται από το σύνολο *Rules*. Οι γραμμές 4—9 αφορούν πολλαπλά αντίγραφα του ίδιου κανόνα, ενώ οι γραμμές 10—21 εντοπίζουν αντικρουόμενους κανόνες. Σε ό,τι αφορά την επίλυση συγκρούσεων, ισχύουν τα ακόλουθα:

i) Οι κανόνες που έχουν οριστεί ρητά υπερισχύουν των μετακανόνων.

ii) Οι απαγορεύσεις, είτε αποτελούν ρητούς είτε μετα- κανόνες, υπερισχύουν των θετικών μετακανόνων (άδειες και υποχρεώσεις).

Στο Σχήμα 10 παρουσιάζεται η εξαγωγή ενός μετακανόνα (Σχήμα 10γ′) από τον αρχικό κανόνα του Σχήματος 10α′. Η υποχρέωση του Σχήματος 10α′ υπαγορεύει την εκτέλεση της ενέργειας `Act#1` που αφορά την τεκμηρίωση ενός περιστατικού (`DocumentIncident`)

[17]Ενδέχεται τα σώματα των κανόνων να μην είναι πανομοιότυπα, αλλά ισοδύναμα· αυτό σημαίνει, ότι μπορεί π.χ., οι διευρυμένες οντότητες που βρίσκονται στην ίδια θέση της ενέργειας πρόσβασης ενός κανόνα να αναφέρονται στην ίδια έννοια του Σημασιολογικού Μοντέλου Πληροφοριών, αλλά να φέρουν διαφορετικούς περιορισμούς που όμως συμπίπτουν. Η επίλυση τέτοιων διαφορών έχει ληφθεί υπόψη ώστε τελικά τα σώματα των κανόνων να θεωρούνται πανομοιότυπα.

**Αλγόριθμος 1** ExtractMetaRules

**Input:** *PM*
**Output:** *PM*

$RU \leftarrow$ FindAllRules(*PM*)
$IRU \leftarrow \emptyset$
**for each** $ru$ **in** $RU$ **do**
  UnfoldPreAndPostActions($ru$)
**end for**
**for each** $ru$ **in** $RU$ **do**
  $IRU$.add(ExtractPurposeRelatedMetaRules($ru$))
**end for**
$RU$.add($IRU$)
$IRU \leftarrow \emptyset$
**for each** $ru$ **in** $RU$ **do**
  $IRU$.add(ExtractActorIsARelatedMetaRules($ru$))
**end for**
$RU$.add($IRU$)
$IRU \leftarrow \emptyset$
**for each** $ru$ **in** $RU$ **do**
  $IRU$.add(ExtractOperationIsARelatedMetaRules($ru$))
**end for**
$RU$.add($IRU$)
$IRU \leftarrow \emptyset$
**for each** $ru$ **in** $RU$ **do**
  $IRU$.add(ExtractResourceIsARelatedMetaRules($ru$))
**end for**
$RU$.add($IRU$)
$IRU \leftarrow \emptyset$
**for each** $ru$ **in** $RU$ **do**
  $IRU$.add(ExtractResourceMoreDetailedRelatedMetaRules($ru$))
**end for**
$RU$.add($IRU$)
$IRU \leftarrow \emptyset$
**for each** $ru$ **in** $RU$ **do**
  $IRU$.add(ExtractActorIsPartOfRelatedMetaRules($ru$))
**end for**
$RU$.add($IRU$)
$IRU \leftarrow \emptyset$
**for each** $ru$ **in** $RU$ **do**
  $IRU$.add(ExtractOperationIsPartOfRelatedMetaRules($ru$))
**end for**
$RU$.add($IRU$)
$IRU \leftarrow \emptyset$
**for each** $ru$ **in** $RU$ **do**
  $IRU$.add(ExtractResourceIsPartOfRelatedMetaRules($ru$))
**end for**
$RU$.add($IRU$)

45: $RU_{red} \leftarrow \emptyset$
46: **for each** $ru$ **in** $RU$ **do**
47:  **if** $RU_{red}$ notContains $ru$ **then**
48:  $RU_{red}$.add(FindRedundantAndConflictingRules($ru$))
49:  **end if**
50:  $RU$.remove($RU_{red}$)
51: **end for**
52: **return** $PM$

**Αλγόριθμος 2** ExtractPurposeRelatedMetaRules

**Input:** $ru$
**Output:** $IRU$
1: $IRU \leftarrow \emptyset$
2: $pu \leftarrow ru$.purpose
3: $XMSP \leftarrow$ FindExplicitMoreSpecificPurposes($pu$)
4: **for each** $xmsp$ **in** $XMSP$ **do**
5:  $iru$.purpose $\leftarrow xmsp$
6:  $iru$.ruleType $\leftarrow ru$.ruleType
7:  $iru$.action $\leftarrow ru$.action
8:  $iru$.preAction $\leftarrow ru$.preAction
9:  $iru$.postAction $\leftarrow ru$.postAction
10:  $iru$.context $\leftarrow ru$.context
11:  $IRU$.add($iru$)
12:  $IRU$.add(ExtractPurposeRelatedMetaRules($iru$))
13: **end for**
14: **return** $IRU$

**Αλγόριθμος 3** ExtractResourceIsPartOfRelatedMetaRules

**Input:** $ru$
**Output:** $IRU$
1: $IRU \leftarrow \emptyset$
2: $RELRES \leftarrow \emptyset$
3: $ruAct \leftarrow ru$.action
4: $ruActRes \leftarrow ruAct$.resource
5: $ruActResCon \leftarrow ruActRes$.concept
6: **if** $ru$.ruleType $= prohibition$ **then**
7:  $RELRES \leftarrow$ FindExplicitContainers($ruActResCon$)
8: **else**
9:  $RELRES \leftarrow$ FindExplicitContainedTypes($ruActResCon$)
10: **end if**

από το προσωπικό ασφάλειας (`SecurityPersonnel`), εφόσον το περιστατικό έχει ολοκληρωθεί (όπως υπαγορεύεται από την έκφραση `Expr#1` ⟨`IncidentIsOver`, `equals`, True⟩), και ενώ έχει εκτελεστεί η προενέργεια `ReqAct#1` που αναφέρεται στην αντιμετώπιση του περιστατικού (`MitigateIncident`). Αρχικά, πραγματοποιείται η ανάπτυξη της προ-ενέργειας `ReqAct#1` με βάση τη σχέση εξειδίκευσης `isA` του υπογράφου λειτουργιών του Σχήματος 10β′,

11: **for each** $relRes$ **in** $RELRES$ **do**
12: *infAct*.actor ← $ruAct$.actor
13: *infAct*.operation ← $ruAct$.operation
14: *infAct*.resource ← CreateResourceEnhancedEntity(*relRes*, $ruActRes$))
15: *infAct*.organisation ← $ruAct$.organisation
16: *iru*.ruleType ← *ru*.ruleType
17: *iru*.purpose ← *ru*.purpose
18: *iru*.action ← *infAct*
19: *iru*.preAction ← *ru*.preAction
20: *iru*.postAction ← *ru*.postAction
21: *iru*.context ← *ru*.context
22: $IRU$.add($iru$)
23: $IRU$.add(ExtractResourceIsPartOfRelatedMetaRules($iru$))
24: **end for**
25: **return** *IRU*

**Αλγόριθμος 4** FindRedundantAndConflictingRules

**Input:** $ru$
**Output:** $RU_{red}$
1: $RU' \leftarrow$ FindRulesWithIdenticalBody($ru$)
2: $RU_{red} \leftarrow \emptyset$
3: **for each** $ru'$ **in** $RU'$ **do**
4: **if** $ru'$.ruleType $=$ $ru$.ruleType **then**
5: **if** $ru'$ $is\ metaRule$ && $ru$ $isNot\ metaRule$ **then**
6: $RU_{red}$.add($ru'$)
7: **else**
8: $RU_{red}$.add($ru$)
9: **end if**
10: **else**
11: **if** $ru'$ $is\ metaRule$ && $ru$ $isNot\ metaRule$ **then**
12: $RU_{red}$.add($ru'$)
13: **else if** $ru'$ $isNot\ metaRule$ && $ru$ $is\ metaRule$ **then**
14: $RU_{red}$.add($ru$)
15: **else**
16: **if** $ru'$.ruletype $=$ $prohibition$ && $ru'$.ruletype $\neq$ $prohibition$ **then**
17: $RU_{red}$.add($ru$)
18: **else if** $ru'$.ruletype $\neq$ $prohibition$ && $ru'$.ruletype $=$ $prohibition$ **then**
19: $RU_{red}$.add($ru'$)
20: **end if**
21: **end if**
22: **end if**
23: **end for**
24: **return** $RU_{red}$

οπότε τελικά αντικαθίσταται από δύο εναλλακτικές προ-ενέργειες, όπως υποδηλώνει το στιγμιότυπο `LogOR#1` του Σχήματος 10γ′. Στη συνέχεια εξάγονται οι μετακανόνες με βάση την κληρονομικότητα των σκοπών και των στοιχείων που συμμετέχουν στην ενέργεια πρό-

σβασης/χρήσης. Συγκεκριμένα, από τον κανόνα `Obligation#1` θα προκύψουν δύο μετακανόνες λόγω κληρονομικότητας μέσω της σχέσης εξειδίκευσης `isA`. Έτσι, λόγω των υπογράφων σκοπών και ρόλων του Σχήματος 10β', οι μετακανόνες που θα προκύψουν θα διατηρούν τα στοιχεία του αρχικού κανόνα που δεν αναφέρονται στο σκοπό (`NetworkSecurity`) και το ρόλο (`SecurityPersonnel`) του δράστη της ενέργειας πρόσβασης (`Act#1`), με τον αρχικό σκοπό να αντικαθίσταται από τους πιο εξειδικευμένους `PerimeterNetworkSecurity` και `CollaborativeNetworkSecurity`, ενώ καθένας από τους μετακανόνες συσχετίζεται με μία νέα ενέργεια όπου ο αρχικός δράστης έχει αντικατασταθεί από τους λογικά συσχετισμένους πιο εξειδικευμένους δράστες. Υπενθυμίζεται ότι η αντικατάσταση του αρχικού δράστη από τη λογική σχέση `LogOR#2` οφείλεται στα πρότυπα κληρονομικότητας που ακολουθούν οι υποχρεώσεις (βλ. Ενότητα 4.4)˙ αν δηλαδή ο αρχικός κανόνας ήταν άδεια, θα προέκυπταν τέσσερις μετακανόνες για τους τέσσερις δυνατούς συνδυασμούς πιο εξειδικευμένων σκοπών και ρόλων, με το δράστη της εκάστοτε ενέργειας πρόσβασης να αναφέρεται σε ένα μόνο ρόλο. Τέλος, σημειώνεται ότι κάθε μετακανόνας επισημειώνεται με την πληροφορία για τον κανόνα (ή μετακανόνα) από τον οποίο προήλθε, με χρήση της αντικειμενικής ιδιότητας `derivedFromRule`, όπως φαίνεται στο Σχήμα 10γ'.

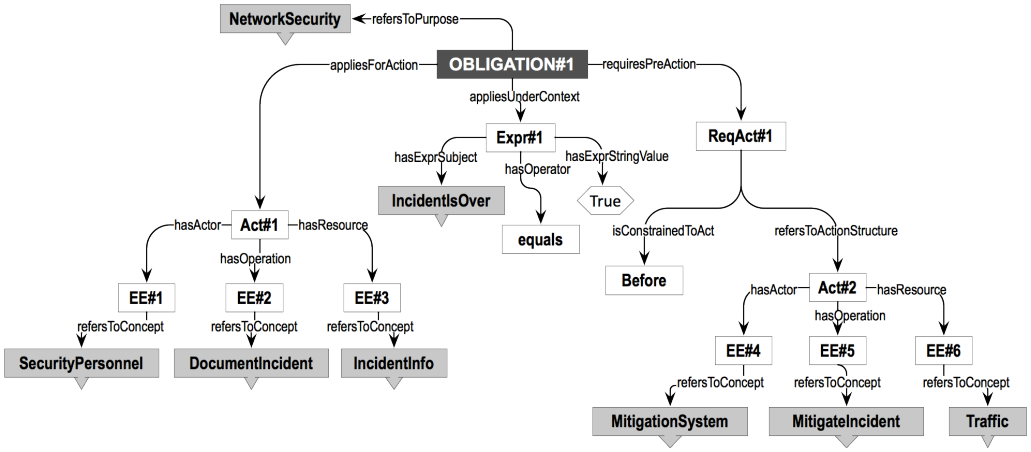
## 6.2 Συλλογιστική στη Βάση των Κανόνων Ελέγχου Πρόσβασης

Το δεύτερο σκέλος της offline διαδικασίας εξαγωγής γνώσης αφορά την εξαγωγή συμπερασμάτων, σχετικών με τις επιτρεπόμενες ενέργειες πρόσβασης, από τους ίδιους τους κανόνες. Η διαδικασία αυτή στοχεύει στο να καθίσταται διαθέσιμη όσο το δυνατόν περισσότερη από την απαραίτητη γνώση για την εξαγωγή των *Οδηγιών Εξουσιοδότησης* (βλ. Ενότητα 7.1) πριν αυτή ζητηθεί σε πραγματικό χρόνο, ενώ το βασικό πλεονέκτημα που παρουσιάζει είναι η ελαχιστοποίηση της ιδιαίτερα απαιτητικής σε πόρους συλλογιστικής σε πραγματικό χρόνο, δηλαδή κατά την αποτίμηση των αιτημάτων πρόσβασης και, κατ' επέκταση, την αξιολόγηση και επαλήθευση ενός διμερούς συσχετισμού.

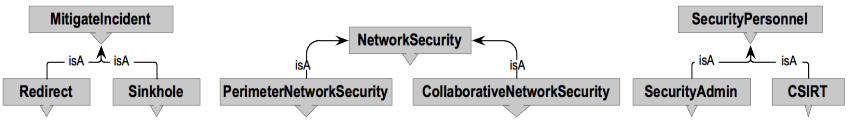
### 6.2.1 Επέκταση του Σημασιολογικού Μοντέλου Πολιτικών

Η βασική οντολογία του Σημασιολογικού Μοντέλου Πολιτικών, η οποία περιγράφηκε στην Ενότητα 5.2, επεκτείνεται έτσι ώστε να υποστηρίζει το δεύτερο σκέλος της offline διαδικασίας εξαγωγής γνώσης, δηλαδή την εκ των προτέρων εξαγωγή γνώσης που περιέχεται στους κανόνες ελέγχου πρόσβασης. Η εν λόγω επέκταση στοχεύει στην ελαχιστοποίηση των αιτημάτων προς την οντολογία PMO σε πραγματικό χρόνο και, επομένως, σε καλύτερες επιδόσεις.

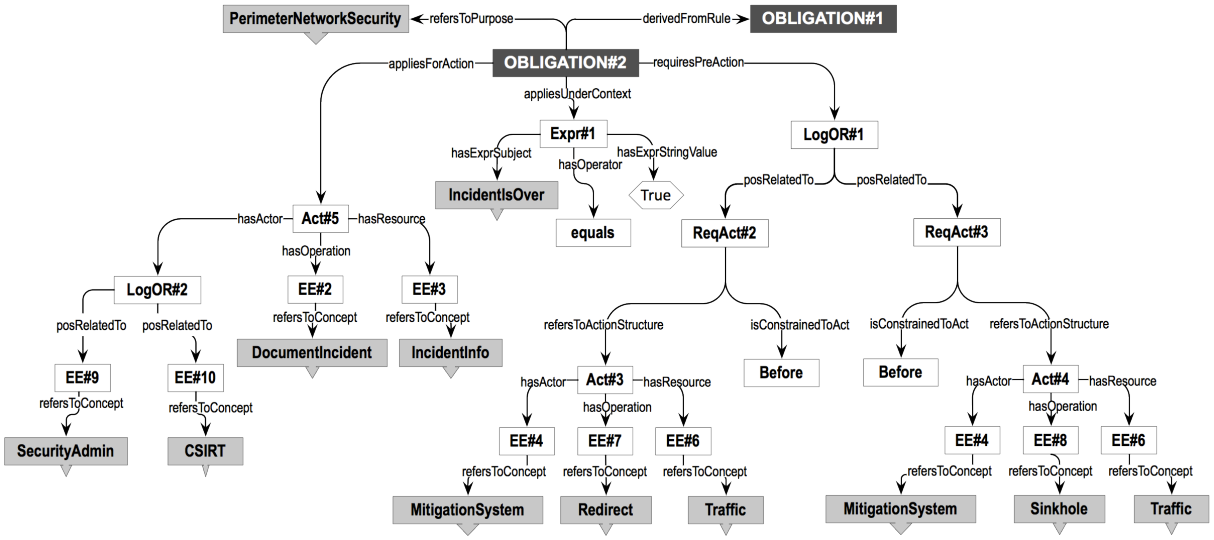
Για το σκοπό αυτό, και όπως απεικονίζεται στο Σχήμα 11, καθορίζονται δύο επιπλέον κλάσεις στο Σημασιολογικό Μοντέλο Πολιτικών, οι `PermittedActions` και `OfflineRequiredActionStructures`. Τα στιγμιότυπα που ανήκουν στην πρώτη κλάση αντιπροσω-




(α′) Αρχικός Κανόνας Ελέγχου Πρόσβασης και Χρήσης




(β′) Υπογράφοι της ΙΜΟ

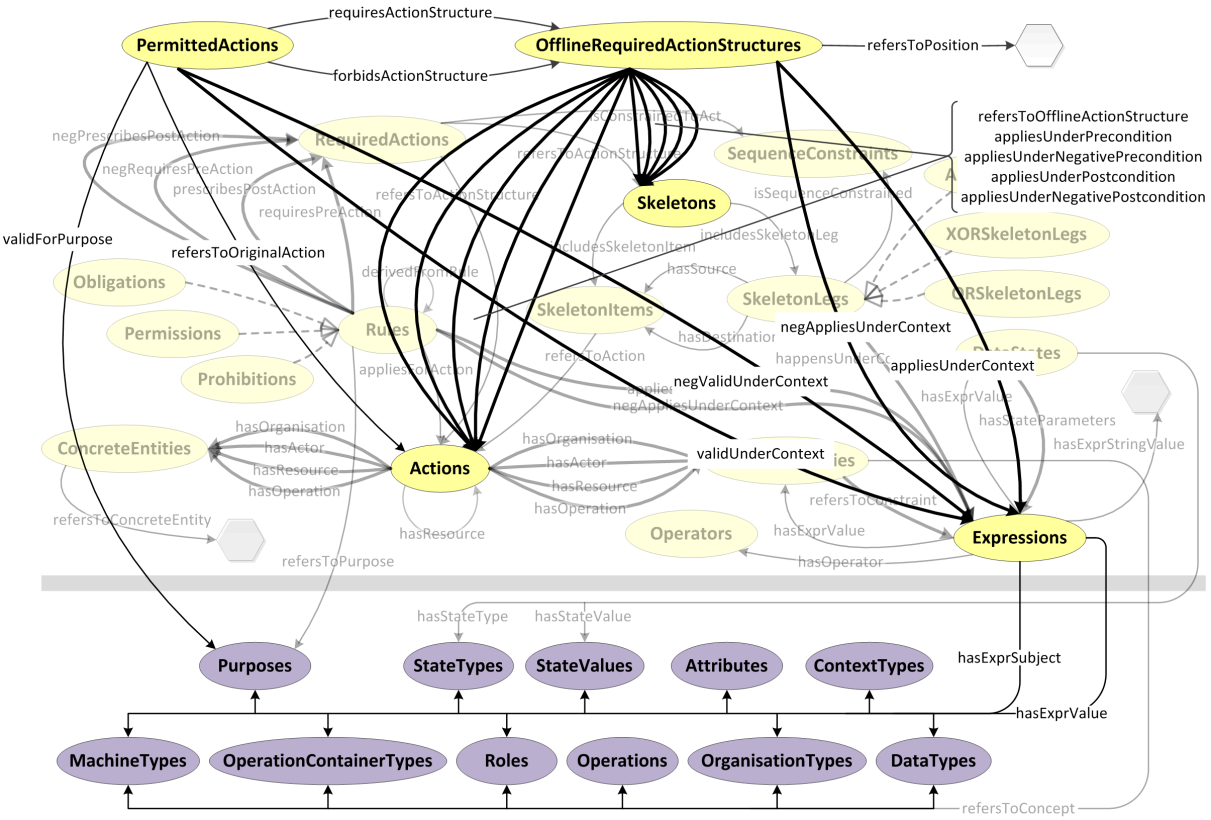



(γ′) Μετακανόνας

Σχήμα 10: Παράδειγμα Εξαγωγής Μετακανόνα

πεύουν όλες τις ενέργειες που επιτρέπονται τελικά να εκτελεστούν στο πλαίσιο της λειτουργίας του συστήματος (ενδεχομένως υπό προϋποθέσεις) και αναφέρονται ως *Επιτρεπόμενες Ενέργειες*. Συγκεκριμένα, οι ενέργειες αυτές είναι *τελείως εξειδικευμένες*, υπό την έννοια ότι οι οντότητες που τις απαρτίζουν αναφέρονται σε στοιχεία του Σημασιολογικού Μοντέλου Πληροφοριών που αποτελούν φύλλα των αντίστοιχων *isA* γράφων (εκτός από την περίπτωση που αυτές είναι ορισμένες στο επίπεδο προσδιορισμού). Αυτή η επιλογή οφείλεται και πάλι στο γεγονός ότι το ζητούμενο είναι κάθε εργασία του διμερούς συσχετισμού που ελέγχεται να έχει αντικατασταθεί (εάν δε βρίσκεται ήδη σε αυτήν τη μορφή) από την πιο εξειδικευμένη ισοδύναμή της, ώστε να ελαχιστοποιούνται σε πραγμα-

τικό χρόνο τα αιτήματα προς τις οντολογίες IMO και PMO, π.χ., αναφορικά με τις σχέσεις που συνδέουν δύο στιγμιότυπα κάποιας κλάσης του IMO. Σε αυτήν τη σχεδιαστική επιλογή συντελεί επίσης το γεγονός ότι μία άδεια μπορεί να ορίζεται σε υψηλό επίπεδο αφαίρεσης, ωστόσο ενδέχεται να ορίζονται εξαιρέσεις διασχίζοντας τους αντίστοιχους γράφους προς πιο εξειδικευμένες έννοιες. Τα στιγμιότυπα της κλάσης `PermittedActions` προκύπτουν από θετικές εξουσιοδοτήσεις, δηλαδή από στιγμιότυπα της κλάσης `Permissions`, με τη λογική ότι για να επιτρέπεται κατ' αρχήν μία ενέργεια θα πρέπει να ορίζεται για αυτήν τουλάχιστον μία άδεια, με την εκάστοτε επιτρεπόμενη ενέργεια να αναφέρεται στην ενέργεια πρόσβασης του κανόνα από τον οποίο προήλθε. Ουσιαστικά, κάθε τέτοια ενέργεια συμπυκνώνει όλη την πληροφορία που φέρει ένας κανόνας, δηλαδή το σκοπό και τις συνθήκες πλαισίου που την καθιστούν έγκυρη, καθώς και τις δομές ενεργειών που απαιτεί ή αποκλείει η εκτέλεση της εν λόγω ενέργειας. Έτσι, ορίζονται τελικά στην οντολογία οι αντίστοιχες αντικειμενικές ιδιότητες για να συμπληρωθεί καταλλήλως μία επιτρεπόμενη ενέργεια, δηλαδή οι `refersToOriginalAction`, `validForPurpose`, `validUnderContext` (και η αρνητική αντίστοιχή της), `requiresActionStructure` και `forbidsActionStructure`. Καθώς σε κάποιες περιπτώσεις έχει σημασία το ποιος εκκινεί τη διαδικασία, ορίζεται επιπλέον η ιδιότητα `refersToValidInitiator`.




Σχήμα 11: Επέκταση της Οντολογίας PMO.

Από την άλλη πλευρά, η κλάση `OfflineRequiredActionStructures` αντανακλά τις απαιτούμενες ή απαγορευμένες προ- και μετα- ενέργειες, οι οποίες συμπληρώνουν την

επιτρεπόμενη ενέργεια πρόσβασης και αναφέρονται ως *Απαιτούμενες Διενέργειες*. Σε αντιστοιχία με την κλάση `RequiredActions` του βασικού PMO, τα στιγμιότυπα της κλάσης αυτής αναφέρονται είτε σε ενέργειες είτε σε σκελετούς (ή σε συνδυασμό τους μέσω λογικών σχέσεων), με τη διαφορά ότι η διάκριση μεταξύ προ- και μετα- ενεργειών επιτυγχάνεται μέσω της ιδιότητας τύπου δεδομένων `refersToPosition` και όχι μέσω διαφορετικών αντικειμενικών ιδιοτήτων, για να διευκολυνθεί περαιτέρω η μετάφραση των απαιτούμενων ή απαγορευμένων δομών ενεργειών στις αντίστοιχες δομές που προβλέπουν οι οδηγίες εξουσιοδότησης (βλ. Ενότητα 7.1). Επίσης, οι συσχετίσεις μεταξύ των προ-και μετα- ενεργειών, καθώς και της ενέργειας πρόσβασης, δημιουργούν την ανάγκη να οριστούν επίσης *προϋποθέσεις* (*preconditions*) και *μετασυνθήκες* (*postconditions*) που καθιστούν τις απαιτούμενες διενέργειες είτε απαραίτητες για την εκτέλεση της επιτρεπόμενης ενέργειας είτε απαγορευμένες. Τόσο οι προϋποθέσεις όσο και οι μετασυνθήκες αναφέρονται με τη σειρά τους σε ενέργειες, σκελετούς, ή λογικές δομές αυτών, και ορίζονται μέσω των ιδιοτήτων `appliesUnderPrecondition`, `appliesUnderPostcondition` και των αντίστοιχων αρνητικών ιδιοτήτων. Τέλος, οι απαιτούμενες διενέργειες εξαρτώνται από τις συνθήκες πλαισίου, οι οποίες ενδέχεται να είναι διαφορετικές από εκείνες που αφορούν την επιτρεπόμενη ενέργεια, καθώς είναι δυνατόν να έχουν προέλθει από διαφορετικούς κανόνες, όπως περιγράφεται στη συνέχεια.

Οι δύο νέες αυτές κλάσεις ουσιαστικά περιέχουν τη γνώση για να απαντηθούν τα εξής κρίσιμα ερωτήματα:

1. Εάν μία ενέργεια είναι *κατ' αρχήν έγκυρη*, δηλαδή ο δράστης $a_i$ έχει το δικαίωμα να εκτελέσει τη λειτουργία $op_i$ στον πόρο $res_i$ εντός του οργανισμού $org_i$. Κατ' αρχήν έγκυρη σημαίνει ότι, αν και μία ενέργεια μπορεί να είναι τυπικά έγκυρη για κάποιο δεδομένο σκοπό, ωστόσο μπορεί τελικά να αποδειχθεί μη έγκυρη, λόγω π.χ., ενδεχόμενης σύγκρουσης με κάποια άλλη ενέργεια ή περιορισμών πλαισίου.

2. Εάν μία ενέργεια προϋποθέτει την ύπαρξη μίας ή περισσότερων ενεργειών, καθώς και την ακριβή ή σχετική θέση της πρόσθετης ενέργειας αναφορικά με τη δεδομένη˙ η απάντηση στο ερώτημα αυτό βρίσκεται σε άμεση συνάρτηση με το εκάστοτε πλαίσιο, το συσχετισμένο με την ενέργεια δράστη, τον εκκινητή, τον υποκείμενο σκοπό, κλπ..

3. Εάν εντοπίζονται ασυμβατότητες και συγκρούσεις μεταξύ ενεργειών, λαμβάνοντας υπόψη τις παραμέτρους που σχετίζονται με τους δράστες και τους πόρους, τον εκκινητή, το σκοπό, κλπ..

Τα στιγμιότυπα της κλάσης `PermittedActions` αντιστοιχούν σε κατ' αρχήν έγκυρες ενέργειες, ενώ εκείνα της κλάσης `OfflineRequiredActionStructures`, σε συνδυασμό με την πληροφορία για το σκοπό, τις συνθήκες πλαισίου και, ενδεχομένως, τον εκκινητή της διαδικασίας, προσδιορίζουν τις προϋποθέσεις που καθιστούν τελικά τις εν λόγω ενέργειες έγκυρες.

### 6.2.2 Μηχανισμός Εξαγωγής Γνώσης

Η λογική πίσω από την εξαγωγή μίας επιτρεπόμενης ενέργειας είναι ότι, για να θεωρηθεί μία ενέργεια κατ' αρχήν έγκυρη, αρχικά θα πρέπει να έχει οριστεί τουλάχιστον μία άδεια που να την αφορά. Στη συνέχεια, θα πρέπει να αναζητηθούν τυχόν απαγορεύσεις για την ενέργεια αυτή, ώστε να συγκεντρωθούν οι συνθήκες που δεν επιτρέπουν την εκτέλεσή της. Από την άλλη πλευρά, με δεδομένη την εκτέλεση της εν λόγω ενέργειας, θα πρέπει να ελεγχθούν ενδεχόμενες συγκρούσεις με άλλες ενέργειες, μέσω κανόνων όπου γίνεται αναφορά σε αυτήν ως προ-ενέργεια. Για παράδειγμα, η εκτέλεση της υπό εξέταση ενέργειας είναι δυνατόν να ενεργοποιεί κάποια υποχρέωση ή απαγόρευση (ως μέρος της προ-ενέργειας), με αποτέλεσμα η ενέργεια πρόσβασης του αντίστοιχου κανόνα να συγκρούεται τελικά μαζί της.

Οι επιτρεπόμενες ενέργειες, όπως αναφέρθηκε προηγουμένως, προκύπτουν από θετικές εξουσιοδοτήσεις και συγκεκριμένα από άδειες. Σε αντίθεση με τα στιγμιότυπα της κλάσης `PermittedActions`, εκείνα της κλάσης `OfflineRequiredActionStructures` δεν εξάγονται μόνο από άδειες, αλλά από κανόνες κάθε τύπου. Ουσιαστικά, κατά τη δημιουργία μίας επιτρεπόμενης ενέργειας, συγκεντρώνονται όλες οι άδειες, οι απαγορεύσεις και οι υποχρεώσεις μέσα στις οποίες η αρχική ενέργεια πρόσβασης —από την οποία προήλθε η εν λόγω επιτρεπόμενη ενέργεια— αποτελεί είτε την κύρια ενέργεια του κανόνα ή κάποια προ-/μετα- ενέργεια. Έτσι, στην περίπτωση των αδειών και των απαγορεύσεων στις οποίες η επιτρεπόμενη ενέργεια αντιστοιχεί στην ενέργεια πρόσβασης, οι καθορισμένες προ- και μετα- ενέργειες αντιστοιχίζονται άμεσα σε απαιτούμενες και απαγορευμένες διενέργειες. Η αντιστοίχιση αυτή δεν είναι τόσο προφανής στην περίπτωση των απαγορεύσεων και των υποχρεώσεων όπου η εν λόγω επιτρεπόμενη ενέργεια συμμετέχει στη δομή των προ-ενεργειών˙ οι απαιτούμενες και απαγορευμένες διενέργειες προκύπτουν τελικά από τις συσχετίσεις μεταξύ των προ- και μετα- ενεργειών, καθώς και της ενέργειας πρόσβασης, και ακολουθούν συγκεκριμένα πρότυπα, όπως θα εξηγηθεί στη συνέχεια.

Ο Αλγόριθμος 5 περιγράφει τη διαδικασία εξαγωγής των επιτρεπόμενων ενεργειών, οι οποίες συνιστούν το σύνολο *PermittedActions* (*PA*). Κάθε μέλος του συνόλου αυτού προκύπτει από τις άδειες που έχουν οριστεί στο μοντέλο πολιτικών *PM* και των οποίων οι κύριες ενέργειες είναι τελείως *εξειδικευμένες*, υπό την έννοια ότι οι οντότητες που τις απαρτίζουν αναφέρονται σε στοιχεία του μοντέλου πληροφοριών που αποτελούν φύλλα των αντίστοιχων *isA* γράφων (εκτός από την περίπτωση που αυτές είναι ορισμένες στο επίπεδο προσδιορισμού). Οι ενέργειες αυτές συνιστούν το σύνολο *PermittedLeafActions* (*PLA*) και σε κάθε μία από αυτές αντιστοιχίζεται μία επιτρεπόμενη ενέργεια (*pa*). Εξαίρεση στην αντιστοίχιση αυτή αποτελεί η περίπτωση όπου ο πόρος της εκάστοτε ενέργειας *plaAct* είναι και ο ίδιος ενέργεια. Στην περίπτωση αυτή, και συγκεκριμένα όταν η ενέργεια-πόρος εκτελείται εντός κάποιου τρίτου οργανισμού, κρίνεται ότι η εργασία της οποίας η εγκυρότητα θα ελεγχθεί θα αφορά την εκτέλεση της ενέργειας-πόρου, οπότε η επιτρεπόμενη ενέργεια τελικά αντιστοιχίζεται σε αυτήν και όχι στην ενέργεια πρόσβασης. Επιπλέον, όπως έχει ήδη

ειπωθεί, σε αυτήν την περίπτωση θα πρέπει να προσδιορίζεται και ο επιτρεπτός εκκινητής της εν λόγω αλληλεπίδρασης, ο οποίος αντιστοιχεί στο δράστη της ενέργειας πρόσβασης.

**Αλγόριθμος 5** GeneratePermittedActions

**Input:** *PM*
**Output:** *PM*
1: $PA \leftarrow \emptyset$
2: $PLA \leftarrow$ FindPermissionsForLeafMainActions()
3: **for each** $pla$ **in** $PLA$ **do**
4: $plaAct \leftarrow pla$.action
5: **if** $plaAct$.resource $isNot\ action$ **then**
6: $pa$.action $\leftarrow plaAct$
7: **else**
8: $pa$.action $\leftarrow plaAct$.resource
9: $pa$.initiator $\leftarrow plaAct$.actor
10: **end if**
11: $pa$.purpose $\leftarrow pla$.purpose
12: $pa$.context $\leftarrow pla$.context
13: $pa \leftarrow$ CreateOfflineRequiredActionStructures($pa$)
14: $PA$.add($pa$)
15: **end for**
16: **return** *PM*

Μετά τη δημιουργία μίας επιτρεπόμενης ενέργειας, αυτή συσχετίζεται θετικά ή αρνητικά με τις απαιτούμενες διενέργειες (γραμμή 13). Η αναζήτηση των σχετικών κανόνων λαμβάνει υπόψη το σκοπό και τις συνθήκες πλαισίου που καθιστούν κατ' αρχήν έγκυρη την ενέργεια αναφοράς (με βάση το συσχετισμό τους με το αντίστοιχο στιγμιότυπο της κλάσης `PermittedActions`). Ο τρόπος με τον οποίο προκύπτουν οι απαιτούμενες διενέργειες περιγράφεται σε υψηλό επίπεδο μέσω του Αλγόριθμου 6, η λογική πίσω από τον οποίο αναλύεται στα ακόλουθα στάδια:

(i) Αρχικά, αναζητούνται οι κανόνες στους οποίους η πρωτότυπη ενέργεια στην οποία αναφέρεται η επιτρεπόμενη ενέργεια αποτελεί την ενέργεια πρόσβασης. Για κάθε τέτοιον κανόνα:

- Αν ο κανόνας είναι άδεια:
  - Κάθε θετική προ-/μετα- ενέργεια —υπό την έννοια ότι συνδέεται με τον εν λόγω κανόνα μέσω των ιδιοτήτων `requiresPreAction` ή `prescribesPostAction`— επιβάλλει την παρουσία της αντίστοιχης ενέργειας για την εκτέλεση της υπό εξέταση ενέργειας και, συνεπώς, προστίθεται στο σύνολο των απαιτούμενων διενεργειών *RequiredActionStructures* (*RAS*) .
  - Αντίστοιχα, κάθε αρνητική προ-/μετα- ενέργεια απαγορεύει την παρουσία της αντίστοιχης ενέργειας με δεδομένη την εκτέλεση της υπό εξέταση ενέργειας και, συνεπώς, προστίθεται στο σύνολο των απαγορευμένων διενεργειών *ForbiddenActionStructures* (*FAS*).

- Στην περίπτωση που ο κανόνας είναι απαγόρευση, εξετάζονται μόνο οι προ-ενέργειες του κανόνα, καθώς ο σκοπός είναι να μην ενεργοποιηθεί ποτέ η εν λόγω απαγόρευση ώστε να προκαλέσει την εκτέλεση της αντίστοιχης μετα-ενέργειας. Η αντιστοίχιση στα σύνολα *RAS* και *FAS* γίνεται κατά τρόπο αντίστροφο από εκείνον για την περίπτωση των αδειών:
  - Κάθε θετική προ-/μετα- ενέργεια υποδηλώνει την ενεργοποίηση της απαγόρευσης που αφορά την εκτέλεση της υπό εξέταση ενέργειας και, συνεπώς, προστίθεται στο σύνολο *FAS*.
  - Κάθε αρνητική προ-ενέργεια προστίθεται στο σύνολο *RAS*, με τη λογική ότι η παρουσία/προσθήκη της εν λόγω προ-ενέργειας σε κάποιον διμερή συσχετισμό θα άρει την απαγόρευση για την ενέργεια πρόσβασης.

(ii) Στη συνέχεια, αναζητούνται οι απαγορεύσεις και οι υποχρεώσεις στις οποίες η πρωτότυπη ενέργεια στην οποία αναφέρεται η επιτρεπόμενη ενέργεια συμμετέχει στη δομή των προ-ενεργειών ως θετική προ-ενέργεια, θεωρώντας δεδομένη την εκτέλεσή της, ενεργοποιώντας έτσι (μερικώς, αν δεν αποτελεί τη μοναδική προ-ενέργεια) τους κανόνες που ικανοποιούν τα κριτήρια[18]. Οι ενέργειες που θα συγκεντρωθούν σε αυτό το βήμα ουσιαστικά αποτελούν μετα-ενέργειες αναφορικά με την εκτέλεση της υπό εξέταση ενέργειας.

- Στην περίπτωση των απαγορεύσεων, η ενέργεια πρόσβασης του κανόνα απαγορεύεται να εκτελεστεί με δεδομένη την εκτέλεση της υπό εξέταση ενέργειας και, συνεπώς, προστίθεται στο σύνολο *FAS*. Εάν η υπό εξέταση ενέργεια είναι λογικά συσχετισμένη με άλλες στη δομή των προ-ενεργειών, οι λογικά συσχετισμένες με αυτήν ενέργειες συνιστούν προϋποθέσεις ώστε να θεωρηθεί τελικά η ενέργεια πρόσβασης απαγορευμένη. Για παράδειγμα, αν η προ-ενέργεια αναφέρεται στη λογική σχέση $A \wedge B$, όπου $A$ η υπό εξέταση ενέργεια της οποίας η εκτέλεση θεωρείται δεδομένη, τότε η ενέργεια πρόσβασης $\Gamma$ κρίνεται απαγορευμένη με την προϋπόθεση ότι θα έχει προηγηθεί η ενέργεια $B$. Εάν η υπό εξέταση ενέργεια συμμετέχει σε σκελετό, ολόκληρος ο σκελετός θεωρείται προϋπόθεση για να αποτελέσει η ενέργεια πρόσβασης του κανόνα απαγορευμένη ενέργεια.
- Από την άλλη πλευρά, στην περίπτωση των υποχρεώσεων, η ενέργεια πρόσβασης του κανόνα αντιστοιχεί σε μία ενέργεια που θα πρέπει να έπεται της υπό εξέταση ενέργειας και, επομένως, προστίθεται στο σύνολο *RAS*. Εάν η υπό εξέταση ενέργεια συμμετέχει σε κάποια λογική σχέση ή σκελετό, ο χειρισμός είναι ο ίδιος με την περίπτωση των απαγορεύσεων. Επιπλέον, σε αυτήν την περίπτωση, οι μετα-ενέργειες του κανόνα υποδεικνύουν επιπρόσθετες ενέργειες που θα πρέπει να συμπληρώνουν την υπό εξέταση ενέργεια και προστίθενται κατάλληλα είτε στο σύνολο *RAS* είτε στο σύνολο *FAS*, ανάλογα με το πρόσημό τους στον κανόνα. Έτσι, όταν στον κανόνα προδιαγράφονται μετα-ενέργειες, τότε αυτές

[18]Και σε αυτήν την περίπτωση, μόνο οι προ-ενέργειες έχουν νόημα.

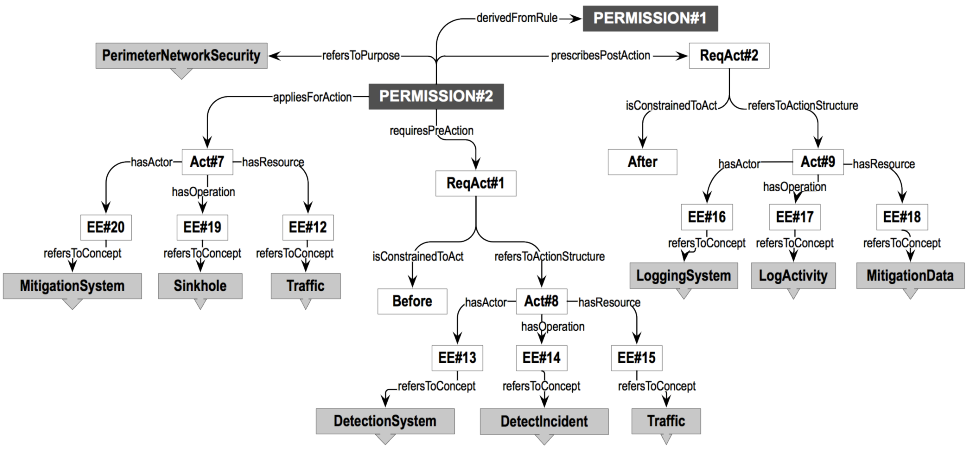
αποτελούν μετασυνθήκες για την απαιτούμενη ενέργεια που προκύπτει από την ενέργεια πρόσβασης, όπως αντίστοιχα η ενέργεια πρόσβασης αποτελεί προϋπόθεση για την απαιτούμενη ή απαγορευμένη ενέργεια που αντιστοιχεί στην εκάστοτε μετα-ενέργεια. Με τον τρόπο αυτό, διατηρούνται οι συσχετίσεις μεταξύ των διαφόρων ενεργειών που περιλαμβάνει ο κανόνας.

**Αλγόριθμος 6** CreateOfflineRequiredActionStructures

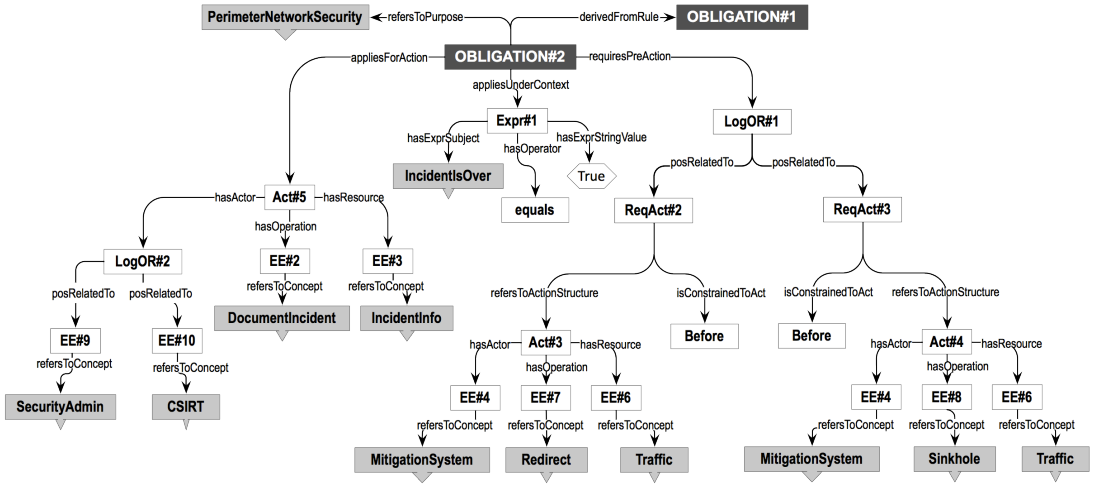
**Input:** *pa*
**Output:** *pa*
1: $PMACT \leftarrow \emptyset$
2: $PMACT \leftarrow$ FindPermissionsWithMainAction($pa$)
3: **for each** $pmAct$ **in** $PMACT$ **do**
4: $pa \leftarrow$ CreateOfflineRequiredActionStructuresFromMainAction($pmAct$, $pa$)
5: **end for**
6: $PRMACT \leftarrow \emptyset$
7: $PRMACT \leftarrow$ FindProhibitionsWithMainAction($pa$)
8: **for each** $prmAct$ **in** $PRMACT$ **do**
9: $pa \leftarrow$ CreateOfflineRequiredActionStructuresFromMainAction($prmAct$, $pa$)
10: **end for**
11: $PRPREACT \leftarrow \emptyset$
12: $PRPREACT \leftarrow$ FindProhibitionsWithPreAction($pa$)
13: **for each** $prpreAct$ **in** $PRPREACT$ **do**
14: $pa \leftarrow$ CreateOfflineRequiredActionStructuresFromPreAction($prpreAct$, $pa$)
15: **end for**
16: $OBPREACT \leftarrow \emptyset$
17: $OBPREACT \leftarrow$ FindObligationsWithPreAction($pa$)
18: **for each** $obpreAct$ **in** $OBPREACT$ **do**
19: $pa \leftarrow$ CreateOfflineRequiredActionStructuresFromPreAction($obpreAct$, $pa$)
20: **end for**
21: **return** *pa*

Τέλος, στο Σχήμα 12 παρουσιάζεται η εξαγωγή μίας επιτρεπόμενης ενέργειας (Σχήμα 12γ′) από την άδεια του Σχήματος 12α′, σε συνδυασμό με την υποχρέωση του Σχήματος 12β′. Η άδεια `Permission#2` αποτελεί τη βάση της επιτρεπόμενης ενέργειας, καθώς η τελευταία θα αναφέρεται στην ενέργεια πρόσβασης `Act#7`. Έτσι, η επιτρεπόμενη ενέργεια `PermittedAct#1` αφορά τελικά την ενέργεια `Act#7`, ενώ επίσης ορίζονται οι απαιτούμενες διενέργειες `OffReqActStr#1` και `OffReqActStr#2` σε αντιστοιχία με τις προ- και μετα-ενέργειες της άδειας (στιγμιότυπα `ReqAct#1` και `ReqAct#2`). Η αναζήτηση κανόνων όπου η ενέργεια ⟨`MitigationSystem`, `Sinkhole`, `Traffic`⟩ αποτελεί προ-ενέργεια, για το σκοπό `PerimeterNetworkSecurity`, οδηγεί στην υποχρέωση `Obligation#2`, όπου η εν λόγω ενέργεια συμμετέχει στη δομή `LogOR#1`, οπότε η εκτέλεσή της θα ενεργοποιήσει τελικά τον κανόνα. Η ενέργεια `Act#5`, η οποία ουσιαστικά αποτελεί μετα-ενέργεια για την υπό εξέταση ενέργεια, σε συνδυασμό με τις συνθήκες πλαισίου που διατυπώνονται μέσω της έκφρασης `Expr#1`, οδηγεί στην προσθήκη της απαιτούμενης διενέργειας `OffReqActStr#3` στην επιτρε-

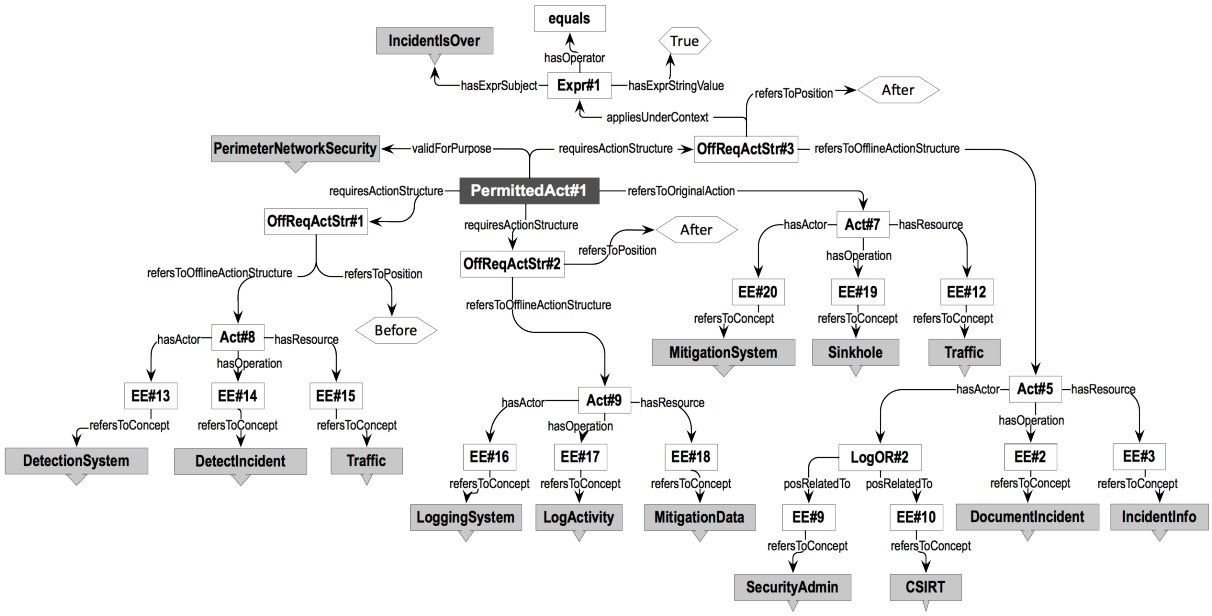
πόμενη ενέργεια PermittedAct#1. Έτσι, ένα ερώτημα σχετικά με την εγκυρότητα της ενέργειας ⟨MitigationSystem, Sinkhole, Traffic⟩ θα επέστρεφε τον έγκυρο σκοπό Perimeter-NetworkSecurity, τις έγκυρες συνθήκες πλαισίου Expr#1, καθώς και τις απαιτούμενες διενέργειες OffReqActStr#1, OffReqActStr#2 και OffReqActStr#3.




(α′) Άδεια στην οποία βασίζεται η επιτρεπόμενη ενέργεια




(β′) Υποχρέωση που αφορά την επιτρεπόμενη ενέργεια ως προ-ενέργεια. Η ενέργεια στην οποία αναφέρεται η επιτρεπόμενη ενέργεια ενεργοποιεί ουσιαστικά την εν λόγω υποχρέωση.




(γ′) Επιτρεπόμενη Ενέργεια. Συνιστά αποτέλεσμα συνδυασμού των παραπάνω κανόνων.

Σχήμα 12: Εξαγωγή Επιτρεπόμενης Ενέργειας

# Κεφάλαιο 7

# Αποτίμηση Αιτημάτων

Το κεφάλαιο αυτό πραγματεύεται θέματα εξαγωγής γνώσης και λήψης αποφάσεων σε πραγματικό χρόνο. Το κέντρο βάρους της αντίστοιχης συλλογιστικής είναι ο διμερής συσχετισμός, όπως τεκμηριώθηκε στο Κεφάλαιο 3, που αντανακλά την αλληλεπίδραση μεταξύ δύο συστημάτων. Έχοντας ως αφετηρία τη λήψη ενός διμερούς συσχετισμού, το σύστημα τον αξιολογεί και αποφαίνεται αναφορικά με την εκτέλεσή του, σε ό,τι αφορά τόσο τους επιτρεπτούς συνδυασμούς εκτέλεσης, όσο και τις συμπληρωματικές οδηγίες που πρέπει να ακολουθηθούν.

Κατά τη διάρκεια της *Διαδικασίας Επαλήθευσης ενός Διμερούς Συσχετισμού*, ο εν λόγω συσχετισμός αναλύεται και αποσυντίθεται στις στοιχειώδεις εργασίες που αντιστοιχούν σε επιτρεπόμενες ενέργειες. Αυτή η μετατροπή καθοδηγείται ουσιαστικά από το στόχο της συμμόρφωσης με τις πολιτικές ασφάλειας και προστασίας της ιδιωτικότητας και, σε αυτό πλαίσιο, πραγματοποιούνται οι αναγκαίοι έλεγχοι και, όπου κρίνεται απαραίτητο, οι κατάλληλες τροποποιήσεις, προκειμένου ο τελικός διμερής συσχετισμός να είναι σύμφωνος με τις υποκείμενες πολιτικές. Σε αυτό το πλαίσιο, η διαδικασία επαλήθευσης θεμελιώνεται στο Μοντέλο Ελέγχου Πρόσβασης και Χρήσης, καθώς αυτό περιλαμβάνει όλες τις έννοιες που προσδιορίζονται από την επεξεργασία των νομικών απαιτήσεων, ενώ οι κανόνες που προδιαγράφει υλοποιούν τις αρχές της αναγκαιότητας, της αναλογικότητας, της επάρκειας, της ελαχιστοποίησης και της ελεγχόμενης πρόσβασης. Η διαδικασία εξαγωγής γνώσης που πραγματοποιείται σε αυτό το στάδιο καλείται *Εξαγωγή Γνώσης Πραγματικού Χρόνου* (online), και βασίζεται σε μεγάλο βαθμό στα αποτελέσματα της διαδικασίας εξαγωγής γνώσης μη πραγματικού χρόνου, η οποία περιγράφηκε στο Κεφάλαιο 6.

Η διαδικασία επαλήθευσης ενός διμερούς συσχετισμού ολοκληρώνεται με τη δημιουργία των κατάλληλων *Οδηγιών Εξουσιοδότησης* που θα πρέπει να εφαρμοστούν στον υπό εξέταση συσχετισμό, ώστε αυτός να ενσωματώνει τις απαιτήσεις που υπαγορεύει το Μοντέλο Ελέγχου Πρόσβασης και Χρήσης.

## 7.1 Οδηγίες Εξουσιοδότησης

Ένας διμερής συσχετισμός κρίνεται έγκυρος όταν μέσω διαδικασίας συλλογιστικής προκύψουν για αυτόν οδηγίες εξουσιοδότησης. Συγκεκριμένα, η δημιουργία τουλάχιστον μίας *Οδηγίας Εγκυρότητας Διμερούς Συσχετισμού* αποτελεί απαραίτητη προϋπόθεση για να χαρακτηριστεί ένας συσχετισμός κατ' αρχήν έγκυρος, ωστόσο οι οδηγίες εγκυρότητας ενδέχεται να συμπληρώνονται από οδηγίες άλλου τύπου που καθιστούν τελικά έγκυρο το συσχετισμό και αφορούν τρίτες εργασίες οι οποίες απαιτείται ή απαγορεύεται να προηγούνται, να έπονται ή να εκτελούνται παράλληλα με εκείνες του συσχετισμού, καθώς και οδηγίες που αφορούν ροή δεδομένων.

Με βάση τα παραπάνω, διακρίνουμε τους εξής τύπους οδηγιών εξουσιοδότησης:

**Οδηγίες Εγκυρότητας Διμερούς Συσχετισμού** Κάθε οδηγία εγκυρότητας διμερούς συσχετισμού (*Bilateral Validity Directive – BVD*) αναφέρεται σε ένα διμερή συσχετισμό στο σύνολό του, υποδεικνύοντας αφενός έναν έγκυρο συνδυασμό δραστών—λειτουργίας—πόρων για καθεμία από τις εμπλεκόμενες εργασίες, και αφετέρου μία έγκυρη συσχέτιση μεταξύ τους. Η τελευταία, στην απλή περίπτωση, περιλαμβάνει τον ορισμό της ακμής που ενώνει τις δύο εργασίες (μεταφερόμενες οντότητες πληροφορίας, συνθήκες, κλπ.), ο οποίος μπορεί να συμπίπτει ή όχι με εκείνον του αρχικού διμερούς συσχετισμού, ενώ σε κάποια πιο σύνθετη δύναται να προδιαγράφει επιπλέον την παρεμβολή ενός ή περισσότερων εργασιών, απαραίτητων για τη σύννομη ανταλλαγή δεδομένων μεταξύ των αρχικών εργασιών (π.χ., κάποια εργασία κρυπτογράφησης ή άλλου είδους μετασχηματισμού). Επιπρόσθετα, κάθε τέτοια οδηγία περιλαμβάνει αναφορά σε ένα ακριβώς ζεύγος εκκινητή–σκοπού, συνδέοντας την ισχύ της με τις συγκεκριμένες οντότητες. Όλοι οι υπόλοιποι τύποι οδηγιών συσχετίζονται πάντα με κάποια οδηγία εγκυρότητας.

**Οδηγίες Απαίτησης Εκτέλεσης** Μία οδηγία απαίτησης εκτέλεσης (*Task Presence Directive – TPD*) χρησιμοποιείται για να εκφράσει ότι μία έγκυρη εργασία, όπως προδιαγράφεται σε μία οδηγία εγκυρότητας διμερούς συσχετισμού, απαιτεί την ύπαρξη μίας άλλης εργασίας ή δομής εργασιών, πιθανώς υπό ορισμένες συνθήκες πλαισίου, προϋποθέσεις ή μετασυνθήκες. Πέρα από τις απαιτούμενες αυτές εργασίες, η οδηγία υποδεικνύει επίσης τη σχετική ή ακριβή θέση ή συσχέτιση σε επίπεδο ανταλλαγής δεδομένων που χαρακτηρίζουν τις πρώτες ως προς την εργασία αναφοράς.

**Οδηγίες Απαγόρευσης Εκτέλεσης** Οι οδηγίες απαγόρευσης εκτέλεσης (*Task Forbiddance Directives – TFD*) απαγορεύουν την εκτέλεση κάποιων εργασιών εν όψει της παρουσίας κάποιων άλλων εργασιών, όπως αυτές προκύπτουν από τις αντίστοιχες οδηγίες εγκυρότητας διμερούς συσχετισμού. Έτσι, κάθε τέτοια οδηγία αναφέρεται σε μία οδηγία εγκυρότητας, καθώς και σε εκείνη την εργασία του συσχετισμού που ενεργοποιεί την απαγόρευση, προσ-

διορίζοντας την εργασία ή εργασίες, με τις οποίες η υπό εξέταση εργασία έρχεται σε σύγκρουση, είτε γενικά είτε αν οι εν λόγω εργασίες εκτελούνται σε κάποια σχετική ή απόλυτη θέση ως προς την εργασία αναφοράς. Ομοίως, μία απαγόρευση μπορεί να ισχύει μόνο υπό συγκεκριμένες συνθήκες πλαισίου, προϋποθέσεις ή μετασυνθήκες.

**Οδηγίες Απαίτησης Εισόδου** Μία οδηγία απαίτησης εισόδου (*Input Requirement Directive – IRD*) υποδεικνύει ότι κάποια εργασία χρειάζεται να λάβει κάποια δεδομένα ως είσοδο (για την εργασία-προορισμό αυτό μεταφράζεται σε επιπλέον δεδομένα εκτός από αυτά που λαμβάνει σύμφωνα με την προσδιορισμένη ακμή του συσχετισμού). Συνδέεται με μία οδηγία εγκυρότητας, δείχνοντας επιπλέον στη μέσα σε αυτή ορισμένη εργασία που πρέπει να λάβει τα δεδομένα, και εμπεριέχει τα δεδομένα εισόδου που πρέπει να παρασχεθούν, υποδεικνύοντας, αν χρειάζεται, και την εργασία ή δομή εργασιών από τις οποίες τα δεδομένα αυτά πρέπει να προέρχονται. Και εδώ είναι δυνατός ο ορισμός συνθηκών πλαισίου, προϋποθέσεων και μετασυνθηκών.

**Οδηγίες Απαγόρευσης Εισόδου** Οι οδηγίες απαγόρευσης εισόδου (*Input Forbiddance Directives – IFD*) αναφέρονται σε έναν έγκυρο διμερή συσχετισμό, απαγορεύοντας τη μεταφορά συγκεκριμένης πληροφορίας προς κάποια από τις εργασίες που περιλαμβάνονται σε αυτόν. Η οδηγία δείχνει στη σχετική εργασία, υποδεικνύοντας τα δεδομένα εισόδου που η τελευταία απαγορεύεται να λάβει, καθώς και, πιθανώς, την εργασία από την οποία αυτά δεν πρέπει να προέρχονται. Σε αντιστοιχία με τις άλλες οδηγίες, υπάρχει δυνατότητα περιορισμού της απαγόρευσης από συνθήκες πλαισίου, προϋποθέσεις ή μετασυνθήκες.

## 7.2 Διαδικασία Επαλήθευσης Διμερούς Συσχετισμού

Στο πλαίσιο της διαδικασίας επαλήθευσης ενός διμερούς συσχετισμού, η Μηχανή Συμπερασμού λαμβάνει ως είσοδο τον υπό εξέταση διμερή συσχετισμό, καθώς και τους δεδηλωμένους σκοπούς που ο εν λόγω συσχετισμός υποτίθεται πως εξυπηρετεί, σε συνδυασμό με τους δεδηλωμένους πιθανούς εκκινητές, δηλαδή ζεύγη σκοπών-εκκινητών. Ο Αλγόριθμος 7 περιγράφει σε υψηλό επίπεδο τη διαδικασία επαλήθευσης ενός διμερούς συσχετισμού, τα βασικά στάδια της οποίας είναι τα ακόλουθα:

1. Έλεγχος συμμόρφωσης σκοπών
2. Εξαγωγή των αυτόνομα έγκυρων εργασιών από τις αρχικές εργασίες που περιλαμβάνει ο υπό εξέταση συσχετισμός
3. Επαλήθευση στο επίπεδο του ίδιου του διμερούς συσχετισμού, όπως αυτός προκύπτει με βάση το προηγούμενο βήμα

**Αλγόριθμος 7** VerifyBilateralAssociation

**Input:** *PIP*, *ba*
**Output:** *DIR*

```
 1: LPIP ← GenerateLeafPIPs(PIP)
 2: src ← ExtractBilateralAssociationSourceTask(ba)
 3: dst ← ExtractBilateralAssociationDestinationTask(ba)
 4: BAO ← ExtractBilateralAssociationOperations(ba)
 5: DIR ← ∅
 6: for each lpip in LPIP do
 7:    pipIsValid ← VerifyPIP(lpip, BAO)
 8:    if pipIsValid then
 9:       SAVST ← CheckStandAloneTaskValidity(srct, lpip)
10:       SAVDT ← CheckStandAloneTaskValidity(dstt, lpip)
11:       BA′ ← ∅
12:       if SAVST ≠ ∅ && SAVDT ≠ ∅ then
13:          BA′ ← GeneratePotentiallyValidBAs(SAVST, SAVDT)
14:       end if
15:       for each ba′ in BA′ do
16:          DIR.add(VerifyMetaAssociation(ba′, ba, lpip))
17:       end for
18:    end if
19: end for
20: return DIR
```

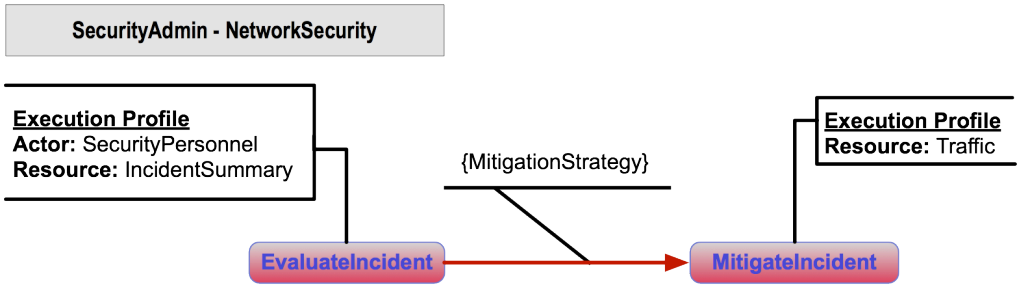
Έχοντας σαν αφετηρία το αρχικό σύνολο ζευγών σκοπών-εκκινητών *PurposeInitiatorPairs* (*PIP*), αρχικά εξάγονται τα ζεύγη που αποτελούνται από στοιχεία-φύλλα των αντίστοιχων *isA* γράφων, δηλαδή σκοπούς και ρόλους που δεν μπορούν να εξειδικευθούν περαιτέρω, τα οποία συνιστούν το σύνολο των ζευγών φύλλων *LeafPurposeInitiatorPairs* (*LPIP*) (γραμμή 1). Επίσης, από το διμερή συσχετισμό (*bilateral association — ba*) εξάγονται η εργασία-αφετηρία (*source task — src*) και η εργασία-προορισμός (*destination task — dst*) και εν συνεχεία, εξάγονται οι αντίστοιχες λειτουργίες (σύνολο *BilateralAssociationOperations — BAO*) (γραμμές 2—4).

Έτσι, τα παραπάνω στάδια πραγματοποιούνται για κάθε ζεύγος *lpip* του συνόλου *LPIP* (γραμμές 6–19), ώστε τελικά οι οδηγίες (σύνολο *Directives — DIR*) που θα προκύψουν να αναφέρονται σε ένα συγκεκριμένο σκοπό και έναν συγκεκριμένο ρόλο εκκινητή. Εάν το εκάστοτε ζεύγος αποδειχθεί έγκυρο, μέσω του ελέγχου συμμόρφωσης σκοπών (γραμμή 7), ο επόμενος έλεγχος αφορά την αυτόνομη εγκυρότητα καθεμίας από τις εργασίες που περιλαμβάνονται αρχικά στο συσχετισμό (γραμμές 9—10). Μία εργασία κρίνεται αυτόνομα έγκυρη, όταν αντιστοιχεί σε τουλάχιστον μία επιτρεπόμενη ενέργεια, δηλαδή η εργασία είναι τυπικά έγκυρη για κάποιο δεδομένο σκοπό και κάποιο δεδομένο εκκινητή, χωρίς να λαμβάνονται υπόψη σε αυτό το στάδιο ενδεχόμενοι περιορισμοί σχετικοί με την εκτέλεσή της ή συγκρούσεις με άλλες εργασίες. Για καθεμία αρχική εργασία είναι δυνατόν να προκύψουν περισσότερες από μία αυτόνομα έγκυρες εργασίες, οι οποίες συνιστούν τα σύ-

νολα *SAVST* και *SAVDT* που περιέχουν αντίστοιχα τις αυτόνομα έγκυρες εργασίες για την εργασία-αφετηρία και την εργασία-προορισμό του αρχικού διμερούς συσχετισμού. Τα μέλη των συνόλων αυτών χρησιμοποιούνται στη συνέχεια για το σχηματισμό ενός ή περισσότερων *μετασυσχετισμών* (σύνολο *BA′*) με βάση την αντιστοίχιση των αυτόνομα έγκυρων εργασιών προς τις αρχικές (γραμμή 13).

Τέλος, για καθέναν από τους διμερείς μετασυσχετισμούς που προέκυψαν ως αποτέλεσμα της παραπάνω διαδικασίας, οι οποίοι πλέον περιλαμβάνουν αυτόνομα έγκυρες εργασίες, ελέγχεται ο συσχετισμός καθεαυτός (γραμμές 15—17). Ο έλεγχος αυτός περιλαμβάνει διάφορα επιμέρους στάδια, όπως είναι ο έλεγχος της αλληλεπίδρασης μεταξύ των δύο εργασιών, ο εντοπισμός τρίτων εργασιών που καθιστούν τελικά έγκυρο το συσχετισμό ή εργασιών που έρχονται σε σύγκρουση με τις εργασίες του εν λόγω συσχετισμού. Σε αυτό το στάδιο δημιουργούνται τελικά οι οδηγίες εξουσιοδότησης που αφορούν τον υπό εξέταση συσχετισμό˙ εφόσον δεν προκύπτουν οδηγίες, αυτό μεταφράζεται ως απαγόρευση εκτέλεσής του σε οποιαδήποτε μορφή του.

Καθένα από τα παραπάνω βήματα παρουσιάζεται σε μεγαλύτερο βάθος στις ενότητες που ακολουθούν. Στο Σχήμα 13 απεικονίζεται ένας υπό εξέταση διμερής συσχετισμός, ο οποίος θα χρησιμοποιηθεί ως παράδειγμα στις επόμενες ενότητες. Οι εργασίες που περιλαμβάνει αφορούν την αξιολόγηση ενός περιστατικού (`EvaluateIncident`) από το προσωπικό ασφάλειας (`SecurityPersonnel`) στη βάση της περιγραφής του εν λόγω περιστατικού (`IncidentSummary`), καθώς και τη μετέπειτα αντιμετώπισή του (`MitigateIncident`) σύμφωνα με τις οδηγίες (`MitigationStrategy`) του προσωπικού ασφάλειας. Εκκινητή της αλληλεπίδρασης αποτελεί ο ρόλος του διαχειριστή ασφάλειας (`SecurityAdmin`), ενώ ο σκοπός που εξυπηρετεί ο συσχετισμός είναι εκείνος της ασφάλειας του δικτύου (`NetworkSecurity`). Μάλιστα, θεωρώντας τους δύο πιο εξειδικευμένους σκοπούς `PerimeterNetworkSecurity` και `CollaborativeNetworkSecurity`, προκύπτουν τελικά μέσω της διαδικασίας που περιγράφηκε παραπάνω δύο ζεύγη σκοπών-εκκινητών για τα οποία θα εξεταστεί η εγκυρότητα του διμερούς συσχετισμού (⟨`PerimeterNetworkSecurity`, `SecurityAdmin`⟩ και ⟨`CollaborativeNetworkSecurity`, `SecurityAdmin`⟩).




Σχήμα 13: Υπό εξέταση διμερής συσχετισμός

## 7.3 Έλεγχος Συμμόρφωσης Σκοπών

Η συμμόρφωση των δεδηλωμένων σκοπών που ο υπό εξέταση διμερής συσχετισμός υποτίθεται πως εξυπηρετεί με εκείνους που πραγματικά είναι σε θέση να εξυπηρετήσει εξετάζεται ως προς δύο διαστάσεις, οι οποίες αντιστοιχούν στα δύο σχετικά ερωτήματα που είναι δυνατόν να υποβληθούν:

- Κατά πόσον οι λειτουργίες που περιλαμβάνει ο διμερής συσχετισμός είναι σύμφωνες με τους σκοπούς τους οποίους ο εν λόγω συσχετισμός υποτίθεται πως εξυπηρετεί.
- Κατά πόσον οι ρόλοι που κατέχει ο εκάστοτε εκκινητής της αλληλεπίδρασης δικαιολογούν την εκκίνηση της εκτέλεσης του εν λόγω συσχετισμού, έτσι ώστε να εξυπηρετηθεί κάποιος συγκεκριμένος σκοπός.

Το πρώτο βήμα ώστε να απαντηθούν τα παραπάνω ερωτήματα αποτελεί η εξαγωγή των σκοπών που ο συσχετισμός πράγματι εξυπηρετεί με βάση τους σκοπούς που εξυπηρετούν οι λειτουργίες που περιλαμβάνει. Έτσι, για καθεμία από αυτές τις λειτουργίες συγκεντρώνονται οι σκοποί που αυτή είναι δυνατόν να εξυπηρετεί, μέσω της σχέσης *mayServePurposes* του Σημασιολογικού Μοντέλου Πληροφοριών και οι κοινοί σκοποί (εάν υπάρχουν) συνιστούν το σύνολο *BilateralAssociationPurposes* (*BAP*). Από την άλλη πλευρά, οι δεδηλωμένοι σκοποί που ο υπό εξέταση συσχετισμός υποτίθεται πως εξυπηρετεί απαρτίζουν το σύνολο *DeclaredPurposes* (*DP*) και με αντιπαραβολή των δύο συνόλων είναι τελικά δυνατόν να απαντηθεί το πρώτο ερώτημα. Οι σκοποί που αποτελούν μέλη και των δύο συνόλων—εάν υπάρχουν τέτοιοι κοινοί σκοποί— συνιστούν τους έγκυρους σκοπούς Οι δεδηλωμένοι σκοποί οι οποίοι δεν περιέχονται στο σύνολο *BAP* δε γίνονται αποδεκτοί.

Για την απάντηση του δεύτερου ερωτήματος, συγκεντρώνονται οι σκοποί για τους οποίους είναι δυνατόν να ενεργεί ο κάθε ρόλος που κατέχει ο εκκινητής της αλληλεπίδρασης, μέσω της σχέσης *mayActForPurposes* του Σημασιολογικού Μοντέλου Πληροφοριών. Οι σκοποί αυτοί συνιστούν το σύνολο *InitiatorPurposes* και αντιπαραβάλλονται με τους έγκυρους σκοπούς που ο συσχετισμός είναι δυνατόν να εξυπηρετεί. Οι κοινοί σκοποί αποτελούν τους σκοπούς για τους οποίους ο εκάστοτε ρόλος μπορεί να εκκινήσει την εκτέλεση του εν λόγω συσχετισμού.

Με βάση τα παραπάνω, το βήμα του ελέγχου συμμόρφωσης σκοπών του Αλγόριθμου 7 αναλύεται όπως φαίνεται στον Αλγόριθμο 8, και το εκάστοτε ζεύγος *pip* κρίνεται έγκυρο, εάν τόσο οι κοινοί σκοποί που εξυπηρετούν οι λειτουργίες που περιλαμβάνονται στο διμερή συσχετισμό, όσο και οι σκοποί για τους οποίους μπορεί να δράσει ο ρόλος του εκκινητή, περιέχουν το σκοπό του δεδομένου ζεύγους.

Σημειώνεται ότι σε όλους τους ελέγχους λαμβάνονται επίσης υπόψη οι ιεραρχικές σχέσεις μεταξύ σκοπών και λειτουργιών. Επίσης, στην περίπτωση που οι σκοποί που πρόκειται να εξυπηρετήσει ένας διμερής συσχετισμός δε δηλώνονται εξαρχής, αυτοί υπο-

**Αλγόριθμος 8** VerifyPIP

**Input:** *pip*, *BAO*
**Output:** *pipIsValid*
1: $pipIsValid \leftarrow$ VerifyOperationsAgainstPurpose(*pip*, *BAO*)
2: &&VerifyInitiatorAgainstPurpose(*pip*)
3: **return** *pipIsValid*

λογίζονται από τη Μηχανή Συμπερασμού όπως περιγράφηκε στο πρώτο βήμα, ενώ εάν δεν έχουν προσδιοριστεί οι πιθανοί εκκινητές, τότε για κάθε συμβατό σκοπό εξάγονται οι έγκυροι εκκινητές μέσω της σχέσης *mayActForPurposes*. Τέλος, εάν δεν έχουν προσδιοριστεί ούτε οι πιθανοί εκκινητές ούτε οι σκοποί, τα έγκυρα ζεύγη εξάγονται συνδυάζοντας τις δύο προηγούμενες περιπτώσεις.

## 7.4 Εξαγωγή των Αυτόνομα Έγκυρων Εργασιών

Στο βήμα αυτό ελέγχεται η αυτόνομη εγκυρότητα των εργασιών του διμερούς συσχετισμού, δηλαδή ανεξάρτητα από λοιπούς περιορισμούς που αφορούν την εγκυρότητα της εκάστοτε εργασίας, πέρα από το σκοπό τον οποίο ο συσχετισμός εξυπηρετεί και το ρόλο του εκκινητή του. Θεωρούμε ότι μία εργασία είναι έγκυρη κατ' αυτόν τον τρόπο, αν υπάρχει τουλάχιστον μία επιτρεπόμενη ενέργεια (βλ. Ενότητα 6.2.1), δηλαδή μία κατ' αρχήν έγκυρη ενέργεια, η οποία να αντιστοιχεί στην εν λόγω εργασία. Μία εργασία μπορεί να αποδειχθεί τελικά έγκυρη όπως ακριβώς έχει οριστεί, ωστόσο είναι πιθανό κάποια από τα στοιχεία που την απαρτίζουν να αντικατασταθούν μέσω της διαδικασίας αυτής από άλλα *σχετικά* στοιχεία, ισοδύναμα προς τα αρχικά, για τα οποία επιτρέπεται τελικά η ενέργεια πρόσβασης. Επίσης, μέσω της διαδικασίας αυτής, συμπληρώνονται τα στοιχεία της εργασίας εκείνα που δεν έχουν προσδιοριστεί εξαρχής κατά την προδιαγραφή του διμερούς συσχετισμού.

Ωστόσο, λόγω των διαφορών που παρουσιάζουν οι εργασίες και οι ενέργειες στον ορισμό τους, στη γενική περίπτωση η αντιστοίχιση αυτή δεν είναι ένα προς ένα (βλ. Ενότητες 3.2.1 και 4.2.1). Πρώτον, κάθε εργασία είναι δυνατόν να συσχετίζεται με περισσότερα του ενός προφίλ εκτέλεσης, τα οποία προσδιορίζουν τη λειτουργία στην οποία αναφέρεται η εργασία, τους δυνητικούς δράστες και τους δυνητικούς πόρους. Ακριβώς σε αυτή τη δομή του προφίλ εκτέλεσης διαφαίνονται οι βασικές διαφορές που εμφανίζει η δομή της εργασίας σε σχέση με εκείνη της ενέργειας. Σε μία ενέργεια προβλέπεται μόνο ένας δράστης ή δράστες λογικά συσχετισμένοι μεταξύ τους με σχέση AND, ενώ στο προφίλ εκτέλεσης μίας εργασίας είναι δυνατόν να περιλαμβάνονται πολλαπλοί δράστες, εναλλακτικοί ή συμπληρωματικοί μεταξύ τους, με χρήση των αντίστοιχων λογικών σχέσεων. Ομοίως, λογικά συσχετισμένοι σε μία εργασία μπορεί να είναι και οι πόροι, ενώ σε μία ενέργεια ο πόρος είναι πάντα ένας, καθώς, όπως έχει ήδη αναφερθεί, στα πλαίσια του ελέγχου πρόσβα-

σης η πρόσβαση εξετάζεται πάντα αναφορικά με κάποιο συγκεκριμένο πόρο. Οι συνθήκες που συμπληρώνουν τον ορισμό ενός προφίλ εκτέλεσης αφορούν παράγοντες που δεν αποτελούν μέρος της προδιαγραφής του διμερούς συσχετισμού (π.χ., εξωγενείς παράμετροι περιβάλλοντος) ή που εκτείνονται πέραν των ορίων της εργασίας και που, συνεπώς, δεν μπορούν να εκφραστούν αποκλειστικά στη βάση των ιδιοτήτων των εμπλεκόμενων οντοτήτων, δηλαδή των δραστών, των πόρων και της λειτουργίας, και αντιστοιχούν στις συνθήκες που είναι συσχετισμένες με την επιτρεπόμενη ενέργεια. Σημειώνεται ότι αν και η λειτουργία είναι κοινή για όλα τα προφίλ, καθώς αυτή ορίζεται μονοσήμαντα και στο επίπεδο της ίδιας της εργασίας, τα διάφορα προφίλ εκτέλεσης ενδέχεται να θέτουν διαφορετικές τιμές στις διάφορες παραμέτρους που συνιστούν τις ρυθμίσεις εκτέλεσης της εν λόγω εργασίας και άλλες ιδιότητές της, μέσω της οντότητας λειτουργίας.

Με βάση τα παραπάνω, προκειμένου να ελεγχθεί η αυτόνομη εγκυρότητα μίας εργασίας, ενδέχεται να είναι απαραίτητος ο έλεγχος της εγκυρότητας περισσότερων της μίας ενεργειών, αφενός λόγω των διαφορετικών προφίλ εκτέλεσης και αφετέρου λόγω των λογικά συσχετισμένων δραστών και πόρων. Η μεθοδολογία που ακολουθείται για να εξαχθούν όλες οι αυτόνομα έγκυρες εργασίες από μία δεδομένη εργασία και κατ' επέκταση να ελεγχθεί η εγκυρότητα της τελευταίας περιγράφεται από τον Αλγόριθμο 9.

Το πρώτο βήμα αφορά στην εξαγωγή των πληροφοριών της υπό εξέταση εργασίας οι οποίες είναι απαραίτητες για την αντιστοίχιση της εν λόγω εργασίας σε μία ή περισσότερες επιτρεπόμενες ενέργειες (γραμμές 2—7). Σε αυτό το πλαίσιο, αρχικά εξάγονται η λειτουργία πάνω στην οποία θεμελιώνεται η εργασία (*taskOperation — tOp*) και τα προφίλ εκτέλεσης που είναι συσχετισμένα με την εργασία (σύνολο *ExecutionProfiles — EP*) και στη συνέχεια, από το κάθε προφίλ εκτέλεσης εξάγονται οι δράστες (σύνολο *Actors — AC*) και οι πόροι (σύνολο *Resources — RES*). Απλοποιημένα, κάθε προφίλ εκτέλεσης ουσιαστικά εξετάζεται σαν ξεχωριστή εργασία και μία εργασία κρίνεται αυτόνομα έγκυρη αν βρεθεί τουλάχιστον μία επιτρεπόμενη ενέργεια που να αντιστοιχεί σε κάποιο από τα προσδιορισμένα προφίλ εκτέλεσης. Αυτό συνεπάγεται ότι οι αυτόνομα έγκυρες εργασίες που τελικά θα προκύψουν θα αφορούν μεν την ίδια εργασία, αλλά θα αναφέρονται σε διαφορετικά προφίλ εκτέλεσης, εφόσον υπάρχουν περισσότερα του ενός προφίλ συσχετισμένα με την εν λόγω εργασία. Επιπλέον, με στόχο να ελαχιστοποιηθούν τα ερωτήματα προς τη Μηχανή Συμπερασμού, ο τελικός διμερής συσχετισμός που θα προκύψει θα πρέπει να περιέχει όσο το δυνατόν πιο εξειδικευμένες έννοιες, οπότε οι οντότητες που συμμετέχουν στην εκάστοτε εργασία αντικαθιστώνται από τις αντίστοιχες οντότητες που αναφέρονται σε στοιχεία-φύλλα του αντίστοιχου γράφου. Σαν αποτέλεσμα, κάθε προφίλ εκτέλεσης είναι δυνατόν να οδηγήσει σε πολλαπλά εξειδικευμένα προφίλ, τα οποία είναι ισοδύναμα προς το αρχικό.

Συνεπώς, για κάθε προφίλ εκτέλεσης συγκεντρώνονται οι πιο εξειδικευμένοι δράστες (σύνολο *LeafActors — LAC*), οι πιο εξειδικευμένες λειτουργίες (σύνολο *LeafOperations — LOP*) και οι πιο εξειδικευμένοι πόροι (σύνολο *LeafResources — LRES*) και για κάθε δυνατό

**Αλγόριθμος 9** CheckStandAloneTaskValidity

**Input:** *t, pip*
**Output:** *SAVT*

```
 1: SAVT ← ∅
 2: EP ← ExtractTaskExecutionProfiles(t)
 3: tOp ← t.operation
 4: LOP ← FindLeafOperations(tOp)
 5: for each ep in EP do
 6:    AC ← ExtractExecutionProfileActors(ep)
 7:    RES ← ExtractExecutionProfileResources(ep)
 8:    for each lop in LOP do
 9:       SAVT_OP ← ∅
10:       if epIsComplete then
11:          for each ac in AC do
12:             PERMACT_AC ← ∅
13:             LAC ← FindLeafActors(ac)
14:             for each lac in LAC do
15:                PERMACT_LAC ← ∅
16:                for each res in RES do
17:                   LRES ← FindLeafResources(res)
18:                   for each lres in LRES do
19:                      PERMACT ← FindPermittedActions(lac, lop, lres, pip)
20:                      if PERMACT = ∅ then
21:                         PERMACT ←
22:                               FindPermittedActionsForLessDetRes(lac, lop, lres, pip)
23:                         if PERMACT = ∅ then
24:                            PERMACT ←
25:                                  FindPermittedActionsForContainedRes(lac, lop, lres, pip)
26:                         end if
27:                      end if
28:                      PERMACT_LAC.add(PERMACT)
29:                   end for
30:                end for
31:                PERMACT_AC.add(PERMACT_LAC)
32:             end for
33:             PERMACT_AC′ ← ClusterAndMergeActions(PERMACT_AC)
34:             SAVT_OP.add(TranslateActionsToTasks(PERMACT_AC′, ep))
35:          end for
36:          SAVT.add(MergeStandAloneValidTasks(SAVT_OP))
37:       end if
38:    end for
39: end for
40: return SAVT
```

συνδυασμό τους ελέγχεται η εγκυρότητά του με την αναζήτηση των επιτρεπόμενων ενεργειών που αναφέρονται στις ίδιες οντότητες και είναι σύμφωνες με το δεδομένο ζεύγος σκοπού-εκκινητή (γραμμές 19—27). Στην περίπτωση που δε βρεθούν επιτρεπόμενες ενέρ-

γειες, οι οποίες να αφορούν την πρόσβαση στον εξειδικευμένο πόρο, τότε αναζητούνται οι επιτρεπόμενες ενέργειες που αναφέρονται σε λιγότερο λεπτομερείς πόρους (για την περίπτωση που ο πόρος αφορά δεδομένα). Εάν και πάλι δε βρεθούν επιτρεπόμενες ενέργειες ή ο παρών πόρος δεν αναφέρεται σε δεδομένα, διερευνάται η πρόσβαση σε συγκεκριμένα τμήματά του, παραπέμποντας στην πράξη της *προβολής* (*projection*) της σχεσιακής άλγεβρας.

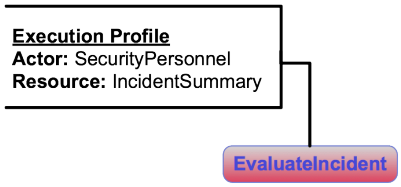
Καθώς οι επιτρεπόμενες ενέργειες που επιστρέφονται αποτελούν προϊόν "αποδόμησης" του προφίλ εκτέλεσης, υπό την έννοια ότι λογικά συσχετισμένοι δράστες και πόροι εξετάζονται στην ουσία ξεχωριστά, θα πρέπει τελικά αυτές να *συγχωνευθούν* (*merging*), ώστε να αποδώσουν πλήρως σημασιολογικά το αρχικό προφίλ εκτέλεσης. Αρχικά εξάγονται οι αυτόνομα έγκυρες εργασίες με βάση το δεδομένο πόρο (γραμμές 16–31). Οι επιτρεπόμενες ενέργειες που βρέθηκαν για τον κάθε δράστη, με χρήση των σχέσεων που δηλώνουν εξειδίκευση, συμπερίληψη και βαθμό λεπτομέρειας, συγχωνεύονται ώστε να αντικατοπτρίζουν κάθε δυνατό συνδυασμό πόρων πάνω στους οποίους ο εν λόγω δράστης επιτρέπεται να επενεργήσει μέσω της δεδομένης λειτουργίας (γραμμή 33) και, κατόπιν, μεταφράζονται στις αντίστοιχες εργασίες (γραμμή 34). Σε αντίθεση με τις αρχικές εργασίες, οι αυτόνομα έγκυρες εργασίες που προκύπτουν φέρουν ένα μοναδικό προφίλ εκτέλεσης. Το επόμενο στάδιο αφορά τη συγχώνευση αυτών των εργασιών, ώστε το νέο προφίλ εκτέλεσης να περιλαμβάνει τους επιτρεπτούς λογικά συσχετισμένους δράστες (γραμμή 36). Κατά τη συγχώνευση, οντότητες που αφορούν εναλλακτικές μεταξύ τους έννοιες συνδέονται λογικά με σχέση OR, ενώ στην περίπτωση που οι έννοιες που συμμετέχουν από κοινού σε κάποια τρίτη συνδέονται μεταξύ τους με σχέση AND[19]. Σημειώνεται ότι κατά τη διαδικασία συγχώνευσης, τόσο στο επίπεδο ενεργειών όσο και στο τελικό επίπεδο εργασιών, η *ομαδοποίηση* (*clustering*) λαμβάνει υπόψη τους περιορισμούς που έχουν οριστεί πάνω στις σχετικές οντότητες, δηλαδή τους δράστες, τις λειτουργίες και τους πόρους, καθώς και τις συνθήκες που συμπληρώνουν το κάθε προφίλ εκτέλεσης και εκείνες που καθιστούν έγκυρες τις ενέργειες. Ουσιαστικά, οι ενέργειες/εργασίες ομαδοποιούνται με τέτοιο τρόπο, ώστε τελικά τα στοιχεία τους να αφορούν πανομοιότυπες, αλληλεπικαλυπτόμενες ή παρεμφερείς οντότητες, δηλαδή οντότητες που αναφέρονται στις ίδιες έννοιες και οι περιορισμοί που έχουν οριστεί σε αυτές είτε να είναι οι ίδιοι, είτε να επικαλύπτονται, είτε να μην έρχονται σε σύγκρουση μεταξύ τους. Τέλος, συγχώνευση πραγματοποιείται και κατά τη φάση μετάφρασης των ενεργειών σε εργασίες μεταξύ των περιορισμών και συνθηκών που ορίζονται πάνω στο προφίλ εκτέλεσης και εκείνων που προδιαγράφονται μέσω των κανόνων του Μοντέλου Ελέγχου Πρόσβασης και Χρήσης· σε περίπτωση συγκρούσεων ή επικάλυψης, προτεραιότητα έχουν οι περιορισμοί εκείνοι που επιβάλλουν οι κανόνες.

Επιστρέφοντας στο διμερή συσχετισμό αναφοράς του Σχήματος 13, για τον έλεγχο της εγκυρότητας της εργασίας-αφετηρίας και τη συνακόλουθη εξαγωγή των αυτόνομα έγκυρων εργασιών, αναζητούνται οι επιτρεπόμενες ενέργειες που αναφέρονται στην ενέρ-

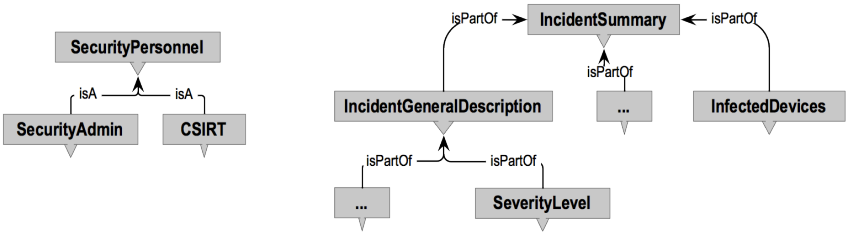
[19]Αυτό ισχύει για οντότητες που προκύπτουν μέσω των σχέσεων του Μοντέλου Πληροφοριών από τις ρητά ορισμένες στην εργασία οντότητες.

γεια πρόσβασης ⟨SecurityPersonnel, EvaluateIncident, IncidentSummary⟩ για το σκοπό PerimeterNetworkSecurity. Με βάση το γράφο των ρόλων του Σχήματος 14β′, οδηγούμαστε στις ενέργειες-φύλλα ⟨CSIRT, EvaluateIncident, IncidentSummary⟩ και ⟨SecurityAdmin, EvaluateIncident, IncidentSummary⟩. Η πρώτη είναι συσχετισμένη με την επιτρεπόμενη ενέργεια PermittedAct#3 (Σχήμα 14γ′), η οποία οδηγεί στην αντίστοιχη αυτόνομη εργασία του Σχήματος 14ε′. Παρατηρούμε ότι εκτός από την αντικατάσταση του ρόλου της αρχικής εργασίας από έναν πιο εξειδικευμένο, προστίθεται ο περιορισμός για το επίπεδο σοβαρότητας του περιστατικού, πληροφορία η οποία περιέχεται στην περιγραφή του τελευταίου (όπως φαίνεται από το γράφο των δεδομένων του Σχήματος 14β′, SeverityLevel $\xrightarrow{\texttt{isPartOf}}$ IncidentSummary). Η δεύτερη ενέργεια-φύλλο δεν είναι συσχετισμένη με κάποια επιτρεπόμενη ενέργεια· σε αυτήν την περίπτωση, όπως περιγράφηκε παραπάνω, αναζητούνται επιτρεπόμενες ενέργειες που αφορούν λιγότερο λεπτομερείς τύπους δεδομένων, ή τύπους δεδομένων που περιέχονται σε εκείνον που αποτελεί τον πόρο της ενέργειας-φύλλου. Έτσι, σύμφωνα με την επιτρεπόμενη ενέργεια PermittedAct#4, οι χρήστες με ρόλο SecurityAdmin επιτρέπεται να αξιολογήσουν ένα περιστατικό βάσει μόνο της γενικής περιγραφής του περιστατικού IncidentGeneralDescription, για την οποία ισχύει IncidentGeneralDescription $\xrightarrow{\texttt{isPartOf}}$ IncidentSummary, όταν το περιστατικό είναι μέτριας σοβαρότητας (έκφραση Expr#2 ⟨SeverityLevel, equals, Medium⟩). Με τον τρόπο αυτό εξάγεται και η δεύτερη αυτόνομα έγκυρη εργασία του Σχήματος 14ε′. Ουσιαστικά, οι δύο αυτές αυτόνομα έγκυρες εργασίες αντανακλούν διαφοροποιήσεις στην εκτέλεση της λειτουργίας EvaluateIncident ανάλογα με το ρόλο του δράστη και τη σοβαρότητα του περιστατικού, με παράλληλη διαφοροποίηση του εκάστοτε πόρου.

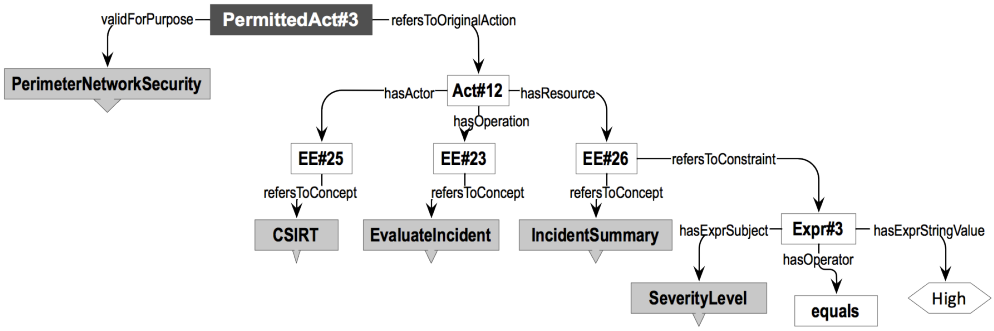
Τέλος, θα πρέπει να σημειωθεί ότι ο Αλγόριθμος 9 παρουσιάζει τον τρόπο διαχείρισης εργασιών στις οποίες τα προφίλ εκτέλεσης είναι πλήρως προσδιορισμένα (*epIsComplete*), δηλαδή, πέρα από τη λειτουργία πάνω στην οποία θεμελιώνεται η εργασία, έχει οριστεί τουλάχιστον ένας δράστης και τουλάχιστον ένας πόρος. Στην περίπτωση που κάποιο/α στοιχείο/α του προφίλ δεν έχουν οριστεί, η μεθοδολογία που ακολουθείται είναι η ίδια, με μόνη διαφορά να αποτελεί το γεγονός ότι η αναζήτηση των επιτρεπόμενων ενεργειών γίνεται με βάση τα προσδιορισμένα στοιχεία, ενώ εκείνα που παραλείπονται υπαγορεύονται τελικά από τις ίδιες τις ενέργειες. Το Σχήμα 15 απεικονίζει την εξαγωγή των αυτόνομα έγκυρων εργασιών για την εργασία-προορισμό του υπό εξέταση διμερούς συσχετισμού του Σχήματος 13, για την οποία, εκτός από τη λειτουργία, έχει προσδιοριστεί μόνο ο πόρος. Μετά την ανάλυση της λειτουργίας MitigateIncident στις πιο εξειδικευμένες από αυτήν Sinkhole και Redirect (Σχήμα 15β′), που αντανακλούν εναλλακτικούς τρόπους υλοποίησης της αρχικής λειτουργίας, αναζητούνται επιτρεπόμενες ενέργειες που αναφέρονται σε ενέργειες πρόσβασης με λειτουργία Sinkhole ή Redirect και πόρο Traffic. Έτσι σύμφωνα με την ενέργεια πρόσβασης της επιτρεπόμενης ενέργειας PermittedAct#1 για τη λειτουργία Sinkhole (αντίστοιχα για τη λειτουργία Redirect) εξάγεται η πρώτη αυτόνομα έγκυρη εργασία του Σχήματος 15δ′, όπου έχει προσδιοριστεί πλέον στο προφίλ εκτέλεσης και ο δράστης (ο περιέκτης λειτουργιών MitigationSystem).



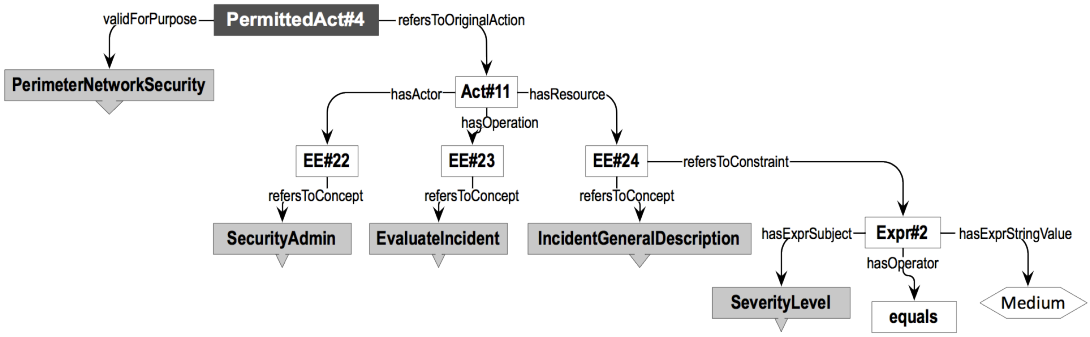

(α′) Αρχική προδιαγραφή εργασίας




(β′) Υπογράφοι της IMO



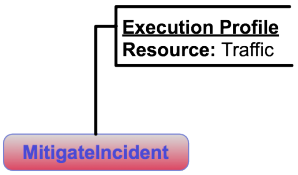

(γ′) Επιτρεπόμενη ενέργεια για δράστη με ρόλο `CSIRT`



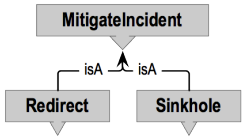

(δ′) Επιτρεπόμενη ενέργεια για δράστη με ρόλο `SecurityAdmin`


(ε′) Αυτόνομα Έγκυρες Εργασίες

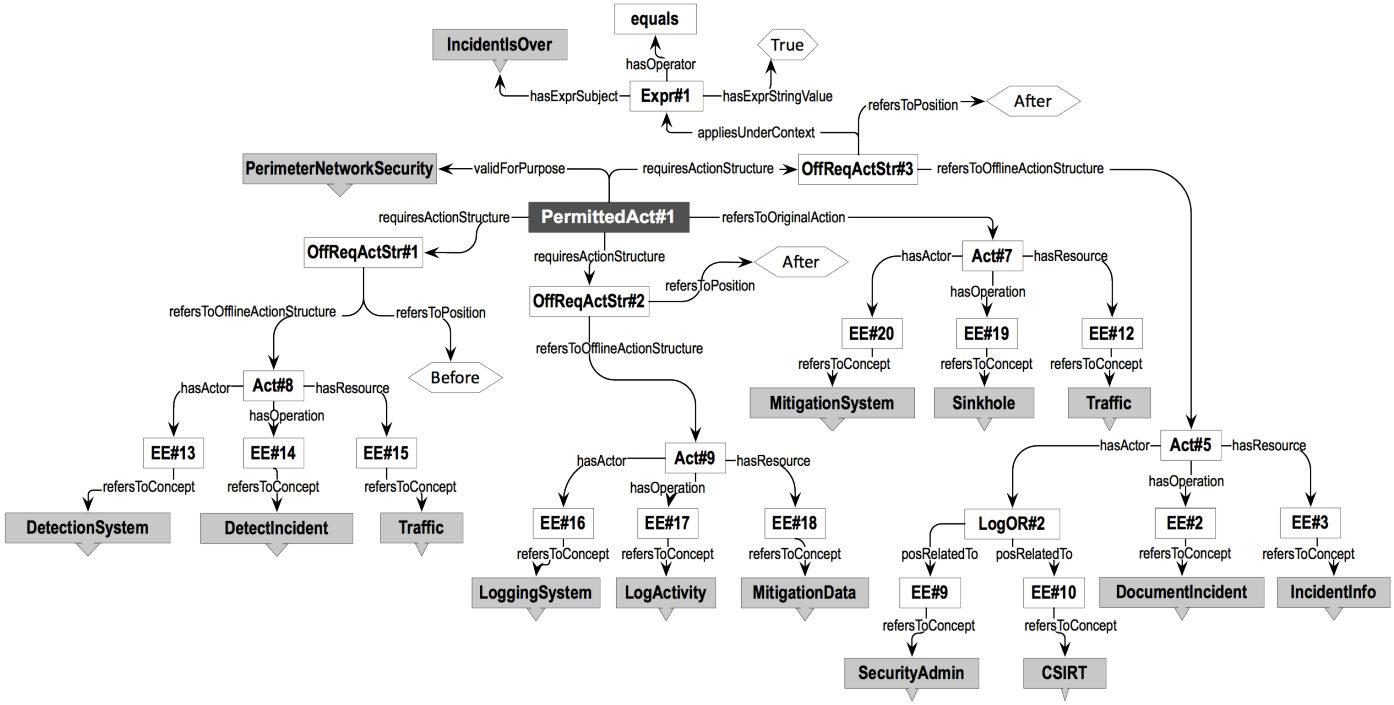
Σχήμα 14: Παράδειγμα Εξαγωγής Αυτόνομα Έγκυρων Εργασιών



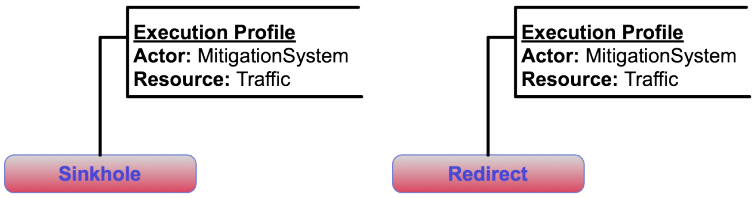

(α′) Αρχική προδιαγραφή εργασίας




(β′) Υπογράφος λειτουργιών της IMO




(γ′) Επιτρεπόμενη ενέργεια για τη λειτουργία `Sinkhole`



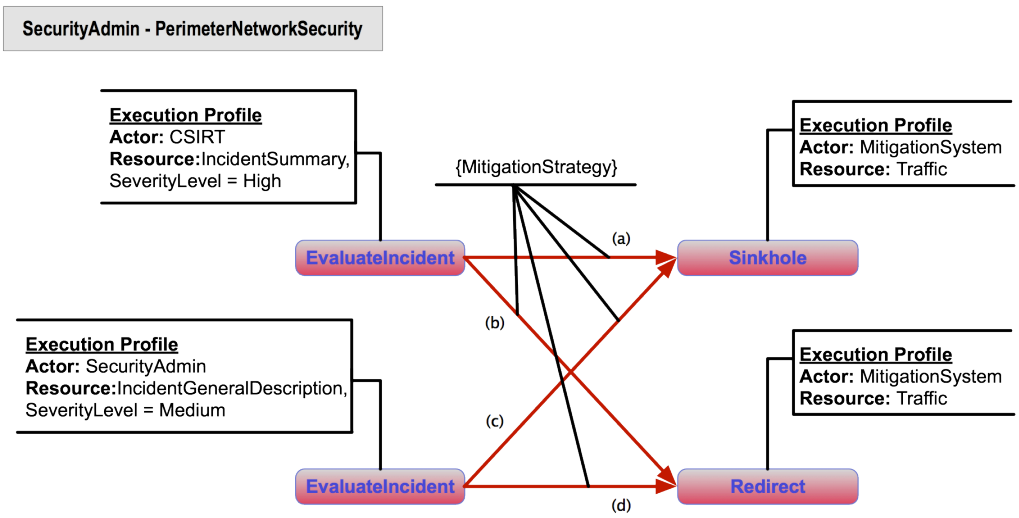

(δ′) Αυτόνομα Έγκυρες Εργασίες

Σχήμα 15: Παράδειγμα εξαγωγής αυτόνομα έγκυρων εργασιών από μη πλήρως προσδιορισμένη εργασία

## 7.5 Επαλήθευση του Διμερούς Μετασυσχετισμού

Μετά την εξαγωγή των αυτόνομα έγκυρων εργασιών για κάθε αρχική εργασία του υπό εξέταση διμερούς συσχετισμού, και όπως φαίνεται στον Αλγόριθμο 7, σχηματίζονται οι *διμερείς μετασυσχετισμοί* (σύνολο $BA'$) με βάση την αντιστοίχιση των αυτόνομα έγκυρων προς τις αρχικές εργασίες του εκάστοτε αρχικού διμερούς συσχετισμού. Σημειώνεται ότι σε αυτήν τη φάση οι διμερείς μετασυσχετισμοί είναι ημιτελείς, καθώς δεν έχει προδιαγραφεί ακόμα η μεταξύ τους αλληλεπίδραση, η οποία θα προκύψει τελικά με τον τρόπο

που περιγράφεται στην Ενότητα 7.5.2. Καθώς από κάθε αρχική εργασία είναι δυνατόν να προκύψει τελικά ένα σύνολο αυτόνομα έγκυρων εργασιών, όπως περιγράφηκε στην Ενότητα 7.4, κάθε αρχικός διμερής συσχετισμός ενδέχεται να οδηγήσει σε ένα αντίστοιχο σύνολο διμερών μετασυσχετισμών, των οποίων οι εργασίες είναι πλέον αυτόνομα έγκυρες. Για παράδειγμα, όπως φαίνεται στο Σχήμα 16, ο αρχικός συσχετισμός του Σχήματος 13 οδηγεί στο σχηματισμό τεσσάρων μετασυσχετισμών με βάση την αρχική ροή και τις αυτόνομα έγκυρες εργασίες που προέκυψαν στο προηγούμενο στάδιο της διαδικασίας για το ζεύγος ⟨`PerimeterNetworkSecurity`, `SecurityAdmin`⟩. Έτσι, για να χαρακτηριστεί ένας αρχικός διμερής συσχετισμός έγκυρος, θα πρέπει τουλάχιστον ένας από τους εξαγμένους μετασυσχετισμούς να αποδειχθεί έγκυρος.




Σχήμα 16: Διμερείς μετασυσχετισμοί που προέκυψαν για τον υπό εξέταση διμερή συσχετισμό

Για να χαρακτηριστεί ένας διμερής μετασυσχετισμός ως έγκυρος θα πρέπει αρχικά να διασφαλιστεί ότι δεν υπάρχουν *απόλυτες συγκρούσεις* μεταξύ των δύο εργασιών, υπό την έννοια ότι η εκτέλεση της μίας δεν αποκλείει την εκτέλεση της άλλης ανεξάρτητα από άλλους παράγοντες, όπως η παρουσία ή απουσία τρίτων εργασιών. Επιπλέον, προϋπόθεση για την εγκυρότητα του διμερούς συσχετισμού αποτελεί η εγκυρότητα της ροής ελέγχου ή δεδομένων η οποία περιγράφει την αλληλεπίδραση των εν λόγω εργασιών, δηλαδή η κατευθυνόμενη ακμή που συνδέει την εργασία-αφετηρία με την εργασία-προορισμό. Η εκπλήρωση των δύο αυτών προϋποθέσεων έχει σαν αποτέλεσμα την εξαγωγή των οδηγιών εξουσιοδότησης που θα πρέπει να εφαρμοστούν ώστε να είναι τελικά έγκυρος ο διμερής συσχετισμός. Εκτός από τις οδηγίες που αφορούν την αλληλεπίδραση καθεαυτή, από τη στιγμή που η τελευταία θα κριθεί έγκυρη, γίνεται ο έλεγχος για άλλες εργασίες που είτε είναι απαραίτητες για, είτε έρχονται σε σύγκρουση με την εκτέλεση καθεμίας από τις εργασίες του συσχετισμού˙ ο έλεγχος αυτός οδηγεί στην εξαγωγή επιπρόσθετων οδηγιών που υπαγορεύουν την παρουσία ή την απουσία τρίτων εργασιών αναφορικά με κάποια από τις εργασίες του συσχετισμού και αντίστοιχα συμπληρωματική ή απαγορευμένη ροή

δεδομένων προς τις εργασίες. Σημειώνεται ότι η μη δημιουργία οδηγιών εξουσιοδότησης για ένα διμερή συσχετισμό συνεπάγεται ότι δεν είναι τελικά δυνατόν αυτός να εκτελεστεί σε οποιαδήποτε μορφή του.

Με βάση τα παραπάνω, η διαδικασία επαλήθευσης ενός διμερούς μετασυσχετισμού περιγράφεται από τον Αλγόριθμο 10 και αναλύεται στα ακόλουθα βήματα:

- Έλεγχος για τον εντοπισμό τυχόν απόλυτων συγκρούσεων μεταξύ της εργασίας-αφετηρίας *src* και της εργασίας-προορισμού *dst* του μετασυσχετισμού *ba′* (γραμμή 4)
- Επαλήθευση της αλληλεπίδρασης των εργασιών του μετασυσχετισμού, με βάση τον αρχικό διμερή συσχετισμό *ba* (γραμμή 6)
- Προσδιορισμός των εργασιών που πρέπει ή απαγορεύεται να έπονται, να προηγούνται ή να εκτελούνται παράλληλα με τις εργασίες του μετασυσχετισμού, καθώς και επιπλέον πληροφορίας που οι τελευταίες πρέπει ή απαγορεύεται να λαμβάνουν ως είσοδο (γραμμές 8—10)

**Αλγόριθμος 10** VerifyMetaAssociation

**Input:** *ba′, ba, pip*
**Output:** *DIR*
1: $DIR \leftarrow \emptyset$
2: $src \leftarrow ba'$.src
3: $dst \leftarrow ba'$.dst
4: $definiteConflictExists \leftarrow$ CheckForDefiniteConflicts(*src*, *dst*, *pip*)
5: **if** !$definiteConflictExists$ **then**
6: $DIR \leftarrow$ VerifyBilateralEdge(*src*, *dst*, *ba*, *pip*)
7: $DIR' \leftarrow \emptyset$
8: **for each** $dir$ **in** $DIR$ **do**
9: $DIR'$.add(CreateOtherDirs(*src*, *dst*, *pip*))
10: **end for**
11: $DIR$.add($DIR'$)
12: **end if**
13: **return** *DIR*

Οι ενότητες που ακολουθούν περιγράφουν εκτενέστερα καθένα από τα προαναφερθέντα βήματα.

### 7.5.1 Εντοπισμός Απόλυτων Συγκρούσεων

Ο σκοπός εκτέλεσης αυτού του βήματος έγκειται στον έγκαιρο εντοπισμό συγκρούσεων μεταξύ των δύο εργασιών αναφοράς του εκάστοτε διμερούς μετασυσχετισμού, ούτως ώστε σε περίπτωση εντοπισμού να μην πραγματοποιηθούν τα επόμενα βήματα της διαδικασίας, τα οποία είναι απαιτητικά σε πόρους.

Καθώς ο έλεγχος πραγματοποιείται σε επίπεδο ενεργειών, αρχικά η εργασία-αφετηρία και η εργασία-προορισμός αποσυντίθενται με τη λογική που περιγράφηκε στην Ενότητα 7.4, ώστε η κάθε εργασία να μπορεί να αντιστοιχηθεί τελικά σε μία ή περισσότερες ενέργειες, δηλαδή καθεμία από τις ενέργειες να αναφέρεται μόνο σε έναν πόρο του προφίλ εκτέλεσης της αντίστοιχης εργασίας και σε ένα μοναδικό δράστη ή δράστες λογικά συνδεδεμένους μεταξύ τους με σχέση AND. Έτσι, προκύπτουν τα σύνολα $ACT_{src}$ και $ACT_{dst}$ που απαρτίζονται από τις ενέργειες που προκύπτουν από την εργασία-αφετηρία και την εργασία-προορισμό, αντίστοιχα.

Ουσιαστικά, για κάθε συνδυασμό $act_{src} \in ACT_{src}$ και $act_{dst} \in ACT_{dst}$ θα πρέπει να διερευνηθούν τα εξής:

(i) Αν οι εν λόγω ενέργειες συνυπάρχουν σε απαγορεύσεις, όπου η $act_{dst}$ αντιστοιχεί στην ενέργεια πρόσβασης και η $act_{src}$ αποτελεί τη μοναδική θετική προ-ενέργεια.

(ii) Αν οι εν λόγω ενέργειες συνυπάρχουν σε άδειες, όπου η $act_{src}$ αποτελεί τη μοναδική αρνητική προ-ενέργεια και η $act_{dst}$ αντιστοιχεί στην ενέργεια πρόσβασης.

(iii) Αν οι εν λόγω ενέργειες συνυπάρχουν σε άδειες, όπου η $act_{src}$ αντιστοιχεί στην ενέργεια πρόσβασης και η $act_{dst}$ αποτελεί τη μοναδική αρνητική μετα-ενέργεια.

Οι απαντήσεις στα παραπάνω ερωτήματα δίδονται μέσω των επιτρεπόμενων ενεργειών (βλ. Ενότητα 6.2.1). Η ενέργεια πρόσβασης αντιστοιχεί στην ενέργεια στην οποία αναφέρεται η επιτρεπόμενη ενέργεια, ενώ οι αρνητικές προ- και μετα- ενέργειες αντανακλώνται από τις απαιτούμενες διενέργειες οι οποίες συνδέονται με την εν λόγω επιτρεπόμενη ενέργεια μέσω της ιδιότητας `forbidsActionStructure` της οντολογίας PMO και με την ιδιότητα τύπου δεδομένων `refersToPosition` να υποδεικνύει κατάλληλα αν το εκάστοτε στιγμιότυπο αποτελεί προ- ή μετα- ενέργεια. Έτσι, για παράδειγμα, λόγω των επιτρεπόμενων ενεργειών των Σχημάτων 14γ′ και 15γ′, δεν εντοπίζονται συγκρούσεις μεταξύ των εργασιών του μετασυσχετισμού (a) του Σχήματος 16.

Στη γενική περίπτωση, όπου οι δεδομένες εργασίες δεν αντιστοιχίζονται η καθεμία σε μία ακριβώς ενέργεια, οι παραπάνω έλεγχοι επεκτείνονται ώστε η εκάστοτε ενέργεια πρόσβασης να ελέγχεται για απόλυτες συγκρούσεις με κάθε μέλος (εκτός του κενού συνόλου) του δυναμοσυνόλου του αντίστοιχου συνόλου ενεργειών που αντιστοιχούν στις προ-/μετα- ενέργειες, λαμβάνοντας παράλληλα υπόψη τις λογικές σχέσεις που περιλαμβάνονται στα προφίλ εκτέλεσης των υπό εξέταση εργασιών. Σημειώνεται ότι στην περίπτωση που η δομή των προ-/μετα- ενεργειών περιέχει και άλλες λογικά συσχετισμένες ενέργειες εκτός από εκείνες που περιλαμβάνονται στο σύνολο $ACT_{src}$ ή στο σύνολο $ACT_{dst}$, οποιαδήποτε σύγκρουση εντοπιστεί δε χαρακτηρίζεται ως απόλυτη, καθώς οι τρίτες λογικά συσχετισμένες ενέργειες ενδέχεται να καταργούν τελικά τη σύγκρουση αυτή με την παρουσία ή απουσία τους πριν, μετά ή παράλληλα με τον υπό εξέταση διμερή συσχετισμό (βλ. Ενότητα 7.5.3).

### 7.5.2 Επαλήθευση της Αλληλεπίδρασης των Εργασιών

Στο στάδιο αυτό, ο εκάστοτε διμερής μετασυσχετισμός, ο οποίος έχει προκύψει από τον υπό εξέταση διμερή συσχετισμό, έχει ελεγχθεί ως προς την αυτόνομη εγκυρότητα των εργασιών που περιλαμβάνει και, επιπλέον, έχει απαλειφθεί η πιθανότητα απόλυτων συγκρούσεων μεταξύ τους. Ωστόσο, υπάρχει το ενδεχόμενο να παρατηρηθούν ασυμβατότητες στο επίπεδο της αλληλεπίδρασης μεταξύ τους, δηλαδή στην κατευθυνόμενη ακμή του αρχικού διμερούς συσχετισμού που αντανακλά την ανταλλαγή πληροφορίας, είτε αυτή αναφέρεται σε ροή δεδομένων είτε σε παραμέτρους ελέγχου, μεταξύ των δύο εργασιών.

Υπό το πρίσμα των παραπάνω, το βήμα αυτό αφορά στον έλεγχο της εγκυρότητας της αλληλεπίδρασης των εργασιών του διμερούς μετασυσχετισμού, όπως αυτή προδιαγράφηκε στον αρχικό συσχετισμό, και περιλαμβάνει τον έλεγχο των δεδομένων που ανταλλάσσονται, καθώς και του ίδιου του τύπου της ροής αυτής, δηλαδή εάν πρόκειται για συνεχή ροή δεδομένων ή για ροή ελέγχου. Σε περίπτωση εντοπισμού ασυμβατοτήτων μεταξύ των δύο εργασιών στο επίπεδο της μεταξύ τους αλληλεπίδρασης, αυτές επιλύονται —εάν είναι δυνατόν— με την υπόδειξη ή/και απευθείας προσθήκη εμβόλιμων εργασιών από τη Μηχανή Συμπερασμού. Η επιτυχής επαλήθευση της αλληλεπίδρασης οδηγεί στην εξαγωγή οδηγιών εγκυρότητας (βλ. Ενότητα 7.1) για τον υπό εξέταση διμερή μετασυσχετισμό *ba'*, ο οποίος είναι πλέον πλήρης, δηλαδή έχει συσχετιστεί με μία ή περισσότερες έγκυρες ακμές αλληλεπίδρασης, με αναφορά στον αρχικό διμερή συσχετισμό *ba*.

#### Σύγκριση Δεδομένων Ροής και Δεδομένων Εισόδου/Εξόδου των Λειτουργιών

Υπενθυμίζεται ότι η ακμή ενός διμερούς συσχετισμού που υποδηλώνει την αλληλεπίδραση μεταξύ των εμπλεκόμενων εργασιών, εκτός από την εργασία-αφετηρία και την εργασία-προορισμό, χαρακτηρίζεται επίσης από ένα σύνολο οντοτήτων πληροφορίας *InformationEntities* (*IE*) και ένα σύνολο συνθηκών *FlowConditions* (*FC*) που πρέπει να ισχύουν προκειμένου να πραγματοποιηθεί η υποδηλούμενη μετάβαση μεταξύ των δύο εργασιών, υποστηρίζοντας έτσι, όταν είναι αναγκαίο, την υπό συνθήκη διακλάδωση της ροής ελέγχου ή δεδομένων (βλ. Ενότητα 3.2.2). Στην παρούσα φάση, ο έλεγχος στρέφεται γύρω από τις οντότητες πληροφορίας που είναι συσχετισμένες με την υπό εξέταση ακμή, καθώς αρχικά θα πρέπει να ελεγχθεί ότι τα δεδομένα που ανταλλάσσονται μεταξύ των δύο εργασιών είναι σύμφωνα τόσο με τα δεδομένα που είναι σε θέση να εξάγει η λειτουργία της εργασίας-αφετηρίας $op_{src}$, όσο και με τα δεδομένα που είναι δυνατόν να λάβει ως είσοδο η λειτουργία της εργασίας-προορισμού $op_{dst}$. Για το σκοπό αυτόν, με χρήση των αντικειμενικών ιδιοτήτων `hasOutput` και `hasInput` του Σημασιολογικού Μοντέλου Πληροφοριών, συγκεντρώνονται όλες οι δυνητικές έξοδοι και είσοδοι (στιγμιότυπα της κλάσης `DataIO`, βλ. Ενότητα 5.1) των λειτουργιών $op_{src}$ και $op_{dst}$, αντίστοιχα, και από αυτές —μέσω των ιδιοτήτων `refersToDataType` και `isA`, ώστε να προκύψουν τελικά τα κατάλληλα φύλλα του γράφου των τύπων δεδομένων— εξάγονται τα σύνολα $OutputDataTypes_{src}$ ($ODT_{src}$) και

$InputDataTypes_{dst}$ ($IDT_{dst}$), τα οποία περιλαμβάνουν τους σχετικούς τύπους δεδομένων.

Ακολουθώντας τη λογική της ανάλυσης των εργασιών του διμερούς συσχετισμού, η υπό εξέταση ακμή αναλύεται σε ένα σύνολο ισοδύναμων προς αυτήν και, επομένως, εναλλακτικών μεταξύ τους ακμών. Έτσι, για κάθε οντότητα πληροφορίας $ie_i$ που φέρει η ακμή, από τον τύπο δεδομένων $dt_i$ που τη χαρακτηρίζει εξάγεται το σύνολο των πιο εξειδικευμένων τύπων, δηλαδή των φύλλων του υπογράφου του γράφου $DT$ που έχει σαν ρίζα τον $dt_i$. Κάθε υποσύνολο του καρτεσιανού γινομένου των συνόλων που προέκυψαν αντανακλά τα δεδομένα που θα φέρει η καθεμία από τις εναλλακτικές ακμές που τελικά θα ελεγχθούν.

Στη συνέχεια, για κάθε εναλλακτική ακμή και για κάθε τύπο δεδομένων *dt* που αυτή φέρει, ελέγχεται αν ο τελευταίος αποτελεί ταυτόχρονα μέλος και των δύο συνόλων $ODT_{src}$ και $IDT_{dst}$. Εδώ παρατηρούνται διάφορες πιθανές περιπτώσεις:

(i) Ο τύπος δεδομένων *dt* πράγματι περιλαμβάνεται και στα δύο σύνολα.

(ii) Ο τύπος δεδομένων *dt* περιλαμβάνεται μόνο στο σύνολο $ODT_{src}$ και το σύνολο $IDT_{dst}$ περιλαμβάνει έναν ή περισσότερους τύπους δεδομένων που αποτελούν συνιστώσες του εν λόγω τύπου, δηλαδή, συνδέονται με αυτόν μέσω της σχέσης *isPartOf*.

(iii) Ο τύπος δεδομένων *dt* περιλαμβάνεται μόνο στο σύνολο $IDT_{dst}$και το σύνολο $ODT_{src}$ περιλαμβάνει έναν ή περισσότερους τύπους δεδομένων που αποτελούν συνιστώσες του εν λόγω τύπου, δηλαδή, συνδέονται με αυτόν μέσω της σχέσης *isPartOf*.

(iv) Ο τύπος δεδομένων *dt* περιλαμβάνεται σε ένα από τα δύο σύνολα, χωρίς να υπάρχει κάποια προφανής σχέση με οποιοδήποτε από τα μέλη του δεύτερου συνόλου.

(v) Ο τύπος δεδομένων *dt* δεν περιλαμβάνεται σε κανένα από τα δύο σύνολα.

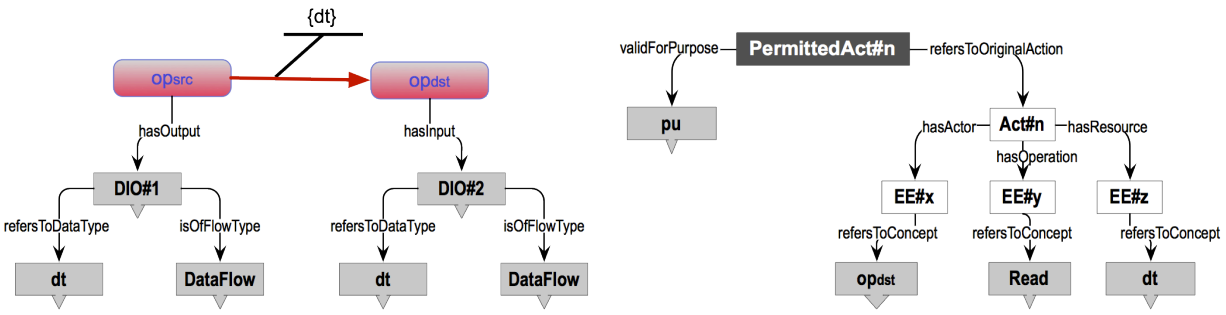
Η πρώτη περίπτωση είναι και η πιο απλή σε ό,τι αφορά το χειρισμό της, καθώς ο παρών έλεγχος τερματίζεται σε αυτό το σημείο και η διαδικασία προχωρά στο επόμενο βήμα. Η δεύτερη περίπτωση υποδεικνύει ότι ενδέχεται μεταξύ των δύο εργασιών να παρεμβληθεί μία νέα εργασία που θα υλοποιεί την πράξη της προβολής της σχεσιακής άλγεβρας, ενώ η τρίτη περίπτωση ενδέχεται να εκφράζει την αντίστροφη κατάσταση, όπου η εμβόλιμη εργασία θα πραγματοποιεί ανασύνθεση ενός τύπου δεδομένων από συνιστώσες του. Ωστόσο, για να αποφανθεί η Μηχανή Συμπερασμού σχετικά με την προσθήκη εμβόλιμων *εργασιών μετασχηματισμού*, θα πρέπει πρώτα να πραγματοποιηθεί και το επόμενο βήμα της διαδικασίας, το οποίο αφορά τα δικαιώματα ανάγνωσης της λειτουργίας $op_{dst}$. Για την τέταρτη περίπτωση, θα πρέπει ουσιαστικά να βρεθεί ένα *μονοπάτι* λειτουργιών, οι οποίες μέσω των εισόδων και εξόδων τους "γεφυρώνουν" τελικά τις δύο λειτουργίες. Εντούτοις, η περίπτωση αυτή αφενός δεν έχει κάποιο ενδιαφέρον όσον αφορά την ασφάλεια και την ιδιωτικότητα και αφετέρου θα μπορούσε να είναι αποτέλεσμα λανθασμένης προδιαγραφής του διμερούς συσχετισμού˙ για το λόγο αυτόν, κρίθηκε ότι ξεφεύγει από τους στόχους της διατριβής και δε λαμβάνεται υπόψη. Η τελευταία περίπτωση σημαίνει ότι ο τύπος *dt* θα

πρέπει να απορριφθεί για την υπό εξέταση ακμή. Εάν αυτό ισχύει για όλους τους τύπους δεδομένων των οντοτήτων πληροφορίας της εν λόγω ακμής, ή εάν εξαρχής δεν έχει προσδιοριστεί η μεταδιδόμενη πληροφορία, τότε μέσω της σύγκρισης των συνόλων $ODT_{src}$ και $IDT_{dst}$, η Μηχανή Συμπερασμού συμπληρώνει τις εναλλακτικές ακμές, με τους κοινούς τύπους ή/και εκείνους που συνδέονται με σχέση συμπερίληψης, εάν υπάρχουν, να οδηγούν σε κάποια από τις τρεις πρώτες περιπτώσεις.

### Έλεγχος Δικαιωμάτων Ανάγνωσης

Μετά τη σύγκριση των μεταδιδόμενων δεδομένων και των δεδομένων που είναι δυνατόν να εξάγουν και να λάβουν ως είσοδο οι λειτουργίες $op_{src}$ και $op_{dst}$, αντίστοιχα, ακολουθεί ο έλεγχος για τα δικαιώματα ανάγνωσης που έχει η λειτουργία $op_{dst}$ όσον αφορά τα δεδομένα που φτάνουν τελικά στην είσοδο της εργασίας $t_{dst}$. Υπενθυμίζεται ότι το σύνολο $IDT_{dst}$ περιέχει τους τύπους δεδομένων που είναι δυνατόν να λάβει η λειτουργία $op_{dst}$ σύμφωνα με τις προδιαγραφές της, χωρίς αυτό να συνεπάγεται την ύπαρξη των αντίστοιχων δικαιωμάτων ανάγνωσης για οποιοδήποτε ζεύγος σκοπού-εκκινητή ή οποιεσδήποτε συνθήκες πλαισίου.

Τα σχετικά δικαιώματα ανάγνωσης αναζητούνται μέσω των επιτρεπόμενων ενεργειών εκείνων, όπου ο σκοπός ταυτίζεται με εκείνον του τρέχοντος ζεύγους σκοπού-εκκινητή, ο δράστης αναφέρεται στη λειτουργία $op_{dst}$, η λειτουργία της ενέργειας είναι το στιγμιότυπο `Read` και ο πόρος αναφέρεται είτε στο μεταδιδόμενο τύπο δεδομένων *dt* ή σε κάποια από τις συνιστώσες του, ανάλογα με το σε ποια περίπτωση από τις (i), (ii) και (iii)[20] οδήγησε ο προηγούμενος έλεγχος. Σημειώνεται ότι ενδέχεται να βρεθούν περισσότερα του ενός δικαιώματα ανάγνωσης, καθώς αυτά μπορεί να ισχύουν κάτω από διαφορετικές συνθήκες πλαισίου ή/και διαφορετικές απαραίτητες ή απαγορευμένες προ-/μετα- ενέργειες, λαμβάνοντας παράλληλα υπόψη της το σύνολο συνθηκών *FC* που είχαν οριστεί για την αρχική ακμή, με το κάθε δικαίωμα ανάγνωσης να αντανακλά στη γενική περίπτωση μία διαφορετική εναλλακτική ακμή για τον υποκείμενο διμερή μετασυσχετισμό.




(α′) Ελεγχος συμφωνίας τύπων δεδομένων (β′) Έλεγχος δικαιωμάτων ανάγνωσης

Σχήμα 17: Επαλήθευση Αλληλεπίδρασης χωρίς Μετασχηματισμό

[20]Η περίπτωση (v) αποτελεί υπερπερίπτωση των (i), (ii) και (iii) και δεν εξετάζεται ξεχωριστά.

Το Σχήμα 17 παρουσιάζει την πιο απλή περίπτωση επαλήθευσης της αλληλεπίδρασης ενός διμερούς συσχετισμού, η οποία συνιστά ροή δεδομένων. Σημειώνεται ότι στην περίπτωση αυτή εμπίπτουν και οι μετασυσχετισμοί του Σχήματος 16. Ο τύπος δεδομένων *dt* στον οποίο αναφέρεται η οντότητα πληροφορίας περιλαμβάνεται τόσο στο $ODT_{src}$ όσο και στο $IDT_{dst}$ (Σχήμα 17α′), ενώ μετά από αναζήτηση για τα σχετικά δικαιώματα ανάγνωσης που έχει η λειτουργία $op_{dst}$ πάνω στα δεδομένα εισόδου, η εύρεση της επιτρεπόμενης ενέργειας `PermittedAct#n` (Σχήμα 17β′), η οποία επιτρέπει την ανάγνωση του τύπου *dt* χωρίς κάποιον περιορισμό, επιβεβαιώνει την εγκυρότητα της αλληλεπίδρασης σε συνδυασμό με τον τύπο ροής `DataFlow` που χαρακτηρίζει την είσοδο και την έξοδο των λειτουργιών. Η διαδικασία επαλήθευσης της ακμής ολοκληρώνεται με τη δημιουργία της αντίστοιχης οδηγίας εγκυρότητας διμερούς συσχετισμού.

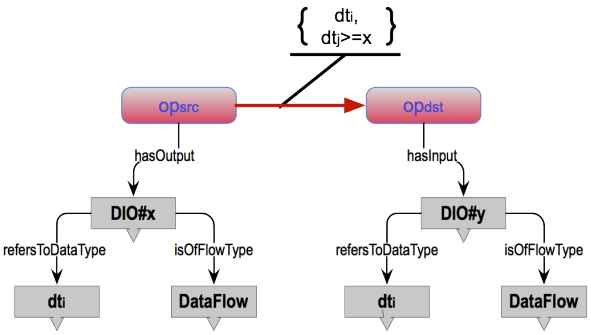
Η παραπάνω περίπτωση χαρακτηρίστηκε ως η πιο απλή, διότι δεν υπαγορεύει κάποια μετατροπή στη ροή με την προσθήκη κάποιας εμβόλιμης εργασίας μετασχηματισμού των μεταδιδόμενων δεδομένων. Προσθήκες τέτοιου τύπου υπαγορεύονται είτε απευθείας από την προδιαγραφή της ροής, μέσω περιορισμών που ορίζονται πάνω σε ιδιότητες των μεταδιδόμενων δεδομένων ή/και περιορισμούς που αφορούν την κατάστασή τους, είτε από το Σημασιολογικό Μοντέλο Πρόσβασης και Χρήσης, λόγω περιορισμών που επιβάλλουν οι κανόνες ή για τη γεφύρωση διαφορών μεταξύ συγγενικών τύπων δεδομένων. Στη συνέχεια παρουσιάζονται τα πιο βασικά πρότυπα μετασχηματισμού μίας ροής, τα οποία ενσωματώνουν στη ροή επιπλέον μηχανισμούς για προστασία της ασφάλειας και της ιδιωτικότητας.

### Προσθήκη Εργασιών Μετασχηματισμού Ροής

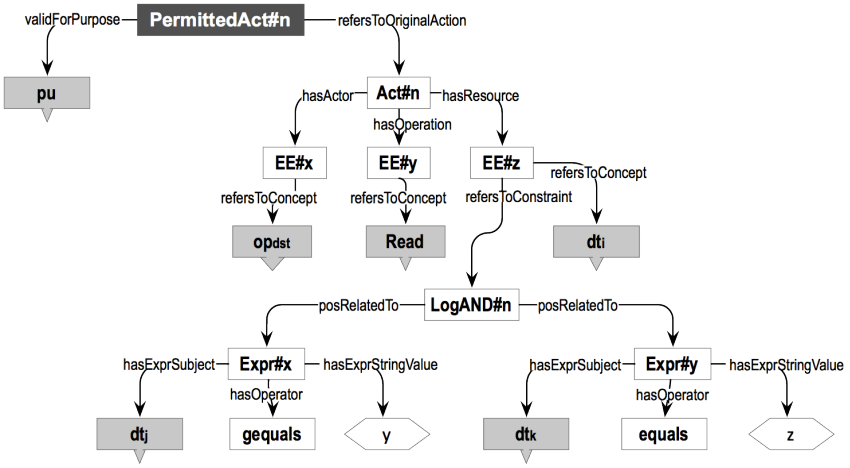
Διακρίνουμε τέσσερα βασικά πρότυπα μετασχηματισμών ροής, τα οποία οδηγούν στην προσθήκη των ακόλουθων εμβόλιμων εργασιών:

**Εργασία επιλογής** Η εμβόλιμη εργασία σε αυτήν την περίπτωση υλοποιεί την πράξη της *επιλογής* (*selection*) της σχεσιακής άλγεβρας και η προσθήκη της υπαγορεύεται από περιορισμούς πάνω στα δεδομένα, που υπονοούν ότι στην είσοδο της λειτουργίας $op_{dst}$ θα φτάσουν μόνο τα δεδομένα εκείνα που ικανοποιούν τους εν λόγω *περιορισμούς φιλτραρίσματος* πάνω στις ιδιότητές τους ή σε άλλους τύπους δεδομένων που αποτελούν συνιστώσες τους. Οι περιορισμοί αυτοί είναι δυνατόν να ορίζονται απευθείας στο επίπεδο του διμερούς συσχετισμού, δηλαδή ως περιορισμοί στην εκάστοτε οντότητα πληροφορίας, ή/και να υπαγορεύονται από κανόνες.

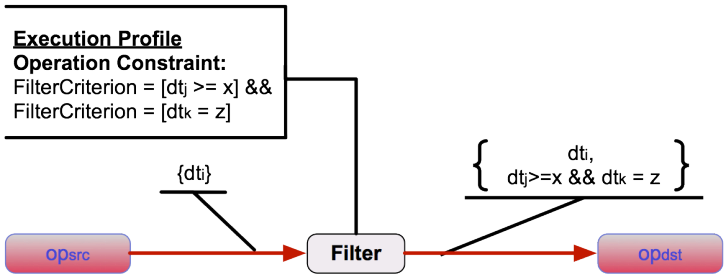
Έτσι, όπως φαίνεται στο Σχήμα 18α′, ένας τέτοιος περιορισμός έχει οριστεί ήδη στο επίπεδο του υπό εξέταση διμερούς συσχετισμού, με τα δεδομένα τύπου $dt_i$ που μεταφέρονται πάνω από την ακμή του να πρέπει να ικανοποιούν τη συνθήκη $dt_j \geq x$, όπου ο τύπος δεδομένων $dt_j$ αποτελεί συνιστώσα του $dt_i$, δηλαδή $dt_j \xrightarrow{\texttt{isPartOf}} dt_i$, και $x$ η επιθυμητή ελάχιστη τιμή του συγκεκριμένου πεδίου των δεδομένων. Από τη σύγκριση των δεδομένων




(α′) Ελεγχος συμφωνίας τύπων δεδομένων




(β′) Έλεγχος δικαιωμάτων ανάγνωσης



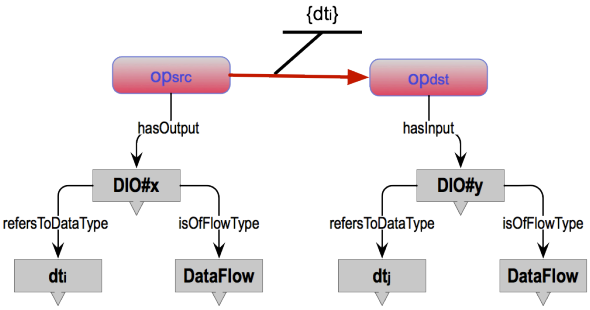

(γ′) Προσθήκη εργασίας επιλογής

Σχήμα 18: Περίπτωση Επιλογής Μεταδιδόμενων Δεδομένων. Οι τύποι $dt_j$ και $dt_k$ αποτελούν πεδία του τύπου $dt_i$, ενώ κατά τη συγχώνευση των περιορισμών της ροής και των περιορισμών των κανόνων θεωρήθηκε ότι $x \geq y$.

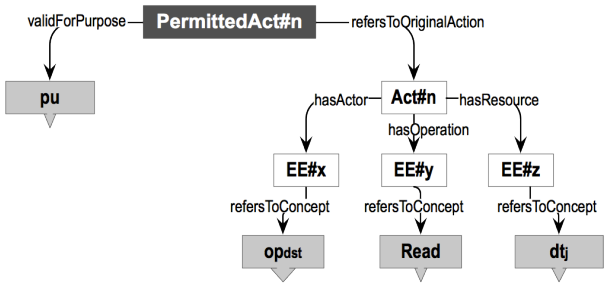
ροής και των δεδομένων εισόδου και εξόδου των λειτουργιών φαίνεται ότι αυτά αφορούν τον ίδιο τύπο δεδομένων, οπότε προχωράμε στον έλεγχο των δικαιωμάτων ανάγνωσης. Η εύρεση της επιτρεπόμενης ενέργειας `PermittedAct#n` (Σχήμα 18β′) καθιστά έγκυρη την αλληλεπίδραση, υπό συγκεκριμένες ωστόσο προϋποθέσεις τις οποίες θέτει η λογική σχέση `LogAND#n`. Τα υποκείμενα των εκφράσεων αποτελούν και πάλι συνιστώσες του τύπου $dt_i$, με τον ένα τύπο να είναι ο ίδιος με αυτόν του περιορισμού της ακμής. Συνεπώς, οι εκφράσεις αποτελούν περιορισμούς φιλτραρίσματος και θα πρέπει να συγχωνευθούν —τόσο στο προφίλ εκτέλεσης της πρόσθετης εργασίας, όσο και στο επίπεδο της ακμής που θα ενώσει

την πρόσθετη εργασία με την εργασία-προορισμό— με εκείνους που προδιαγράφηκαν για την ακμή του αρχικού διμερούς συσχετισμού. Το Σχήμα 18γ′ απεικονίζει την τελική έγκυρη μορφή του υπό εξέταση διμερούς συσχετισμού, μετά την προσθήκη της εργασίας επιλογής, με κατάλληλη ρύθμιση των παραμέτρων της λειτουργίας της, και την αντικατάσταση της αρχικής ακμής.

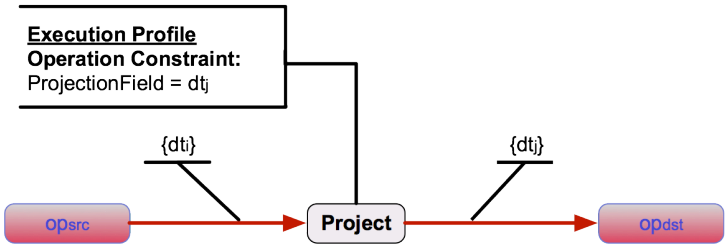
**Εργασία προβολής** Η πράξη της *προβολής* (*projection*) της σχεσιακής άλγεβρας που υλοποιεί η εργασία αυτή υπαγορεύεται είτε από τα δικαιώματα ανάγνωσης της λειτουργίας $op_{dst}$, είτε από καθεαυτό το χαρακτηριστικό της λειτουργίας να λάβει συγκεκριμένους τύπους δεδομένων. Όπως φαίνεται στο Σχήμα 19α′, ο μεταδιδόμενος τύπος δεδομένων $dt_i$ περιλαμβάνεται μόνο στο σύνολο $ODT_{src}$. Ωστόσο, το σύνολο $IDT_{dst}$ περιλαμβάνει τον τύπο $dt_j$, για τον οποίο ισχύει $dt_j \xrightarrow{\texttt{isPartOf}} dt_i$. Η εύρεση των σχετικών δικαιωμάτων ανάγνωσης της λειτουργίας $op_{dst}$ για αυτόν τον τύπο δεδομένων (Σχήμα 19β′) υπονοεί την προσθήκη της εργασίας προβολής, η οποία αποσπά από τον τύπο $dt_i$ το επιτρεπτό πεδίο του $dt_j$, με κατάλληλη ρύθμιση των παραμέτρων της λειτουργίας της και παράλληλη διαμόρφωση των νέων ακμών (Σχήμα 19γ′).




(α′) Ελεγχος συμφωνίας τύπων δεδομένων




(β′) Έλεγχος δικαιωμάτων ανάγνωσης




(γ′) Προσθήκη εργασίας προβολής

Σχήμα 19: Περίπτωση Προβολής Μεταδιδόμενων Δεδομένων. Ο τύπος $dt_j$ αποτελεί πεδίο του τύπου $dt_i$.

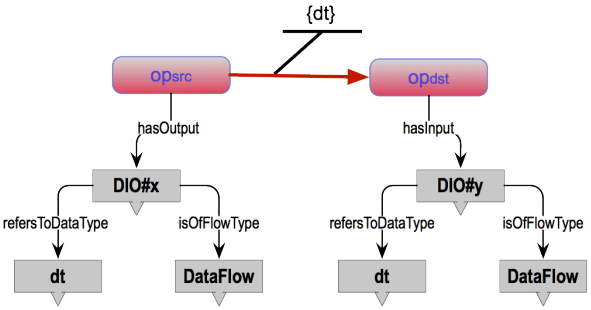
**Εργασία ανασύνθεσης** Αποτελεί το αντίστροφο της προβολής και η προσθήκη της εξετάζεται στην περίπτωση όπου ο μεταδιδόμενος τύπος δεδομένων $dt_i$ περιλαμβάνεται μόνο στο σύνολο $IDT_{dst}$, ενώ το σύνολο $ODT_{src}$ περιέχει τουλάχιστον έναν τύπο που αποτελεί πεδίο του $dt_i$. Εάν όλες οι συνιστώσες του $dt_i$ περιλαμβάνονται στο $ODT_{src}$, τότε αυτές τρο-

φοδοτούν την εργασία ανασύνθεσης, η οποία με τη σειρά της συνθέτει τον τύπο $dt_i$ από τα πεδία του και τροφοδοτεί την εργασία-προορισμό. Στην περίπτωση που η ανασύνθεση δεν μπορεί να πραγματοποιηθεί μόνο με τύπους του $ODT_{src}$, αναζητούνται άλλες λειτουργίες που δύνανται να παράσχουν τις υπόλοιπες συνιστώσες, με παράλληλο έλεγχο των δικαιωμάτων ανάγνωσης (βλ. επίσης Ενότητα 7.5.3).

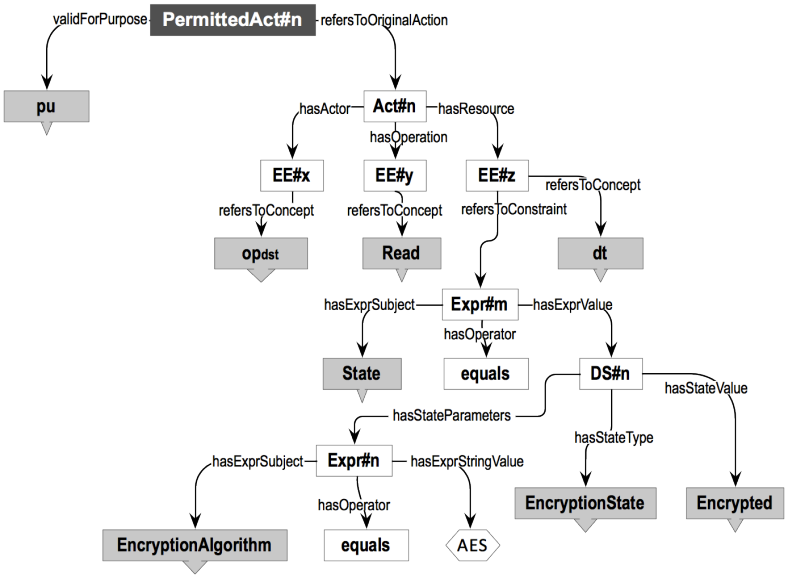
**Εργασία αλλαγής κατάστασης** Χαρακτηριστικά παραδείγματα εργασιών αυτού του τύπου αποτελούν η *κρυπτογράφηση* (*encryption*) και η *ανωνυμοποίηση* (*anonymisation*) των δεδομένων πριν φτάσουν στην είσοδο της λειτουργίας $op_{dst}$. Η προσθήκη τέτοιων εργασιών υπαγορεύεται από *περιορισμούς αλλαγής κατάστασης*, οι οποίοι ορίζονται στο επίπεδο του διμερούς συσχετισμού ή/και στους κανόνες και προδιαγράφονται με χρήση εκφράσεων οι οποίες αναφέρονται στην κατάσταση των μεταδιδόμενων δεδομένων. Έτσι, στο Σχήμα 20β′ φαίνεται ότι οι περιορισμοί υπαγορεύονται από κανόνες, μέσω της επιτρεπόμενης ενέργειας. Ο περιορισμός που μοντελοποιεί η έκφραση `Expr#m` επιβάλλει τα δεδομένα να είναι κρυπτογραφημένα και μάλιστα με κάποιο συγκεκριμένο τρόπο, οδηγώντας στην προσθήκη της εργασίας κρυπτογράφησης του Σχήματος 20γ′. Σημειώνεται ότι μία τέτοια μετατροπή είναι δυνατόν να εφαρμόζεται μόνο σε συγκεκριμένα πεδία των εν λόγω δεδομένων και όχι σε ολόκληρη τη δομή των δεδομένων, όπως συμβαίνει στο συγκεκριμένο παράδειγμα.

Τα παραπάνω πρότυπα είναι δυνατόν να εφαρμοστούν συνδυαστικά, ως απόρροια ιδιαίτερα εκφραστικών περιορισμών που επιβάλλουν οι κανόνες. Ένα τέτοιο παράδειγμα παρουσιάζεται στο Σχήμα 21, όπου τα δεδομένα εξόδου της λειτουργίας $op_{src}$ πρώτα φιλτράρονται και στη συνέχεια υποβάλλονται σε προβολή ώστε να τροφοδοτήσουν καταλλήλως την είσοδο της $op_{dst}$. Ο συνδυασμός αυτός προκύπτει από τους περιορισμούς πάνω στην επιτρεπόμενη ενέργεια (Σχήμα 21β′), σύμφωνα με τους οποίους η λειτουργία $op_{dst}$ επιτρέπεται να διαβάσει τμήμα των δεδομένων εξόδου $dt_i$ της $op_{src}$ ($dt_j \xrightarrow{\texttt{isPartOf}} dt_i$), εάν ο περιέκτης τους, δηλαδή ο τύπος $dt_i$ ικανοποιεί κάποια συνθήκη σχετική με μία άλλη συνιστώσα του $dt_k$.

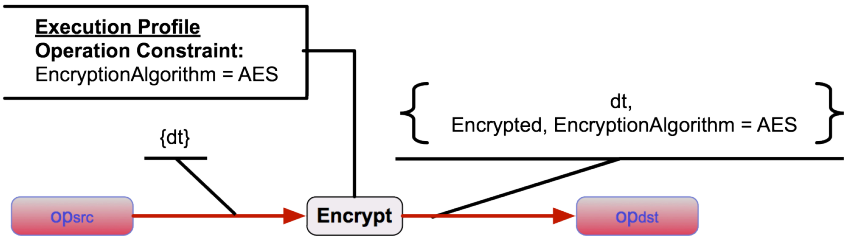
Τέλος, σημειώνεται ότι με την ολοκλήρωση των ελέγχων για όλους τους τύπους δεδομένων που σχετίζονται με την εκάστοτε εναλλακτική ακμή πραγματοποιείται μία διαδικασία συγχώνευσης των τύπων που θα συμπεριληφθούν τελικά στην έγκυρη ακμή. Η διαδικασία λαμβάνει υπόψη τόσο τους περιορισμούς πλαισίου που ορίζουν τα δικαιώματα ανάγνωσης όσο και το σύνολο συνθηκών *FC* της αρχικής ροής. Με τον τρόπο αυτόν, είναι δυνατόν να προκύψουν διαφορετικές ή νέες διακλαδώσεις των ροών ελέγχου/δεδομένων. Επίσης, με βάση τα παραπάνω, ο τελικός διμερής συσχετισμός όπως διαμορφώθηκε μετά τους ελέγχους και τις ενδεχόμενες προσθήκες εμβόλιμων εργασιών, στην πραγματικότητα δεν αποτελεί κατ' ανάγκη διμερή συσχετισμό, καθώς είναι δυνατόν να περιλαμβάνει περισσότερες από τις αρχικές δύο εργασίες και περισσότερες από μία ακμές.




(α′) Ελεγχος συμφωνίας τύπων δεδομένων




(β′) Έλεγχος δικαιωμάτων ανάγνωσης

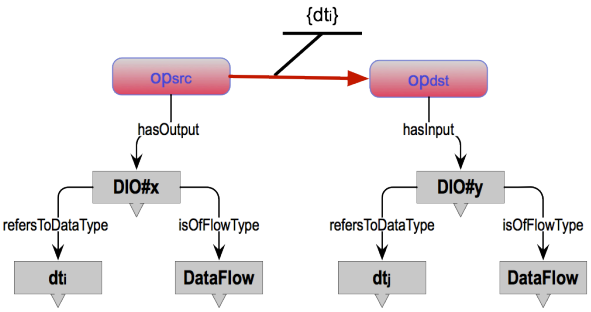



(γ′) Προσθήκη εργασίας αλλαγής κατάστασης

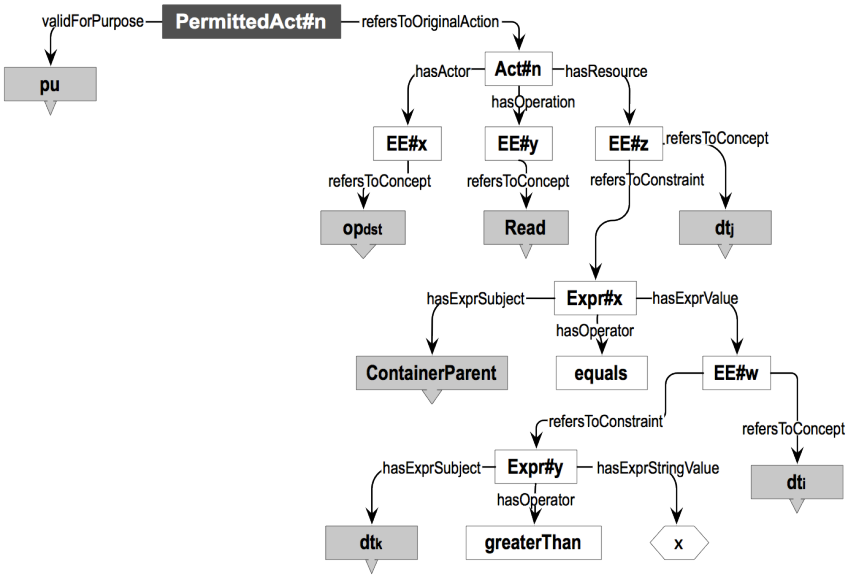
Σχήμα 20: Περίπτωση Αλλαγής Κατάστασης Μεταδιδόμενων Δεδομένων

### 7.5.3 Προσδιορισμός Απαραίτητων και Απαγορευμένων Εργασιών

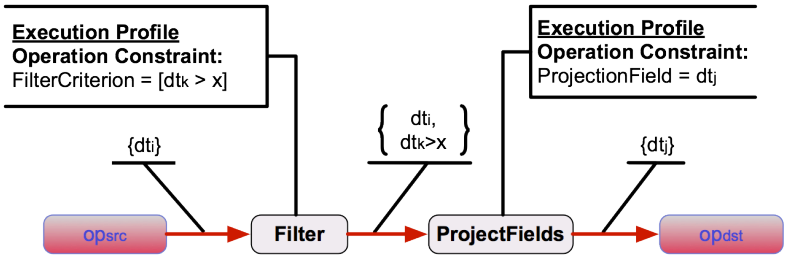
Μετά την επαλήθευση καθεαυτού του διμερούς συσχετισμού, τόσο στο επίπεδο των εργασιών όσο και στο επίπεδο της μεταξύ τους αλληλεπίδρασης, και την εξαγωγή των σχετικών οδηγιών εγκυρότητας, το τελευταίο στάδιο αφορά στον εντοπισμό τρίτων εργασιών που θα πρέπει να συμπληρώνουν εκείνες του διμερούς συσχετισμού, ώστε αυτός να επιτρέπεται τελικά να εκτελεστεί, ή εργασιών που έρχονται σε σύγκρουση με αυτές και επομένως απαγορεύεται να εκτελούνται σε συνδυασμό με το συσχετισμό, καθώς και τον




(α′) Ελεγχος συμφωνίας τύπων δεδομένων




(β′) Έλεγχος δικαιωμάτων ανάγνωσης




(γ′) Προσθήκη εργασιών επιλογής και προβολής

Σχήμα 21: Συνδυαστική Προσθήκη Εργασιών Μετασχηματισμού

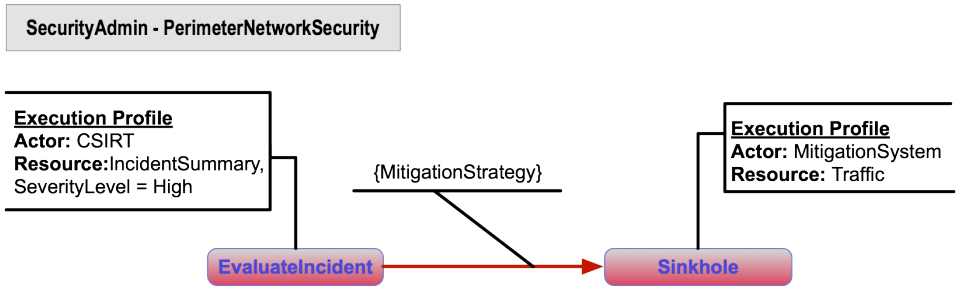
προσδιορισμό της σχετικής ή απόλυτης θέσης τους σε σχέση με τις εργασίες αναφοράς.

Για την πραγματοποίηση των απαραίτητων ελέγχων, οι εργασίες που περιλαμβάνονται στο συσχετισμό, συμπεριλαμβανομένων κι εκείνων που ενδεχομένως προστέθηκαν κατά την επαλήθευση της αλληλεπίδρασης (βλ. Ενότητα 7.5.2) αντιστοιχίζονται και πάλι σε επιτρεπόμενες ενέργειες με τον τρόπο που περιγράφηκε στις προηγούμενες ενότητες, λαμβάνοντας υπόψη το ζεύγος σκοπού-εκκινητή και τις ισχύουσες συνθήκες, ώστε να εξαχθούν από αυτές όλες οι απαραίτητες και απαγορευμένες προ- και μετα- ενέργειες. Έτσι,

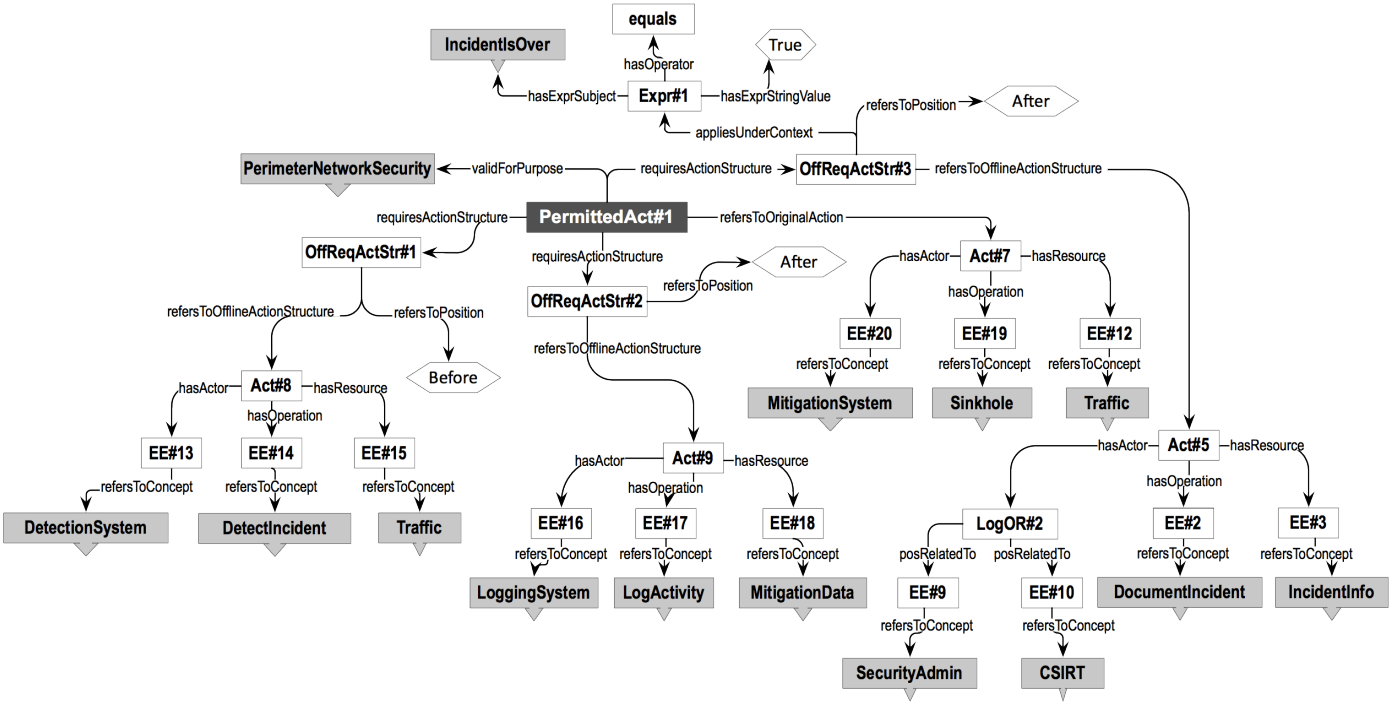
για κάθε επιτρεπόμενη ενέργεια, συγκεντρώνονται όλα τα συσχετισμένα με αυτήν στιγμιότυπα της κλάσης `OfflineRequiredActionStructures`, μέσω των ιδιοτήτων `requires-ActionStructure` και `forbidsActionStructure`, με την πρώτη να υποδεικνύει τις απαραίτητες διενέργειες και τη δεύτερη τις απαγορευμένες (βλ. Ενότητα 6.2.1). Ωστόσο, λόγω των διαφορών που παρουσιάζουν οι εργασίες και οι ενέργειες ως προς τον ορισμό τους, αφενός οι ενέργειες που συγκεντρώθηκαν δε μεταφράζονται όλες απαραίτητα σε εργασίες, καθώς είναι πιθανό να συνιστούν ενέργειες ανάγνωσης και επομένως θα πρέπει να μεταφραστούν ως ακμές του διμερούς συσχετισμού, αφετέρου η ίδια διαδικασία θα πρέπει να πραγματοποιηθεί για τις ακμές που περιλαμβάνει ο συσχετισμός, διότι η ανάγνωση κάποιων δεδομένων από μία λειτουργία συνιστά ενέργεια στο επίπεδο του ελέγχου πρόσβασης. Κατά συνέπεια, η διαδικασία αυτή οδηγεί στη διαμόρφωση οδηγιών απαίτησης εκτέλεσης, απαγόρευσης εκτέλεσης, απαίτησης εισόδου και απαγόρευσης εισόδου, με τα δύο πρώτα είδη οδηγιών να αφορούν εργασίες και τα άλλα δύο ακμές. Σημειώνεται ότι οδηγίες απαίτησης εισόδου είναι δυνατόν να προκύψουν και λόγω της προσθήκης εμβόλιμης εργασίας ανασύνθεσης.

Όλη η απαραίτητη πληροφορία για τη διαμόρφωση των εν λόγω οδηγιών, όπως πληροφορία σχετική με τις συνθήκες πλαισίου, καθώς και λοιπές προϋποθέσεις και μετασυνθήκες για την εφαρμογή τους, υπαγορεύεται από τη δομή των απαραίτητων διενεργειών. Παραδείγματος χάριν, όπως φαίνεται στο Σχήμα 22 και όσον αφορά την εργασία-προορισμό του έγκυρου μετασυσχετισμού του Σχήματος 22α′, οι απαιτούμενες διενέργειες της επιτρεπόμενης ενέργειας `PermittedAct#1`, δηλαδή οι `OffReqActStr#1`, `OffReqActStr#2` και `OffReqActStr#3`, υπαγορεύουν την εκτέλεση των εργασιών του Σχήματος 22γ′ πριν ή μετά την εκτέλεση της εργασίας αναφοράς. Για καθεμία από τις εργασίες αυτές δημιουργείται η αντίστοιχη οδηγία απαίτησης εκτέλεσης, η οποία, εκτός από την απαραίτητη εργασία, περιλαμβάνει επιπλέον πληροφορία για τον απόλυτο ή σχετικό χρόνο εκτέλεσής της σε σχέση με το χρόνο εκτέλεσης της εργασίας αναφοράς, καθώς και τις συνθήκες κάτω από τις οποίες θα εφαρμοστεί η εν λόγω οδηγία. Ειδικά σε ό,τι αφορά τις οδηγίες απαίτησης εκτέλεσης και εισόδου, πραγματοποιείται ένας επιπλέον έλεγχος για παράλειψη εκείνων που αφορούν εργασίες ή δεδομένα που περιλαμβάνονται ήδη στο συσχετισμό. Για δεδομένα που περιλαμβάνονται στην αρχική ακμή του διμερούς συσχετισμού, και για τα οποία δεν προέκυψαν δικαιώματα ανάγνωσης από την εργασία-προορισμό, δε δημιουργούνται ξεχωριστές οδηγίες απαγόρευσης εισόδου.

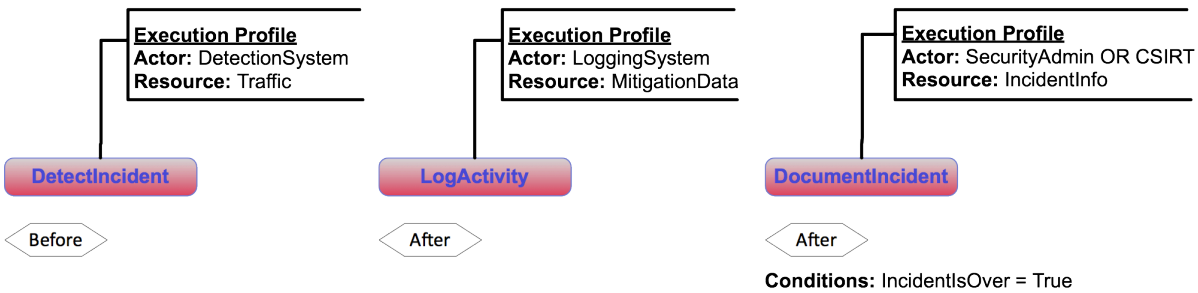
Τέλος, αξίζει να σημειωθεί ότι αν και αυτές οι οδηγίες θα μπορούσαν να έχουν εξαχθεί νωρίτερα, στο στάδιο της εξαγωγής των αυτόνομα έγκυρων εργασιών και στο στάδιο του ελέγχου δικαιωμάτων ανάγνωσης, έγινε η επιλογή το βήμα αυτό να αποτελέσει το τελευταίο της διαδικασίας επαλήθευσης ενός διμερούς συσχετισμού, ώστε να αποφευχθεί η πραγματοποίηση πολύπλοκων υπολογισμών για συσχετισμούς που στο τέλος είναι δυνατόν να αποδειχθούν μη επαληθεύσιμοι.




(α′) Έγκυρος Μετασυσχετισμός




(β′) Επιτρεπόμενη ενέργεια για την εργασία-προορισμό




(γ′) Εργασίες που απαιτούνται να εκτελεστούν λόγω της εργασίας προορισμού

Σχήμα 22: Εξαγωγή Οδηγιών Απαίτησης Εκτέλεσης

## 7.6 Επαλήθευση Διμερών Συσχετισμών στο Πλαίσιο Επαλήθευσης Ροής Εργασιών

Η διαδικασία συλλογιστικής που παρουσιάστηκε στις προηγούμενες ενότητες για την επαλήθευση ενός διμερούς συσχετισμού εφαρμόστηκε επιτυχώς για την επαλήθευση κατανεμημένων ροών εργασιών αναφορικά με την προστασία της ιδιωτικότητας, στα πλαίσια του ευρωπαϊκού ερευνητικού προγράμματος FP7 ICT DEMONS[21], προωθώντας κατ' αυτόν τον τρόπο τη διασφάλιση *Ιδιωτικότητας εκ Σχεδιασμού* (*Privacy by Design*) [127]. Η Ιδιωτικότητα εκ Σχεδιασμού πραγματεύεται μία σειρά από αρχές που πρέπει να εξετάζονται σε όλες τις φάσεις της διαδικασίας ανάπτυξης τεχνολογιών, από την αρχική ανάλυση μέχρι την τελική υλοποίηση τους, με σκοπό την ενσωμάτωση απαιτήσεων ιδιωτικότητας και προστασίας των δεδομένων στο νωρίτερο δυνατό στάδιο του κύκλου ζωής των νέων τεχνολογιών.

Ο κύκλος ζωής μίας ροής εργασιών περιλαμβάνει δύο φάσεις, το *Σχεδιασμό* (*Planning*) και την *Εκτέλεση* (*Execution*) [128]. Κατά τη διάρκεια της φάσης σχεδιασμού, πραγματοποιείται ο προσδιορισμός της ροής εργασιών, ο οποίος περιλαμβάνει όλα τα βήματα για το γραφικό ορισμό της ροής, την αποσύνθεσή της σε στοιχειώδεις εργασίες, τον έλεγχο της συμμόρφωσής της με τις πολιτικές ασφάλειας και προστασίας της ιδιωτικότητας, καθώς και τους ενδεχόμενους απαραίτητους μετασχηματισμούς που θα πρέπει να υποστεί, με βάση το αποτέλεσμα του ελέγχου συμμόρφωσης. Από την άλλη πλευρά, η φάση εκτέλεσης στηρίζεται στην έκβαση της φάσης σχεδιασμού και αναφέρεται στην εγκατάσταση της ροής εργασιών στο σύστημα και την επακόλουθη εκτέλεσή της από τα αντίστοιχα στοιχεία.

Ένα σημαντικό μέρος της φάσης σχεδιασμού είναι η λεγόμενη *Διαδικασία Επαλήθευσης* [129][130][131], η οποία ουσιαστικά καθοδηγείται από το προτεινόμενο Μοντέλο Ελέγχου Πρόσβασης και Χρήσης. Στο πλαίσιο αυτό, ο *Αναλυτής Ροών Εργασιών* αναλύει την οντολογία της υπό εξέτασης ροής εργασιών και περνά στη Μηχανή Συμπερασμού τα ζεύγη σκοπών-εκκινητών που ορίζονται για την εν λόγω ροή και όλους τους διμερείς συσχετισμούς που σχηματίζουν οι εργασίες της. Όπως προκύπτει από τον Αλγόριθμο 11 που περιγράφει σε υψηλό επίπεδο τη διαδικασία επαλήθευσης διμερών συσχετισμών μίας ροής εργασιών, αυτή περιλαμβάνει όλα τα στάδια επαλήθευσης διμερούς συσχετισμού όπως περιγράφηκαν στον Αλγόριθμο 7. Σημειώνεται ότι η εξαγωγή των αυτόνομα έγκυρων εργασιών πραγματοποιείται στο επίπεδο της ροής εργασιών και όχι ξεχωριστά για κάθε διμερή συσχετισμό, ώστε να αποφευχθεί επανάληψη του βήματος αυτού κάθε φορά που μία εργασία συμμετέχει σε περισσότερους του ενός διμερείς συσχετισμούς. Η διαδικασία ολοκληρώνεται με τη Μηχανή Συμπερασμού να παρέχει στον Αναλυτή Ροών Εργασιών τις κατάλληλες οδηγίες που θα πρέπει να εφαρμοστούν στην υπό εξέταση ροή εργασιών, ώστε

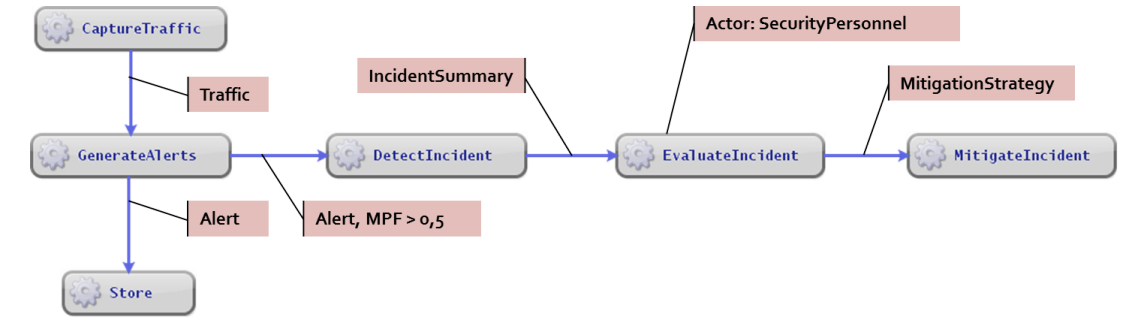
[21]DEcentralized, cooperative, and privacy-preserving MONitoring for trustworthinesS — DEMONS, homepage: http://fp7-demons.eu/.

οι λειτουργίες για την προστασία της ασφάλειας και της ιδιωτικότητας να είναι εγγενώς ενσωματωμένες σε αυτήν ήδη από τη φάση σχεδιασμού της, χωρίς αυτό να σημαίνει ότι δεν θα χρειαστεί περαιτέρω αλληλεπίδραση με τη Μηχανή Συμπερασμού σε μετέπειτα στάδια της διαδικασίας επαλήθευσης, π.χ., σε περίπτωση εντοπισμού ασυνεπειών. Το Σχήμα 23 παρουσιάζει την αρχική και την επαληθευμένη προδιαγραφή μίας ροής εργασιών, όπως αυτή τελικά διαμορφώνεται από τον Αναλυτή Ροών Εργασιών μετά την εφαρμογή των οδηγιών της Μηχανής Συμπερασμού.

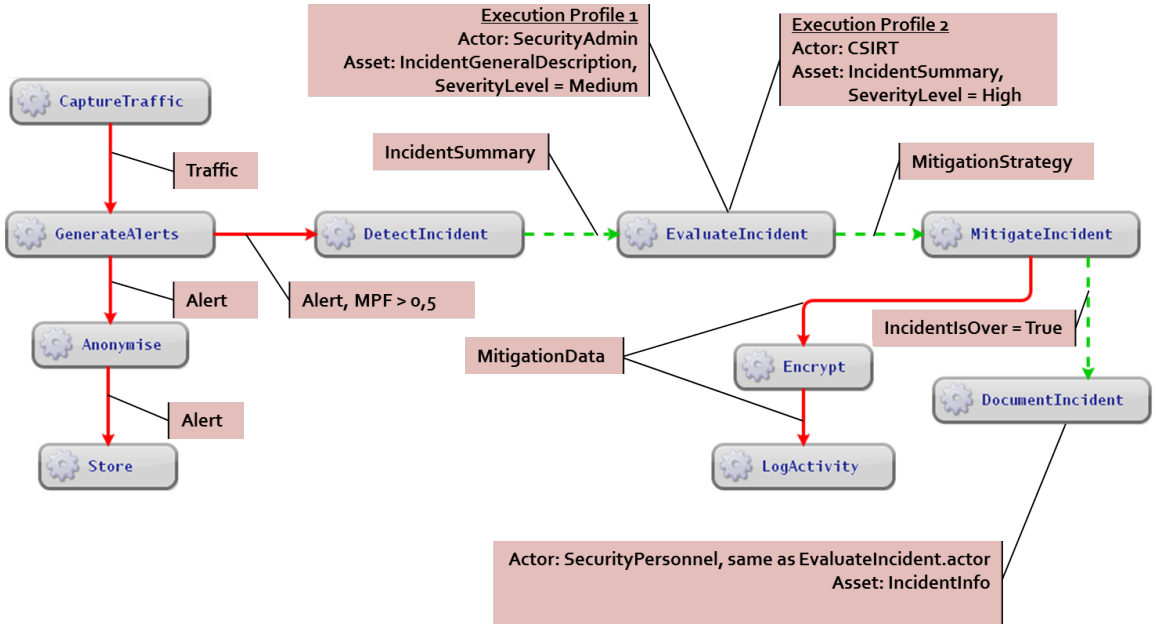
**Αλγόριθμος 11** VerifyWorkflowBilateralAssociations

**Input:** *PIP, BA*
**Output:** *DIR*

1: $LPIP \leftarrow$ GenerateLeafPIPs(*PIP*)
2: $WT \leftarrow$ ExtractWorkflowTasks(*BA*)
3: $WOP \leftarrow$ ExtractWorkflowOperations(*BA*)
4: $WSAVT \leftarrow \emptyset$
5: $DIR \leftarrow \emptyset$
6: **for each** $lpip$ **in** $LPIP$ **do**
7: $pipIsValid \leftarrow$ VerifyPIP(*lpip*, *WOP*)
8: **if** $pipIsValid$ **then**
9: **for each** $wt$ **in** $WT$ **do**
10: $SAVT \leftarrow$ CheckStandAloneTaskValidity(*wt*, *lpip*)
11: $WSAVT$.add($SAVT$)
12: **end for**
13: **if** $WSAVT \neq \emptyset$ **then**
14: **for each** $ba$ **in** $BA$ **do**
15: $SAVST \leftarrow$ AssociateOrigSrcTaskWithStAlValidTasks(*ba*, *WSAVT*)
16: $SAVDT \leftarrow$ AssociateOrigDstTaskWithStAlValidTasks(*ba*, *WSAVT*)
17: $BA' \leftarrow \emptyset$
18: **if** $SAVST \neq \emptyset$ && $SAVDT \neq \emptyset$ **then**
19: $BA' \leftarrow$ GeneratePotentiallyValidBAs(*SAVST*, *SAVDT*)
20: **end if**
21: **for each** $ba'$ **in** $BA'$ **do**
22: $DIR$.add(VerifyMetaAssociation(*ba'*, *ba*, *lpip*))
23: **end for**
24: **end for**
25: **end if**
26: **end if**
27: **end for**
28: **return** *DIR*




(α′) Αρχική προδιαγραφή ροής εργασιών




(β′) Μετασχηματισμένη έγκυρη προδιαγραφή ροής εργασιών

Σχήμα 23: Επαλήθευση Ροής Εργασιών

# Κεφάλαιο 8

# Αξιολόγηση της Προτεινόμενης Λύσης

Το Κεφάλαιο αυτό παρουσιάζει την αξιολόγηση της προτεινόμενης λύσης. Η αξιολόγηση πραγματοποιείται σε δύο βάσεις: τις βασικές αρχές που θα πρέπει να ακολουθεί το σύστημα, όπως αυτές προέκυψαν από τη μελέτη των απαιτήσεων ασφάλειας και ιδιωτικότητας, και την επίδοση των προτεινόμενων διαδικασιών για εξαγωγή γνώσης από το Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης και Χρήσης.

## 8.1 Αξιολόγηση σε Σχέση με τις Απαιτήσεις του Συστήματος

Με βάση την Ενότητα 1.2, στην Ενότητα 3.3 συνοψίστηκαν οι απαιτήσεις ιδιωτικότητας που θέτει η νομοθεσία για την προστασία των προσωπικών δεδομένων, σε συνδυασμό με τις απαιτήσεις ασφάλειας και ιδιωτικότητας που δημιουργεί το ίδιο το πλαίσιο λειτουργίας του κατανεμημένου περιβάλλοντος και της αλληλεπίδρασης μεταξύ ετερογενών συστημάτων. Η Ενότητα αυτή αναφέρεται στον τρόπο με τον οποίο η προτεινόμενη λύση ανταποκρίνεται αποτελεσματικά στις απαιτήσεις αυτές.

### 8.1.1 Έλεγχος Πρόσβασης — Πολυδιάστατος Προσδιορισμός Δικαιωμάτων Πρόσβασης

Όπως έχει καταστεί σαφές, το μονοδιάστατο μοντέλο ελέγχου πρόσβασης, όπου προσδιορίζεται απλώς *ποιος χρήστης*, ο οποίος κατέχει *κάποιο ρόλο*, μπορεί να εκτελέσει *κάποια ενέργεια σε κάποιον πόρο*, δεν επαρκεί για την αντιμετώπιση ζητημάτων που σχετίζονται με την εγγενή πολυπλοκότητα της έννοιας της ιδιωτικότητας και όχι μόνο, και ειδικά σε ό,τι αφορά τη λειτουργία κατανεμημένων αλληλεπιδρώντων συστημάτων. Με στόχο την κατά περίπτωση ελαχιστοποίηση των πληροφοριών που υφίστανται επεξεργα-

σία και μεταδίδονται μεταξύ διαφορετικών οργανισμών, η προτεινόμενη προσέγγιση λαμβάνει υπόψη επιπλέον παραμέτρους πέρα από το βασικό τρίπτυχο *δράστης—ενέργεια—πόρος*, περιλαμβάνοντας στα κριτήρια για τη λήψη απόφασης παροχής πρόσβασης τις *ιδιότητες* που χαρακτηρίζουν τις οντότητες που συμμετέχουν στην ενέργεια πρόσβασης, τον *οργανισμό* μέσα στον οποίο λαμβάνει χώρα η ενέργεια πρόσβασης, το *σκοπό* για τον οποίο ζητείται η πρόσβαση, τις *συνθήκες πλαισίου* που θα πρέπει να ισχύουν, και τις αναγκαίες *συμπληρωματικές* ή/και *απαγορευμένες ενέργειες* που θα πρέπει (ή αντιστοίχως απαγορεύεται) να προηγούνται ή να έπονται της ενέργειας πρόσβασης.

Με βάση τα παραπάνω, βασικό ρόλο για την επίτευξη πολυδιάστατου ελέγχου πρόσβασης παίζουν οι έννοιες της *Ενέργειας* και της *Διευρυμένης Οντότητας* που εισάγει η προτεινόμενη προσέγγιση, καθώς και το πλούσιο Σημασιολογικό Μοντέλο Πληροφοριών που αποτελεί τη βάση για το Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης και Χρήσης. Η δομή της ενέργειας αφενός αντικατοπτρίζει πλήρως το γεγονός ότι ένας δράστης πραγματοποιεί κάποια λειτουργία σε κάποιον πόρο εντός κάποιου οργανισμού, αφετέρου η αντιστοίχιση των εμπλεκόμενων οντοτήτων σε διευρυμένες οντότητες επιτρέπει την ιδιαίτερα λεπτομερή περιγραφή μίας ενέργειας, με "ρύθμιση" των χαρακτηριστικών που φέρουν οι οντότητες μέσω του προσδιορισμού των κατάλληλων περιορισμών. Επιπλέον οι *Εκφράσεις* και οι *Λογικές Σχέσεις* επιτρέπουν τον προσδιορισμό πολύπλοκων και εκφραστικών περιορισμών. Καθώς η δομή της ενέργειας χρησιμοποιείται επίσης για τον προσδιορισμό συμπληρωματικών/απαγορευμένων προ/-μετα- ενεργειών, ενώ επίσης οι ενέργειες είναι δυνατόν να ορίζονται σε οποιοδήποτε επίπεδο αφαίρεσης, καθίσταται σαφές ότι οι κανόνες που τελικά προδιαγράφονται με βάση το προτεινόμενο μοντέλο είναι ιδιαίτερα ευέλικτοι και μπορούν να εκφράσουν πολύ σύνθετους περιορισμούς.

Τέλος, ο έλεγχος πρόσβασης δεν εστιάζει σε μεμονωμένες ενέργειες, αλλά η διαδικασία λήψης απόφασης για την παροχή πρόσβασης λαμβάνει υπόψη τόσο τη ροή λειτουργίας όσο και τη ροή δεδομένων στο πλαίσιο της αλληλεπίδρασης μεταξύ συστημάτων, με αποτέλεσμα μία ολιστική θεώρηση του ελέγχου πρόσβασης κατά μήκος ενός *Διμερούς Συσχετισμού*, ο οποίος αντικατοπτρίζει τη λειτουργία ενός κατανεμημένου συστήματος (βλ. Ενότητα 3.2).

### 8.1.2 Σκοπός Συλλογής και Επεξεργασίας Δεδομένων

Η "αρχή του σκοπού" είναι απαραίτητη για την επίτευξη επίγνωσης της ιδιωτικότητας, καθώς αποτελεί αναπόσπαστο κομμάτι της διασφάλισης της νομιμότητας κατά τη συλλογή και επεξεργασία των δεδομένων [12]. Στην προτεινόμενη προσέγγιση η έννοια του σκοπού κατέχει σημαντική θέση, η οποία αντανακλάται ήδη από τον προσδιορισμό ενός ή περισσότερων σκοπών για την πραγματοποίηση της αλληλεπίδρασης στο πλαίσιο ενός κατανεμημένου συστήματος (βλ. Ενότητα 3.2). Ως εκ τούτου, το Μοντέλο Πληροφοριών περιλαμβάνει το σύνολο των *Σκοπών* (*Purposes — Pu*), που μεταφράζεται στην αντί-

στοιχη οντολογική κλάση του Σημασιολογικού Μοντέλου Πληροφοριών, όπου οι διάφοροι σκοποί και οι μεταξύ τους σχέσεις (γενίκευσης/εξειδίκευσης) περιγράφονται με μεγάλη λεπτομέρεια. Επιπλέον, ο σκοπός αποτελεί αναπόσπαστο κομμάτι των κανόνων και παράμετρο η οποία επηρεάζει το διαχωρισμό και τη σύζευξη καθηκόντων.

Επίσης, η αρχή του σκοπού υπαγορεύει την πρόβλεψη μηχανισμών για τον προσδιορισμό της συμβατότητας μεταξύ σκοπών επεξεργασίας, καθώς και της συμφωνίας των τελευταίων με τους σκοπούς για τους οποίους τα δεδομένα εξαρχής συλλέγονται. Εκτός από τη συμπερίληψη του συνόλου *Pu* στο Μοντέλο Πληροφοριών, προς την κατεύθυνση αυτή προδιαγράφηκε το κατηγόρημα *mayServePurposes*, για την απευθείας συσχέτιση των λειτουργιών συλλογής και επεξεργασίας δεδομένων με τους σκοπούς που αυτές εν δυνάμει εξυπηρετούν. Αντίστοιχα, το προτεινόμενο μοντέλο παρέχει τα μέσα για τον προσδιορισμό των σκοπών για τους οποίους είναι δυνατόν να ενεργεί κάποιος ρόλος (κατηγόρημα *mayActForPurposes*), ενώ προκειμένου να ελεγχθεί η συμβατότητα μεταξύ διαφορετικών σκοπών, αναζητείται αν αυτοί έχουν τουλάχιστον έναν κοινό πρόγονο —δηλαδή έναν πιο γενικό από αυτούς σκοπό— στο γράφο των σκοπών, ακολουθώντας τα μονοπάτια που δημιουργεί η σχέση εξειδίκευσης *isA*. Τα παραπάνω συμπληρώνονται από σαφώς καθορισμένα πρότυπα ώστε οι εν λόγω συσχετίσεις να κληρονομούνται κατά μήκος των αντίστοιχων γράφων των εμπλεκόμενων εννοιών.

Οι αρχές της *αναγκαιότητας*, της *καταλληλότητας* και της *αναλογικότητας* είναι επίσης στενά συνδεδεμένες με την έννοια του σκοπού. Στην πραγματικότητα, το προτεινόμενο μοντέλο παρέχει τα μέσα για τον προσδιορισμό της αναγκαιότητας, καθώς και για να ελεγχθεί εάν η συλλογή ή η επεξεργασία κάποιων συγκεκριμένων δεδομένων είναι αναγκαία για την παροχή κάποιας υπηρεσίας. Στο πλαίσιο αυτό, η προσέγγιση που ακολουθήθηκε για τον προσδιορισμό των κανόνων ελέγχου πρόσβασης και χρήσης υλοποιεί μία σχέση ανάμεσα σε δεδομένα, λειτουργίες συλλογής και επεξεργασίας, ρόλους και σκοπούς, επιτρέποντας έτσι τον ορισμό περιορισμών σχετικών με την αναγκαιότητα και την αναλογικότητα. Πράγματι, ο σκοπός καταλαμβάνει ξεχωριστή θέση στη δομή του κανόνα.

### 8.1.3 Έλεγχος Ροής Πληροφορίας

Η προτεινόμενη προσέγγιση δίνει ιδιαίτερο βάρος στον έλεγχο της πληροφορίας που ανταλλάσσεται στα πλαίσια της λειτουργίας ενός κατανεμημένου συστήματος. Το πρώτο βήμα προς αυτήν την κατεύθυνση αποτελεί η συμπερίληψη της έννοιας του οργανισμού στη δομή της ενέργειας, επιλογή η οποία επιτρέπει ένας κανόνας να αναφέρεται σε ενέργειες (ενέργεια πρόσβασης, προ-/μετα- ενέργειες) που εκτελούνται σε διαφορετικούς οργανισμούς. Έτσι, είναι δυνατόν να παρεμποδίζεται η κοινοποίηση κάποιων δεδομένων από ένα σύστημα σε κάποιο άλλο, ενώ το τελευταίο μπορεί να επιτρέπεται να λαμβάνει τα ίδια δεδομένα από ένα τρίτο σύστημα.

Ουσιαστικά όμως, ροή πληροφορίας με επίγνωση ασφάλειας και ιδιωτικότητας επι-

τυγχάνεται μέσω της αξιολόγησης καθεαυτής της αλληλεπίδρασης μεταξύ των εργασιών του διμερούς συσχετισμού (βλ. Ενότητα 7.5.2), και συγκεκριμένα με τον έλεγχο των δικαιωμάτων ανάγνωσης των δεδομένων, τα οποία ανταλλάσσονται στο πλαίσιο της αλληλεπίδρασης, από τις εμπλεκόμενες λειτουργίες και την προσθήκη εργασιών μετασχηματισμών ροής, όπου αυτό κρίνεται αναγκαίο. Έτσι, διασφαλίζεται ότι η υπό εξέταση αλληλεπίδραση θα πραγματοποιηθεί μόνο εφόσον υπάρχουν τα απαραίτητα δικαιώματα ανάγνωσης για καθέναν από τους τύπους δεδομένων που ανταλλάσσονται και για τους σκοπούς που εξυπηρετεί η εν λόγω αλληλεπίδραση, ενώ τα δικαιώματα ανάγνωσης ενδέχεται να υπαγορεύουν τις συνθήκες πλαισίου κάτω από τις οποίες καθίσταται επιτρεπτή η αλληλεπίδραση. Επιπλέον, καθώς τα δικαιώματα πρόσβασης είναι δυνατόν να αφορούν *μέρος* μόνο της ανταλλασσόμενης πληροφορίας (σχέση *isPartOf* του Μοντέλου Πληροφοριών), πληροφορία που πρέπει να φέρει συγκεκριμένα *χαρακτηριστικά* (περιορισμοί της διευρυμένης οντότητας που αποτελεί τον πόρο της ενέργειας) ή πληροφορία σε διαφορετική *κατάσταση* από την προσδιορισμένη (περιορισμοί της διευρυμένης οντότητας του πόρου με βάση την ιδιότητα κατάστασης *state*), όπως η απαίτηση η σχετική πληροφορία να είναι κρυπτογραφημένη, η προσθήκη των εργασιών μετασχηματισμού *προβολής*, *επιλογής* και *αλλαγής κατάστασης*, αντίστοιχα, διασφαλίζει τελικά την ελαχιστοποίηση των πληροφοριών που μεταδίδονται, ικανοποιώντας τις αρχές της αναγκαιότητας, της καταλληλότητας και της αναλογικότητας. Το ίδιο ισχύει και για την περίπτωση που κάποιος από τους αρχικά προσδιορισμένους τύπους δεδομένων που μεταδίδονται αντικαθίσταται βάσει των δικαιωμάτων ανάγνωσης με κάποιον λιγότερο λεπτομερή, μέσω της σχέσης *lessDetailedThan* του Μοντέλου Πληροφοριών.

### 8.1.4 Μη Διασύνδεση

Σε αντίθεση με την απαίτηση για ελεγχόμενη ροή πληροφορίας, η οποία αναφέρεται στην "άμεση" μεταβίβαση δεδομένων μεταξύ συστημάτων, διεργασιών ή ανθρώπων, η ανάγκη για μη διασύνδεση αντανακλά μία γενίκευση προς την κατεύθυνση του αμοιβαίου αποκλεισμού αναφορικά με τη διάθεση ή επεξεργασία των δεδομένων, είτε άμεσα είτε έμμεσα. Στην προτεινόμενη προσέγγιση, η απαίτηση για μη διασύνδεση αντιμετωπίζεται με χρήση προ- ή μέτα- ενεργειών οι οποίες έρχονται σε σύγκρουση με την ενέργεια πρόσβασης. Έτσι, για παράδειγμα, ο περιορισμός *"Για οποιονδήποτε σκοπό και κάτω από οποιεσδήποτε συνθήκες, ο δράστης a επιτρέπεται να επεξεργαστεί δεδομένα τύπου $dt_i$ εάν και μόνο εάν δεν έχει αποκτήσει πρόσβαση σε δεδομένα τύπου $dt_j$"*, ο οποίος έχει σκοπό να αποτρέψει τη διασύνδεση δεδομένων τύπου $dt_i$ και $dt_j$ από κάποιον δράστη, μπορεί να εκφραστεί είτε σαν άδεια είτε σαν απαγόρευση:

**Κανόνας 1** $Permission(*, \langle a, *, dt_i, org\rangle, \neg\langle a, *, dt_j, org\rangle, *, *)$

**Κανόνας 2** $Prohibition(*, \langle a, *, dt_i, org\rangle, \langle a, *, dt_j, org\rangle, *, *)$

Παρατηρούμε ότι και στους δύο κανόνες η ενέργεια πρόσβασης συγκρούεται με

την προ-ενέργεια. Στην πρώτη περίπτωση, ο περιορισμός εκφράζεται ως άδεια για παροχή πρόσβασης στον τύπο δεδομένων $dt_i$, με την προϋπόθεση ο ίδιος δράστης να μην έχει αποκτήσει πρόσβαση σε δεδομένα τύπου $dt_j$, η οποία εκφράζεται ως αρνητική προ-ενέργεια. Στην περίπτωση της απαγόρευσης, η προ-ενέργεια ορίζεται ως θετική.

### 8.1.5 Διαχωρισμός και Σύζευξη Καθηκόντων

Η απάντηση στην απαίτηση για μη διασύνδεση ουσιαστικά αποτελεί παράδειγμα και υποπερίπτωση της περιγραφής περιορισμών διαχωρισμού καθηκόντων. Ακολουθώντας το ίδιο πρότυπο, οι περιορισμοί αυτοί μπορούν να γενικευτούν και με τον ίδιο τρόπο (αλλά με αντιστροφή των προσήμων στις προ-ενέργειες των Κανόνων 1 και 2) να χρησιμοποιηθούν για τη μοντελοποίηση της σύζευξης καθηκόντων. Η γενίκευση αναφέρεται στον προσδιορισμό SoD και BoD περιορισμών στη βάση οποιασδήποτε οντότητας των ενεργειών ενός κανόνα˙ η ίδια η δομή των κανόνων επεκτείνει τις έννοιες του αμοιβαίου αποκλεισμού και της σύζευξης, εφαρμόζοντάς τες σε όλα τα στοιχεία που συνθέτουν μία ενέργεια, δηλαδή τους δράστες, τις λειτουργίες, τους πόρους και τους οργανισμούς. Γίνεται εμφανής η χρησιμότητα των προ- και μετα- ενεργειών στον προσδιορισμό περιορισμών SoD και BoD, για το λόγο ότι επιτρέπουν τη δημιουργία εξαρτήσεων μεταξύ των ενεργειών ενός κανόνα.

### 8.1.6 Συμπληρωματικές Ενέργειες

Η απαίτηση για τον προσδιορισμό συμπληρωματικών ενεργειών αντιμετωπίζεται από το προτεινόμενο μοντέλο ελέγχου πρόσβασης με τον προσδιορισμό στους κανόνες δομών ενεργειών που θα πρέπει να προηγούνται ή να έπονται της ενέργειας πρόσβασης του εκάστοτε κανόνα. Μάλιστα, η έννοια των συμπληρωματικών ενεργειών επεκτείνεται με τον προσδιορισμό και των αντίστοιχων απαγορευμένων ενεργειών. Επιπλέον, οι αναγκαίες και απαγορευμένες προ- και μετα- ενέργειες είναι δυνατόν να εκφράσουν ιδιαίτερα λεπτομερείς και σύνθετες προϋποθέσεις και μετασυνθήκες, επωφελούμενες από τη χρήση της δομής της ενέργειας και συνακολούθως της διευρυμένης οντότητας, δομή η οποία χρησιμοποιείται για τον προσδιορισμό των συνιστωσών της ενέργειας και επιτρέπει την περιγραφή κριτηρίων που θα πρέπει να πληρούν οι σχετικές οντότητες. Με χρήση λογικών συσχετίσεων είναι δυνατόν να οριστούν πολύπλοκες λογικές εκφράσεις προ- και μετα- ενεργειών, ενώ επίσης η προτεινόμενη προσέγγιση εισάγει την έννοια του *Σκελετού* προκειμένου να καταστεί δυνατός ο συνδυασμός ενεργειών, έτσι ώστε οι τελευταίες να σχηματίζουν πολύπλοκες δομές, σε περιπτώσεις όπου περιορισμοί σχετικοί με την αλληλουχία και γενικά με τη ροή είναι απαραίτητο να καθορίζονται, όταν οι λογικές συσχετίσεις ενεργειών δεν αρκούν.

Επιπλέον, η προτεινόμενη προσέγγιση επιτρέπει την περιγραφή περιορισμών σχετικά με το *πότε* εκτελείται κάποια προ-/μετα- ενέργεια σε σχέση με την ενέργεια για την οποία εφαρμόζεται ο κανόνας, απαίτηση που καλύπτεται με την εισαγωγή του κατηγο-

ρήματος *isConstrainedToAct*, το οποίο επιτρέπει τον προσδιορισμό χρονικών περιορισμών και περιορισμών που αφορούν τη σειρά εκτέλεσης για τις προ- και μετα- ενέργειες έχοντας σαν σημείο αναφοράς την κύρια ενέργεια του κανόνα ελέγχου πρόσβασης. Έτσι ένας οντολογικός κανόνας δε συσχετίζεται άμεσα με μία ενέργεια που υποδηλώνει κάποια προ ή μετα- ενέργεια, αλλά με κάποιο στιγμιότυπο της κλάσης `RequiredActions`, ενώ για τον προσδιορισμό των χρονικών περιορισμών και των περιορισμών αλληλουχίας το εν λόγω στιγμιότυπο συσχετίζεται με κάποιο στιγμιότυπο της κλάσης `SequenceConstraints`.

Σημειώνεται ότι συμπληρωματικές ενέργειες είναι δυνατόν να προκύψουν όχι μόνο απευθείας από τις δομές των προ- και μετα- ενεργειών των κανόνων, αλλά και από τους περιορισμούς των διευρυμένων οντοτήτων που αντανακλούν τους πόρους των ενεργειών πρόσβασης, καθώς και από δικαιώματα πρόσβασης μόνο σε τμήμα των δεδομένων για τα οποία ζητείται πρόσβαση. Έτσι, όπως παρουσιάστηκε στην Ενότητα 7.5.2, κατά τον έλεγχο της αλληλεπίδρασης μεταξύ δύο εργασιών, ενδέχεται να προκύψει η ανάγκη για προσθήκη εργασιών μετασχηματισμού της ροής πληροφορίας μεταξύ των εν λόγω εργασιών, όπως είναι η προσθήκη κάποιας εργασίας αλλαγής κατάστασης των μεταδιδόμενων δεδομένων (π.χ. εργασία ανωνυμοποίησης) ή της εργασίας επιλογής δεδομένων που πληρούν συγκεκριμένα κριτήρια.

### 8.1.7 Επίγνωση Πλαισίου

Στην προτεινόμενη προσέγγιση η επίγνωση πλαισίου είναι πλήρως ενσωματωμένη. Ήδη στο Μοντέλο Πληροφοριών ορίζεται το σύνολο *Context* (*Con*) για τον προσδιορισμό παραμέτρων πλαισίου, με την αντίστοιχη οντολογική κλάση `ContextTypes` να περιέχει τους τύπους πληροφορίας πλαισίου. Οι τύποι αυτοί αποτελούν το υποκείμενο σε εκφράσεις, οι οποίες ορίζουν περιορισμούς σχετικούς με το πλαίσιο. Η χρήση λογικών συσχετίσεων επιτρέπει τον προσδιορισμό σύνθετων και λεπτομερών συνθηκών πλαισίου που θα πρέπει να ισχύουν, προκειμένου να τεθεί σε εφαρμογή κάποιος κανόνας ελέγχου πρόσβασης. Μάλιστα, οι κανόνες συσχετίζονται άμεσα με τους περιορισμούς πλαισίου, στο ίδιο επίπεδο με τις ενέργειες και το σκοπό. Τέλος, στα πλαίσια του ελέγχου ενός διμερούς συσχετισμού, καθώς είναι δυνατόν να ορίζονται διαφορετικά δικαιώματα πρόσβασης ανάλογα με τους ισχύοντες περιορισμούς, ενδέχεται να προδιαγραφούν διαφορετικές ροές λειτουργίας και πληροφοριών για διαφορετικές συνθήκες πλαισίου ή/και διαφορετικά προφίλ εκτέλεσης των εργασιών του συσχετισμού.

### 8.1.8 Ετερογενή Περιβάλλοντα

Το προτεινόμενο σύστημα παρέχει εξαιρετικά ευέλικτο τρόπο για αναπαράσταση γνώσης μέσω οντολογιών και είναι αρκούντως γενικό ώστε να μπορεί να υιοθετηθεί από ευρύ φάσμα οργανισμών και εφαρμογών. Μάλιστα, οι κλάσεις του Σημασιολογικού Μοντέλου Πληροφοριών είναι δυνατόν να αντικατασταθούν από άλλες ώστε να αναπαρα-

σταθεί γνώση αναγκαία για κάποιο άλλο πεδίο εφαρμογής, χωρίς να επηρεάζεται το υπερκείμενο Σημασιολογικό Μοντέλο Πολιτικών ή οι διαδικασίες εξαγωγής γνώσης από αυτό. Επιπλέον, οι οντολογίες αποτελούν εξέχουσα τεχνολογία για σημασιολογική διαλειτουργικότητα οργανισμών. Καθώς οντολογίες που έχουν δημιουργηθεί από διαφορετικούς ανθρώπους είναι πολύ φυσικό να εμφανίζουν διαφορές, τόσο συντακτικής αλλά και σημασιολογικής φύσης, ακόμα και αν αυτές αναφέρονται στο ίδιο αντικείμενο, έχουν αναπτυχθεί τεχνολογίες εναρμόνισης οντολογιών, όπως αλγόριθμοι εύρεσης σημασιολογικών ομοιοτήτων και εξαγωγής κανόνων σημασιολογικής συσχέτισης μεταξύ οντολογιών, μηχανισμός ο οποίος αναφέρεται στη βιβλιογραφία ως Ευθυγράμμιση Οντολογιών (Ontology Alignment) [132][133].

Επίσης, το προτεινόμενο μοντέλο ενσωματώνει ρητά την έννοια του οργανισμού στη δομή της ενέργειας. Αυτό, σε συνδυασμό με το γεγονός ότι η δομή του κανόνα συσχετίζεται με ενέργειες σε δύο επίπεδα, δηλαδή τόσο με την ενέργεια πρόσβασης όσο και με τις αναγκαίες ή/και απαγορευμένες προ- και μετα- ενέργειες, καθώς και η χρήση λογικών σχέσεων και εκφράσεων στις διάφορες δομές που απαρτίζουν τον κανόνα, επιτρέπει την προδιαγραφή ιδιαίτερα εκφραστικών και σύνθετων κανόνων, οι οποίοι εξ' ορισμού υποδηλώνουν σχέσεις και εξαρτήσεις μεταξύ διαφορετικών οργανισμών.

Τέλος, σε περίπτωση που δύο συστήματα ενός διμερούς συσχετισμού ανήκουν σε διαφορετικούς οργανισμούς, ο έλεγχος του εν λόγω συσχετισμού ισοδυναμεί με έλεγχο ροής μεταξύ των οργανισμών αυτών, ούτως ώστε να διασφαλίζεται η ιδιωτικότητα των υποκειμένων των δεδομένων καθώς και ευαίσθητη πληροφορία των οργανισμών που περνάει τα σύνορά τους.

### 8.1.9 Μηχανισμοί Ασφάλειας

Χωρίς το θέμα της ασφάλειας αυτής καθεαυτής να αποτελεί το κύριο αντικείμενο της παρούσας διατριβής, η προτεινόμενη λύση εξασφαλίζει την κατά περίπτωση ενσωμάτωση των αναγκαίων μηχανισμών ασφάλειας κατά την αλληλεπίδραση δύο συστημάτων. Οι εν λόγω μηχανισμοί είτε αντανακλώνται από τις απαραίτητες προ- ή/και μετα- ενέργειες ενός κανόνα, είτε προκύπτουν κατά τον έλεγχο της αλληλεπίδρασης ενός διμερούς συσχετισμού (βλ. Ενότητα 7.5.2) από τους περιορισμούς των διευρυμένων οντοτήτων που αντανακλούν τους πόρους των ενεργειών πρόσβασης, όπως συμβαίνει στην περίπτωση της προσθήκης μίας εργασίας κρυπτογράφησης των μεταδιδόμενων δεδομένων.

### 8.1.10 Σημασιολογική Αναπαράσταση Πληροφοριών

Η προτεινόμενη προσέγγιση αξιοποιεί πλήρως τις δυνατότητες των οντολογιών για την προδιαγραφή ιδιαίτερα εκφραστικών κανόνων ελέγχου πρόσβασης. Ένα σημαντικό χαρακτηριστικό της αποτελεί το γεγονός ότι βασίζεται σε ένα σημασιολογικά πλού-

σιο μοντέλο πληροφοριών που περιλαμβάνει πληθώρα εννοιών σχετικών με τον έλεγχο πρόσβασης σε κατανεμημένα περιβάλλοντα, καθώς και τις μεταξύ τους σχέσεις, συμπεριλαμβανομένων εννοιών που δεν έχουν συναντηθεί σε άλλες προσεγγίσεις (π.χ. περιέκτες λειτουργιών), καθώς και σχεσιακών δομών που δεν έχουν εξετασθεί ακόμα ευρέως στη βιβλιογραφία, όπως ιεραρχίες τύπου AND για τους ρόλους. Επιπλέον, θεμελιώνεται στη βάση των απαιτήσεων που προκύπτουν από την επεξεργασία των νομικών και κανονιστικών διατάξεων που αφορούν την προστασία των δεδομένων, γεγονός που αντικατοπτρίζεται από τις έννοιες που περιλαμβάνονται στο μοντέλο.

Οι έννοιες που περιλαμβάνει το μοντέλο μεταφράζονται σε κλάσεις των αντίστοιχων οντολογιών, δηλαδή του Σημασιολογικού Μοντέλου Πληροφοριών και του Σημασιολογικού Μοντέλου Ελέγχου Πρόσβασης και Χρήσης. Στο Σημασιολογικό Μοντέλο Πληροφοριών, τα στιγμιότυπα της κάθε κλάσης είναι δυνατόν να συσχετίζονται μεταξύ τους με ιδιότητες που υποδηλώνουν τη σχέση εξειδίκευσης (ιδιότητα `isA`), τη σχέση συμπερίληψης (ιδιότητα `isPartOf`) ή τη σχέση που εκφράζει το βαθμό λεπτομέρειας (ιδιότητα `lessDetailedThan`). Έτσι, σχηματίζονται ιεραρχίες, οι οποίες επιτρέπουν τον προσδιορισμό εξαρτήσεων καθώς και την κληρονομικότητα χαρακτηριστικών και κανόνων και, συνεπώς, τον ορισμό των κανόνων σε υψηλά επίπεδα αφαίρεσης, με αποτέλεσμα τη μείωση του αριθμού των ρητά οριζόμενων πολιτικών. Σημειώνεται ότι στο μοντέλο προβλέπονται ακόμα συσχετίσεις και μεταξύ στιγμιοτύπων διαφορετικών κλάσεων, όπως η συσχέτιση ενός ρόλου με τους σκοπούς για τους οποίους μπορεί να ενεργεί.

Έχοντας σαν βάση του του το συγκεκριμένο σημασιολογικό μοντέλο πληροφοριών, και παράλληλα περιλαμβάνοντας όλες τις απαραίτητες κλάσεις και ιδιότητες, το Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης και Χρήσης επιτρέπει τελικά την προδιαγραφή σύνθετων κανόνων που προωθούν την προστασία της ιδιωτικότητας και λαμβάνουν υπόψη τα χαρακτηριστικά των εμπλεκόμενων οντοτήτων, τις συνθήκες πλαισίου, περιορισμούς διαχωρισμού και σύζευξης καθηκόντων και άλλες εξαρτήσεις μεταξύ των σχετικών ενεργειών.

## 8.2 Αξιολόγηση Επίδοσης

Ουσιαστικά, αυτό που θα μπορούσε να αποτελέσει ενδεχομένως το βασικότερο πρόβλημα επίδοσης στο προτεινόμενο σύστημα είναι οι διαδικασίες συλλογιστικής. Πράγματι, η εξαγωγή γνώσης πραγματοποιείται με βάση οντολογίες που περιλαμβάνουν μεγάλο αριθμό στιγμιοτύπων συσχετισμένων μεταξύ τους μέσω διαφόρων αντικειμενικών ιδιοτήτων. Λαμβάνοντας επίσης υπόψη την ύπαρξη των διαφόρων βοηθητικών κλάσεων, που ορίζονται για την αναπαράσταση πολύπλοκων δομών (π.χ., η κλάση `Skeletons`, η οποία χρησιμοποιείται για την αναπαράσταση ανεξάρτητων ενεργειών με καλώς ορισμένα πρότυπα αλληλεπιδράσεων μεταξύ τους οι οποίες σχηματίζουν μία σύνθετη ενέργεια, ή η κλάση `EnhancedEntities`, για τον προσδιορισμό οντοτήτων, όπως οι δράστες ή ο πόρος

μίας ενέργειας, που αναφέρονται σε κάποιο σημασιολογικό τύπο και περιγράφονται περαιτέρω μέσω περιορισμών πάνω σε χαρακτηριστικά τους), η συλλογιστική καθίσταται ιδιαίτερα απαιτητική διαδικασία, καθώς ακόμα και σε περιπτώσεις φαινομενικά απλών ερωτημάτων ενδέχεται να είναι απαραίτητη η διάσχιση πολλών ακμών και κόμβων σε περισσότερους του ενός γράφους.

Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση των οντολογικών κανόνων πρόσβασης, για τον προσδιορισμό των οποίων απαιτείται ο προσδιορισμός επιμέρους στιγμιοτύπων. Έτσι, θα πρέπει σε κάθε περίπτωση να οριστεί η ενέργεια πρόσβασης, δηλαδή ένα στιγμιότυπο της κλάσης `Actions`, το οποίο θα συσχετιστεί στη συνέχεια με τους δράστες, τη λειτουργία, τον πόρο και τον οργανισμό. Οι οντότητες της ενέργειας με τη σειρά τους ορίζονται είτε στο επίπεδο προσδιορισμού, μέσω της κλάσης `ConcreteEntities`, είτε ως στιγμιότυπα της κλάσης `EnhancedEntities`. Στη δεύτερη περίπτωση, εάν χρειάζεται να περιοριστούν περαιτέρω οι οντότητες, οι εν λόγω περιορισμοί εκφράζονται μέσω της κλάσης `Expressions`, και σε κάποιες περιπτώσεις σε συνδυασμό με την κλάση `LogicalRelations` για λογικά συσχετισμένους περιορισμούς. Η περίπτωση των προ-/μετα- ενεργειών είναι ακόμα πιο σύνθετη, καθώς οι ενέργειες συσχετίζονται τελικά με τον κανόνα μέσω της κλάσης `RequiredActions`, με την κλάση `LogicalRelations` να παρεμβάλλεται για λογικά συσχετισμένες προ-/μετα- ενέργειες. Καθίσταται λοιπόν σαφές ότι, ακόμα και με την προσθήκη ενός μικρού συνόλου κανόνων στην οντολογία, το μέγεθός της και οι απαιτήσεις της διαδικασίας συλλογιστικής σε πόρους και χρόνο αυξάνονται σημαντικά.

Για τη διαχείριση του ζητήματος της αυξημένης πολυπλοκότητας —σε ένα σύστημα που παρέχει δυνατότητες υψηλής εκφραστικότητας— υιοθετήθηκαν δύο στάδια συλλογιστικής, που αφορούν αντίστοιχα την εξαγωγή γνώσης από το σύνολο των κανόνων και την επαλήθευση της αλληλεπίδρασης μεταξύ δύο συστημάτων, δηλαδή την επαλήθευση ενός δεδομένου διμερούς συσχετισμού. Όπως παρουσιάστηκε στο Κεφάλαιο 6, η διαδικασία εξαγωγής γνώσης από τους κανόνες περιλαμβάνει δύο επιμέρους διαδικασίες, με την πρώτη να αφορά την εξαγωγή των μετακανόνων από τους ρητά προσδιορισμένους κανόνες και τη δεύτερη την καθεαυτή εξαγωγή γνώσης που περιέχεται στους κανόνες, ώστε να χρησιμοποιηθεί στη συνέχεια κατά την επαλήθευση του διμερούς συσχετισμού. Οι μετακανόνες εξάγονται με τη διαδικασία που περιγράφεται στην Ενότητα 6.1, με βάση τις ιεραρχίες του Σημασιολογικού Μοντέλου Πληροφοριών και συγκεκριμένα καλώς ορισμένα πρότυπα κληρονομικότητας κατά μήκος των ιεραρχιών αυτών. Έτσι, το τελικό σύνολο κανόνων καθίσταται διαθέσιμο εκ των προτέρων, υπό την έννοια ότι όταν η Μηχανή Συμπερασμού λάβει ένα αίτημα για παροχή πρόσβασης, δε θα λάβει απόφαση αποτιμώντας τους ρητά προσδιορισμένους κανόνες, γεγονός που θα απαιτούσε παράλληλα την υποβολή σειράς ερωτημάτων προς το Σημασιολογικό Μοντέλο Πληροφοριών, ώστε να ελεγχθεί η εφαρμοσιμότητα του εκάστοτε κανόνα σε οντότητες συσχετισμένες (μέσω ιδιοτήτων του Σημασιολογικού Μοντέλου Πληροφοριών) με εκείνες του κανόνα. Η εξαγωγή των μετακανόνων πραγματοποιείται μόνο σε περίπτωση που μεταβληθεί το σύνολο των κανόνων ή η οντολογία του Μοντέλου Πληροφοριών, μειώνοντας με αυτόν τον τρόπο τους χρόνους απόκρισης

του συστήματος κατά την αποτίμηση αιτημάτων ελέγχου πρόσβασης.

Το δεύτερο σκέλος της διαδικασίας εξαγωγής γνώσης παρουσιάζει το μεγαλύτερο ενδιαφέρον σε ό,τι αφορά τη βελτίωση της επίδοσης του συστήματος. Στην πρώτη φάση υλοποίησης της προτεινόμενης προσέγγισης, ο έλεγχος πρόσβασης βασιζόταν αποκλειστικά στους κανόνες, με αποτέλεσμα για κάθε αίτημα πρόσβασης να πρέπει να αξιολογηθούν συνδυαστικά όλοι οι κανόνες (άδειες, απαγορεύσεις και υποχρεώσεις) που αφορούσαν την εκάστοτε ενέργεια πρόσβασης, δηλαδή όλοι οι κανόνες όπου η εν λόγω ενέργεια εμφανιζόταν είτε σαν ενέργεια πρόσβασης είτε σαν προ-/μετα- ενέργεια. Λαμβάνοντας υπόψη την πολύπλοκη δομή ενός οντολογικού κανόνα, όπως περιγράφηκε παραπάνω, η συλλογιστική απευθείας πάνω στο σύνολο των κανόνων σε πραγματικό χρόνο —όπου πραγματικός χρόνος θεωρείται ο χρόνος αποτίμησης ενός αιτήματος πρόσβασης— είναι ιδιαίτερα απαιτητική σε πόρους και ως εκ τούτου χρονοβόρα, ειδικά σε περιβάλλοντα όπου το σύνολο των κανόνων είναι μεγάλο. Ως εκ τούτου, επιλέχθηκε τελικά να επεκταθεί η οντολογία του Μοντέλου Ελέγχου Πρόσβασης και Χρήσης, ώστε να περιλαμβάνει δομές για την αποθήκευση συνδυαστικής εξαχθείσας γνώσης από τους κανόνες (κλάσεις `PermittedActions` και `OfflineRequiredActionStructures`, βλ. Ενότητα 6.2.1), ώστε να είναι όσο το δυνατόν περισσότερη γνώση διαθέσιμη πριν την υποβολή των αιτημάτων πρόσβασης. Όπως και το στάδιο εξαγωγής μετακανόνων, οι δομές αυτές δημιουργούνται κατά την αρχικοποίηση του συστήματος και η διαδικασία επαναλαμβάνεται κάθε φορά που μεταβάλλονται οι οντολογίες.

Ουσιαστικά, μέσω της παραπάνω διαδικασίας καθίσταται διαθέσιμη η γνώση που αφορά όλες τις επιτρεπόμενες ενέργειες στα πλαίσια της λειτουργίας του συστήματος, συμπεριλαμβανομένων των συνθηκών πλαισίου που θα πρέπει να ισχύουν, το σκοπό εκτέλεσης της εκάστοτε ενέργειας και τις απαιτούμενες ή απαγορευμένες προ- και μετα- ενέργειες. Με τον τρόπο αυτό, χρειάζεται πλέον να διασχιστούν σημαντικά λιγότεροι αλλά και μικρότεροι σε βάθος γράφοι στο Σημασιολογικό Μοντέλο Ελέγχου Πρόσβασης και Χρήσης για την αποτίμηση ενός αιτήματος πρόσβασης, καθώς για κάθε επιτρεπόμενη ενέργεια θα υπάρχει τουλάχιστον ένα στιγμιότυπο της κλάσης `PermittedActions`. Έτσι, κατά την επαλήθευση ενός διμερούς συσχετισμού, όπως παρουσιάστηκε στο Κεφάλαιο 7, υπάρχει διαθέσιμη σχεδόν όλη η γνώση που απαιτείται για την εγκυρότητα της κάθε εργασίας (υπό την έννοια ότι μία εργασία μπορεί να υπονοεί περισσότερες από μία ενέργειες, οπότε απαιτείται συνδυασμός γνώσης, βλ. Ενότητα 7.4), και η συλλογιστική που πραγματοποιείται περιορίζεται στην επαλήθευση των σκοπών και της αλληλεπίδρασης, με ό,τι αυτή συνεπάγεται.

Για την αξιολόγηση των διαδικασιών συλλογιστικής, πραγματοποιήθηκε ένα σύνολο πειραμάτων, όπου οι διαδικασίες αυτές εκτελέστηκαν με βάση διαφορετικές οντολογίες του Σημασιολογικού Μοντέλου Πληροφοριών. Οι εν λόγω διαφοροποιήσεις αφορούσαν ποιοτικά χαρακτηριστικά ως προς τον αριθμό των στιγμιοτύπων, των μεταξύ τους συσχετίσεων και, επομένως, την κληρονομικότητα κανόνων και χαρακτηριστικών, ούτως

ώστε το σύνολο των μετακανόνων που θα προέκυπταν από το ίδιο αρχικό σύνολο ρητά ορισμένων κανόνων να είναι από ∼8 έως ∼60 φορές μεγαλύτερο του αρχικού συνόλου. Σε όλα τα πειράματα χρησιμοποιήθηκε ο ίδιος προσωπικός υπολογιστής, με τα εξής χαρακτηριστικά: επεξεργαστή Intel Core 2 Duo 2.4 GHz, με RAM 4GB, λειτουργικό σύστημα Mac OS X 10.6.8 και Java Runtime Environment v.1.6.

Σε ό,τι αφορά την εξαγωγή των μετακανόνων, παρατηρήθηκε ότι για κάθε ∼500 μετακανόνες απαιτείται ∼1 sec, ενώ για τη δημιουργία των στιγμιοτύπων των κλάσεων `PermittedActions` και `OfflineRequiredActionStructures` με βάση το εκάστοτε τελικό σύνολο των κανόνων ο χρόνος κυμάνθηκε από ∼25 sec για "απλές" οντολογίες της τάξης των ∼600 κανόνων έως ∼700 sec για πολύ μεγάλες οντολογίες της τάξης των ∼4000 κανόνων. Με βάση τις μετρήσεις αυτές γίνεται εμφανές ότι το δεύτερο στάδιο της εξαγωγής γνώσης από τους κανόνες είναι και το πιο απαιτητικό, ωστόσο πραγματοποιείται άπαξ offline, οδηγώντας σε θεαματική βελτίωση των χρόνων απόκρισης της Μηχανής Συμπερασμού στα επόμενα στάδια συλλογιστικής.

Για την αξιολόγηση της διαδικασίας επαλήθευσης ενός διμερούς συσχετισμού, η τελευταία εκτελέστηκε στο σύνολο των οντολογιών του Σημασιολογικού Μοντέλου Πρόσβασης και Χρήσης που προέκυψαν όπως περιγράφηκε παραπάνω, όπου δόθηκε προς επεξεργασία στη Μηχανή Συμπερασμού ένα σύνολο από 8 διμερείς συσχετισμούς διαφοροποιούμενης πολυπλοκότητας ως προς τα χαρακτηριστικά τους. Με εξαγωγή γνώσης από την επέκταση της οντολογίας παρατηρήθηκε βελτίωση κατά μέσο όρο ∼45% σε σχέση με την εξαγωγή γνώσης απευθείας από τους κανόνες, με ελάχιστη βελτίωση ∼33% και μέγιστη ∼57%. Ο μέσος χρόνος επαλήθευσης ενός διμερούς συσχετισμού μετρήθηκε για απλές οντολογίες, όπου ∼100 κανόνες αφορούσαν τους δεδομένους συσχετισμούς, στα ∼310 msec με συλλογιστική απευθείας στη βάση των κανόνων και στα ∼160 msec με εξαγωγή γνώσης από την επέκταση, ενώ η αύξηση του χρόνου που παρατηρήθηκε ήταν μικρή για ∼400 κανόνες σχετικούς με τους εν λόγω συσχετισμούς. Ακόμα και με βάση μεγαλύτερες οντολογίες όπου οι σχετικοί κανόνες είναι πολύ περισσότεροι (π.χ., περισσότεροι από 1000), οι χρόνοι επαλήθευσης παραμένουν σε επίπεδα κάτω του 1 sec, εκτός από κάποιες περιπτώσεις πολύπλοκων διμερών συσχετισμών, για τους οποίους προκύπτουν πολλοί εναλλακτικοί διμερείς μετασυσχετισμοί ή απαιτήσεις για εκτέλεση συμπληρωματικών εργασιών, όπου ο χρόνος απόκρισης φτάνει τα ∼14 και ∼7 sec για καθέναν από τους τρόπους επαλήθευσης, αντίστοιχα.

Τέλος, θα πρέπει να σημειωθεί ότι, αν και το προτεινόμενο μοντέλο στοχεύει στον έλεγχο πρόσβασης σε κατανεμημένα περιβάλλοντα, εστιάζοντας στην αλληλεπίδραση μεταξύ συστημάτων, δε θα πρέπει να παραγνωριστεί ότι αποτελεί ένα μοντέλο ελέγχου πρόσβασης γενικού σκοπού και παρέχει τη δυνατότητα αποτίμησης αιτημάτων πρόσβασης που αφορούν μεμονωμένες ενέργειες[22] . Έτσι, λαμβάνοντας ένα αίτημα για την εκτέ-

[22]Εξάλλου, ο έλεγχος μεμονωμένων ενεργειών αποτελεί στάδιο της διαδικασίας επαλήθευσης ενός διμερούς συσχετισμού, στο πλαίσιο της εξαγωγής των αυτόνομα έγκυρων εργασιών (βλ. Ενότητα 7.4).

λεση μίας συγκεκριμένης ενέργειας, η Μηχανή Συμπερασμού είναι σε θέση να αποφανθεί για την εγκυρότητα της εν λόγω ενέργειας για κάποιο σκοπό, υποδεικνύοντας παράλληλα τις συνθήκες πλαισίου που θα πρέπει να ισχύουν και τις απαραίτητες και απαγορευμένες προ- και μετα- ενέργειες που την καθιστούν τελικά έγκυρη. Ακόμα και στην περίπτωση του ελέγχου μεμονωμένων ενεργειών, που εμφανίζει σημαντικά μικρότερη πολυπλοκότητα από τη διαδικασία επαλήθευσης ενός διμερούς συσχετισμού, είναι εμφανής η βελτίωση που επιτυγχάνεται μέσω της εκ των προτέρων εξαγωγής γνώσης που περιέχεται στους κανόνες με χρήση των κλάσεων `PermittedActions` και `OfflineRequiredActionStructures` της επέκτασης της οντολογίας του Μοντέλου Ελέγχου Πρόσβασης και Χρήσης, αντί για την εξαγωγή γνώσης απευθείας από τους κανόνες. Η διαφορά στους χρόνους απόκρισης με εξαγωγή γνώσης απευθείας από τους κανόνες και με εξαγωγή γνώσης από την επέκταση της οντολογίας οφείλεται στο γεγονός ότι στην πρώτη περίπτωση απαιτείται να αξιολογηθούν συνδυαστικά όλοι οι κανόνες (άδειες, απαγορεύσεις και υποχρεώσεις) που αφορούν την εκάστοτε ενέργεια πρόσβασης, δηλαδή όλοι οι κανόνες όπου η εν λόγω ενέργεια εμφανίζεται είτε σαν ενέργεια πρόσβασης είτε σαν προ-/μετα- ενέργεια, γνώση που υπάρχει εκ των προτέρων διαθέσιμη στη δεύτερη περίπτωση. Έτσι, παρατηρήθηκε βελτίωση της τάξης του ∼35% για ενέργειες οι οποίες ήταν συσχετισμένες μόνο με άδειες (δηλαδή, αποτελούσαν την ενέργεια πρόσβασης στους εκάστοτε κανόνες), ενώ σε πιο σύνθετες περιπτώσεις, όπου η εν λόγω ενέργεια συσχετίζεται και με απαγορεύσεις ή/και υποχρεώσεις και δεν αντανακλά μόνο την ενέργεια πρόσβασης, αναδεικνύονται τα σημαντικά πλεονεκτήματα που εισάγει η αμιγώς offline διαδικασία, με τη βελτίωση να φτάνει το ∼60% και το χρόνο απόκρισης να είναι σε κάθε περίπτωση μικρότερος του 1 sec.

# Κεφάλαιο 9

# Συμπεράσματα — Μελλοντική Εργασία

Η παρούσα διδακτορική διατριβή έχει σαν αντικείμενο την εφαρμογή μηχανισμών ελέγχου πρόσβασης και χρήσης σε κατανεμημένα περιβάλλοντα, με έμφαση στην προστασία της ιδιωτικότητας που αποτελεί και την πλέον πολύπλοκη περίπτωση χρήσης. Σε αυτό το πλαίσιο, προτείνεται ένα καινοτόμο μοντέλο ελέγχου πρόσβασης και χρήσης, βασισμένο στις ειδικές ανάγκες που δημιουργεί η λειτουργία των κατανεμημένων περιβαλλόντων και στις απαιτήσεις που απορρέουν από τη νομοθεσία για την προστασία της ιδιωτικότητας. Το εν λόγω μοντέλο, παρόλο που εστιάζει στην αποτίμηση της αλληλεπίδρασης μεταξύ συστημάτων, αποτελεί ένα μοντέλο ελέγχου πρόσβασης γενικού σκοπού, γεγονός που το καθιστά ιδανικό για ευρύ φάσμα περιπτώσεων χρήσης.

Η προτεινόμενη λύση βασίζεται σε δύο σημασιολογικά μοντέλα. Τη βάση του συστήματος συνιστά το Σημασιολογικό Μοντέλο Πληροφοριών που παρέχει αφαιρετική αναπαράσταση των βασικών οντοτήτων των κατανεμημένων συστημάτων, καθώς και τις μεταξύ τους συσχετίσεις, συμπεριλαμβανομένων εννοιών και σχεσιακών δομών που δεν έχουν εξετασθεί ακόμα ευρέως. Επιπλέον, θεμελιώνεται στη βάση των απαιτήσεων που προκύπτουν από την επεξεργασία των νομικών και κανονιστικών διατάξεων που αφορούν την προστασία των δεδομένων, γεγονός που αντικατοπτρίζεται από τις έννοιες που περιλαμβάνονται σε αυτό.

Το Σημασιολογικό Μοντέλο Πολιτικών χρησιμοποιείται για την προδιαγραφή κανόνων πάνω στις οντότητες του μοντέλου πληροφοριών. Οι κανόνες του χαρακτηρίζονται από υψηλό βαθμό εκφραστικότητας και, μέσω των καινοτόμων χαρακτηριστικών του, δύνανται να περιγράψουν περιορισμούς που τα υφιστάμενα μοντέλα αδυνατούν να ενσωματώσουν. Μεταξύ άλλων, το μοντέλο λαμβάνει υπόψη τις συνθήκες πλαισίου και τις ιδιότητες των εμπλεκόμενων οντοτήτων κατά τη λήψη αποφάσεων πρόσβασης και επιτρέπει τον προσδιορισμό κανόνων σε οποιοδήποτε επίπεδο αφαίρεσης, καθώς και σύνθετων εξαρτήσεων μεταξύ ενεργειών και οντοτήτων. Μία ακόμη συνεισφορά του προτεινόμενου μοντέ-

λου ελέγχου πρόσβασης έγκειται στα μέσα που προσφέρει για την προδιαγραφή προηγμένων περιορισμών διαχωρισμού και σύζευξης καθηκόντων. Βασική συνεισφορά της προτεινόμενης λύσης, όμως, αποτελεί το γεγονός ότι ο έλεγχος πρόσβασης δεν εστιάζει σε μεμονωμένες ενέργειες, αλλά η διαδικασία λήψης απόφασης για την παροχή πρόσβασης λαμβάνει υπόψη τόσο τη ροή λειτουργίας όσο και τη ροή δεδομένων στο πλαίσιο της αλληλεπίδρασης μεταξύ συστημάτων, με αποτέλεσμα μία ολιστική θεώρηση του ελέγχου πρόσβασης και ροή πληροφορίας με επίγνωση ιδιωτικότητας.

Και τα δύο μοντέλα υλοποιούνται από σημασιολογικές οντολογίες, λόγω της υψηλής πολυπλοκότητας και της εκφραστικότητας που παρουσιάζουν. Πράγματι, η χρήση οντολογιών επιτρέπει τον ορισμό πολύπλοκων δομών και κανόνων, ενώ παρουσιάζει διάφορα πλεονεκτήματα, όπως οι δυνατότητες εξαγωγής λογικών συμπερασμάτων, συμπεριλαμβανομένης γνώσης που δεν περιέχεται ρητά στην οντολογία, η δυνατότητα αξιολόγησης των κανόνων ως προς τη συνέπειά τους και η δυνατότητα ολοκλήρωσης με άλλα σημασιολογικά μοντέλα τα οποία περιγράφουν συμπληρωματικές έννοιες. Οι εν λόγω οντολογίες λοιπόν αποτελούν τη βάση για την εξαγωγή γνώσης από τα μοντέλα.

Η εξαγωγή γνώσης πραγματοποιείται σε δύο στάδια. Το πρώτο αφορά την εξαντλητική εξαγωγή γνώσης σε μη πραγματικό χρόνο και περιλαμβάνει την εξαγωγή μετακανόνων από τους ρητά ορισμένους κανόνες και την εξαγωγή γνώσης από το σύνολο των κανόνων, παρέχοντας τη δυνατότητα για αποτίμηση μεμονωμένων ενεργειών πρόσβασης. Το δεύτερο στάδιο, εκμεταλλευόμενο τα αποτελέσματα του πρώτου, αφορά τη σε πραγματικό χρόνο λήψη αποφάσεων αναφορικά με την αλληλεπίδραση μεταξύ των κατανεμημένων συστημάτων, τα επιτρεπτά σενάρια εκτέλεσης και την εξαγωγή συμπληρωματικών οδηγιών που πρέπει να ακολουθούνται. Με βάση την αξιολόγηση των σχετικών αλγόριθμων, οι πόροι που απαιτούνται σε όλα τα στάδια της διαδικασίας δεν κρίνονται υπερβολικοί, ενώ η επιλογή της εκ των προτέρων εξαγωγής γνώσης οδήγησε ούτως ή άλλως σε σημαντική βελτίωση της επίδοσης του συστήματος.

Η τρέχουσα και μελλοντική ερευνητική εργασία αφορά βελτιώσεις και επεκτάσεις του συστήματος και κινείται στους παρακάτω άξονες:

- *Επέκταση της προδιαγραφής χρονικών περιορισμών:* Αν και χρονικοί περιορισμοί και περιορισμοί αλληλουχίας λαμβάνονται ήδη υπόψη στους κανόνες ελέγχου πρόσβασης και χρήσης, όσον αφορά την εκτέλεση των προ-/μετα- ενεργειών σε σχέση με την ενέργεια πρόσβασης, ωστόσο υπάρχουν περιπτώσεις στις οποίες τέτοιου είδους περιορισμοί δεν επαρκούν. Αυτό οφείλεται κυρίως στο γεγονός ότι στην παρούσα μορφή του συστήματος κανόνες κάθε τύπου προδιαγράφονται με έναν ενιαίο τρόπο, ενώ, για παράδειγμα, συγκεκριμένα για τις υποχρεώσεις θα έπρεπε να προσδιορίζεται επιπλέον μέχρι πότε αυτές ισχύουν ή πότε παραβιάζονται, όπως προτείνεται στο [134].

- *Εκχώρηση εξουσιοδοτήσεων:* Εκτός από τις απευθείας εξουσιοδοτήσεις, υπάρχουν πε-

ριπτώσεις κατά τις οποίες μη εξουσιοδοτημένοι χρήστες χρειάζεται να αποκτήσουν πρόσβαση σε πόρους, όταν για παράδειγμα ένας εξουσιοδοτημένος χρήσης δεν είναι σε θέση να εκτελέσει κάποια ενέργεια. Σε αυτήν την περίπτωση, ο εξουσιοδοτημένος χρήστης μπορεί να εκχωρήσει το σύνολο −δηλαδή το ρόλο συνολικά− ή μέρος των δικαιωμάτων του σε κάποιο μη εξουσιοδοτημένο χρήστη ώστε ο τελευταίος να εκτελέσει κάποια εργασία για λογαριασμό του πρώτου, μέσω της διαδικασίας εκχώρησης εξουσιοδοτήσεων (Delegation of Authorisations), ενώ αυτά είτε θα ισχύουν επ'αόριστον είτε θα ανακαλούνται μετά το πέρας της συγκεκριμένης εργασίας. Συνεπώς, κρίνεται απαραίτητη η επέκταση του μηχανισμού διαχείρισης εξουσιοδοτήσεων, ο οποίος, εκτός από ορισμό, ανάθεση και ανάκληση δικαιωμάτων, θα περιλαμβάνει και εκχώρηση.

- *Αναπαράσταση ασαφούς γνώσης:* Καθώς υπάρχουν περιπτώσεις όπου η γνώση που αναπαρίσταται μέσω των εννοιών του Σημασιολογικού Μοντέλου Πληροφοριών και των μεταξύ τους συσχετίσεων είναι ασαφής, κρίνεται απαραίτητη η ενσωμάτωση της *Ασαφούς Λογικής* (*Fuzzy Logic*). Έτσι, ερευνάται η συμπλήρωση των συσχετίσεων που περιέχουν ασάφεια από ένα *βαθμό αληθείας* (*membership degree*), ώστε να επιτυγχάνεται ορθότερη και πληρέστερη εξαγωγή συμπερασμάτων.

- *Εφαρμογή των πολιτικών:* Ερευνητική προτεραιότητα αποτελεί ο συνδυασμός του προτεινόμενου μοντέλου με *Κρυπτογράφηση βάσει Ιδιοτήτων* (*Attribute-Based Encryption — ABE*) [135][136], προκειμένου να καταστεί δυνατή η αποτίμηση των δικαιωμάτων πρόσβασης με κρυπτογραφικά μέσα. Στο πλαίσιο αυτό, διερευνώνται οι μηχανισμοί για την εξαγωγή από το μοντέλο πολιτικών πρόσβασης υλοποιημένων σε ABE, με επέκταση του μηχανισμού εξαγωγής γνώσης σε μη πραγματικό χρόνο.

# Βιβλιογραφία


[1] D. Lewis, "What is web 2.0?," *Crossroads*, vol. 13, no. 1, pp. 3–3, 2006.

[2] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010.

[3] L. Camarinha-Matos, I. Silveri, H. Afsarmanesh, and A. Oliveira, "Towards a framework for creation of dynamic virtual organizations," in *Collaborative Networks and Their Breeding Environments* (L. Camarinha-Matos, H. Afsarmanesh, and A. Ortiz, eds.), vol. 186 of *IFIP - The International Federation for Information Processing*, pp. 69–80, Springer US, 2005.

[4] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, pp. 2787–2805, Oct. 2010.

[5] M. P. Papazoglou and W.-J. Heuvel, "Service oriented architectures: approaches, technologies and research issues," *The VLDB Journal*, vol. 16, pp. 389–415, July 2007.

[6] F. Curbera, M. Duftler, R. Khalaf, W. Nagy, N. Mukhi, and S. Weerawarana, "Unraveling the Web services web: an introduction to SOAP, WSDL, and UDDI," *Internet Computing, IEEE*, vol. 6, no. 2, pp. 86–93, 2002.

[7] S. Dustdar and W. Schreiner, "A Survey on Web Services Composition," *Int. J. Web Grid Serv.*, vol. 1, pp. 1–30, Aug. 2005.

[8] A. F. Westin, *Privacy and Freedom*. Atheneum, 1967.

[9] Ηνωμένα Έθνη, "Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα." `http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=grk`, Δεκέμβριος 1948.

[10] European Parliament, Council and Commission, "Charter of Fundamental Rights of the European Union," *Official Journal of the European Communities*, vol. C 364, pp. 1–22, December 2000.

[11] Organisation for Economic Co-operation and Development, "OECD guidelines on the protection of privacy and transborder flows of personal data." `http://dx.doi.org/10.1787/9789264196391-en`, 1980.

[12] European Parliament and Council, "Directive 95/46/EC of the European Parliament and of the Council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal of the European Communities*, vol. L 281, pp. 31–50, November 1995.

[13] European Parliament and Council, "Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," *Official Journal of the European Communities*, vol. L 201, pp. 37–47, July 2002.

[14] European Parliament and Council, "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," *Official Journal of the European Communities*, vol. L 105, pp. 54–63, April 2006.

[15] European Parliament and Council, "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws," *Official Journal of the European Communities*, vol. L 337, pp. 11–36, December 2009.

[16] Ευρωπαϊκή Επιτροπή, "Πρόταση: Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων)," Βρυξέλλες, Ιανουάριος 2012.

[17] Ζ' Αναθεωρητική Βουλή των Ελλήνων, "Το Σύνταγμα της Ελλάδας." `http://www.parliament.gr/politeuma/syntagma.pdf`, Απρίλιος 2001.

[18] Βουλή των Ελλήνων, "Νόμος 2472/1997: Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα," Απρίλιος 1997. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 50, Τεύχος Πρώτο.

[19] Βουλή των Ελλήνων, "Νόμος 3471/2006: Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Νόμου 2472/1997," Ιούνιος 2006. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 133, Τεύχος Πρώτο.

[20] Βουλή των Ελλήνων, "Νόμος 3115/2003: Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών," Φεβρουάριος 2003. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 47, Τεύχος Πρώτο.

[21] Βουλή των Ελλήνων, "Νόμος 3917/2011: Διατήρηση των δεδομένων που παράγονται ή υπόκεινται σε επεξεργασία στα πλαίσια της παροχής δημόσια διαθέσιμων υπηρεσιών ηλεκτρονικής επικοινωνίας ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επικοινωνιών με λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και σχετικές διατάξεις.," Φεβρουάριος 2011. Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 22.

[22] S. D. C. di Vimercati, S. Paraboschi, and P. Samarati, "Access Control: Principles and Solutions," *Softw. Pract. Exper.*, vol. 33, pp. 397–421, Apr. 2003.

[23] S. Capitani di Vimercati, P. Samarati, and S. Jajodia, "Policies, Models, and Languages for Access Control," in *Databases in Networked Information Systems* (S. Bhalla, ed.), vol. 3433 of *Lecture Notes in Computer Science*, pp. 225–237, Springer Berlin Heidelberg, 2005.

[24] S. De Capitani di Vimercati and P. Samarati, "Authorization specification and enforcement in federated database systems," *J. Comput. Secur.*, vol. 5, pp. 155–188, Mar. 1997.

[25] S. De Capitani di Vimercati, P. Samarati, and R. Sandhu, "Access Control," in *Computer Science Handbook (3rd edition) - Information Systems and Information Technology* (A. Tucker and H. Topi, eds.), Taylor and Francis Group, 2014. to appear.

[26] E. Bertino, S. Jajodia, and P. Samarati, "Database security: Research and practice," *Information Systems*, vol. 20, no. 7, pp. 537–556, 1995.

[27] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, pp. 38 –47, February 1996.

[28] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for Role-Based Access Control," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 224–274, 2001.

[29] J. Park and R. Sandhu, "The $\text{UCON}_{\text{ABC}}$ Usage Control Model," *ACM Trans. Inf. Syst. Secur.*, vol. 7, pp. 128–174, Feb. 2004.

[30] E. Yuan and J. Tong, "Attributed Based Access Control (ABAC) for Web Services," in *ICWS '05: Proceedings of the IEEE International Conference on Web Services*, 2005.

[31] C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "A Privacy-Aware Access Control System," *Journal of Computer Security*, vol. 16, pp. 369–392, September 2008.

[32] A. Abou-El-Kalam, R. E. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel, and G. Trouessin, "Organization Based Access Control," in *4th IEEE International Workshop on Policies for Distributed Systems and Networks (Policy'03)*, pp. 120–131, June 2003. Lake Come, Italy.

[33] F. Cuppens and N. Cuppens-Boulahia, "Modeling Contextual Security Policies," *International Journal of Information Security*, vol. 7, no. 4, pp. 285–305, 2008.

[34] S. Preda, F. Cuppens, N. Cuppens-Boulahia, J. Garcia-Alfaro, and L. Toutain, "Dynamic deployment of context-aware access control policies for constrained security devices," *Journal of Systems and Software*, vol. 84, pp. 1144–1159, July 2011.

[35] F. Cuppens, N. Cuppens, T. Sans, and A. Miège, "A formal approach to specify and deploy a network security policy," in *Second Workshop on Formal Aspects in Security and Trust*, (Toulouse, France), pp. 203–218, August 2004.

[36] C. Coma, N. Cuppens-Boulahia, F. Cuppens, and A. R. Cavalli, "Context Ontology for Secure Interoperability," in *3rd International Conference on Availability, Reliability and Security (ARES'08)*, pp. 821–827, IEEE, 2008.

[37] F. Cuppens, N. Cuppens-Boulahia, and B. Ben-Ghorbel, "High-level conflict management strategies in advanced access control models," *Electronic Notes in Theoretical Computer Science*, vol. 186, pp. 3–26, 2007. 2007.

[38] F. Cuppens, N. Cuppens-Boulahia, and A. Miége, "Inheritance hierarchies in the Or-BAC Model and application in a network environment," in *2nd Foundations of Computer Security Workshop (FCS'04)*, 2004. Turku, Finlande.

[39] N. Ajam, N. Cuppens-Boulahia, and F. Cuppens, "Contextual Privacy Management in Extended Role Based Access Control Model," in *Data Privacy Management and Autonomous Spontaneous Security* (J. Garcia-Alfaro, G. Navarro-Arribas, N. Cuppens-Boulahia, and Y. Roudier, eds.), vol. 5939 of *Lecture Notes in Computer Science*, pp. 121–135, Springer, 2010.

[40] Organization for the Advancement of Structured Information Standards (OASIS), "eXtensible Access Control Markup Language (XACML) Version 2.0." `http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf`, February 2005. OASIS Standard.

[41] Organization for the Advancement of Structured Information Standards (OASIS), "Privacy policy profile of XACML v2.0." `http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-privacy_profile-spec-os.pdf`, February 2005. OASIS Standard.

[42] Organization for the Advancement of Structured Information Standards (OASIS), "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0." `http://www.oasis-open.org/committees/document.php?document_id=34164&wg_abbrev=xacml`, August 2009. Committee Specification.

[43] M. Casassa Mont, "Dealing with Privacy Obligations: Important Aspects and Technical Approaches," in *Trust and Privacy in Digital Business* (S. Katsikas, J. Lopez, and G. Pernul, eds.), vol. 3184 of *Lecture Notes in Computer Science*, pp. 120–131, Springer Berlin / Heidelberg, 2004.

[44] A. Antonakopoulou, G. V. Lioudakis, F. Gogoulos, D. I. Kaklamani, and I. S. Venieris, "Leveraging Access Control for Privacy Protection: A Survey," in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (G. Yee, ed.), pp. 65–94, IGI Global, 2012.

[45] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy-Aware Access Control," in *Encyclopedia of Information Science and Technology* (M. Khosrow-Pour, ed.), IGI Global, 2014. (under review).

[46] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Hippocratic databases," in *VLDB '02: Proceedings of the 28th international conference on Very Large Data Bases*, pp. 143–154, VLDB Endowment, 2002.

[47] K. LeFevre, R. Agrawal, V. Ercegovac, R. Ramakrishnan, Y. Xu, and D. DeWitt, "Limiting disclosure in hippocratic databases," in *VLDB '04: Proceedings of the 30th international conference on Very Large Data Bases*, pp. 108–119, VLDB Endowment, 2004.

[48] F. Massacci, J. Mylopoulos, and N. Zannone, "Hierarchical hippocratic databases with minimal disclosure for virtual organizations," *The VLDB Journal*, vol. 15, pp. 370–387, November 2006.

[49] J.-W. Byun, E. Bertino, and N. Li, "Purpose Based Access Control for Privacy Protection in Relational Database Systems," Tech. Rep. TR 2004-52, CERIAS, Purdue University, 2004.

[50] J.-W. Byun, E. Bertino, and N. Li, "Purpose based access control of complex data for privacy protection," in *SACMAT '05: Proceedings of the 10th ACM symposium on Access Control Models And Technologies*, pp. 102–110, ACM, 2005.

[51] J.-W. Byun and N. Li, "Purpose Based Access Control for Privacy Protection in Relational Database Systems," *The VLDB Journal*, vol. 17, no. 4, pp. 603–619, 2008.

[52] Q. Ni, E. Bertino, and J. Lobo, "An obligation model bridging access control policies and privacy policies," in *SACMAT '08: Proceedings of the 13th ACM Symposium on Access Control Models And Technologies*, (New York, NY, USA), pp. 133–142, ACM, 2008.

[53] Q. Ni, E. Bertino, J. Lobo, C. Brodie, C.-M. Karat, J. Karat, and A. Trombetta, "Privacy-aware Role-based Access Control," *ACM Transactions on Information and System Security*, vol. 13, no. 3, pp. 1–31, 2010.

[54] Q. Ni, E. Bertino, J. Lobo, and S. Calo, "Privacy-Aware Role-Based Access Control," *IEEE Security Privacy*, vol. 7, pp. 35 –43, July 2009.

[55] Q. Ni, D. Lin, E. Bertino, and J. Lobo, "Conditional Privacy-Aware Role Based Access Control," in *ESORICS 2007: Proceedings of the 12th European Symposium On Research In Computer Security*, pp. 72–89, Springer, 2007.

[56] A. Masoumzadeh and J. Joshi, "PuRBAC: Purpose-Aware Role-Based Access Control," in *On the Move to Meaningful Internet Systems: OTM 2008* (R. Meersman and Z. Tari, eds.), vol. 5332 of *Lecture Notes in Computer Science*, pp. 1104–1121, Springer Berlin / Heidelberg, 2008.

[57] C. A. Ardagna, J. Camenisch, M. Kohlweiss, R. Leenes, G. Neven, B. Priem, P. Samarati, D. Sommer, and M. Verdicchio, "Exploiting cryptography for privacy-enhanced access control: A result of the PRIME Project," *Journal of Computer Security*, vol. 18, no. 1, pp. 123–160, 2010.

[58] P. A. Bonatti and P. Samarati, "A uniform framework for regulating service access and information release on the web," *Journal of Computer Security*, vol. 10, pp. 241–271, September 2002.

[59] G. Karjoth, M. Schunter, and M. Waidner, "Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data," in *PET 2002: Proceedings of of the 2nd International Workshop on Privacy Enhancing Technologies* (R. Dingledine and P. Syverson, eds.), vol. 2482 of *Lecture Notes in Computer Science*, pp. 69–84, Springer Berlin / Heidelberg, 2003.

[60] F. Gogoulos, A. Antonakopoulou, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "Privacy-Aware Access Control and Authorization in Passive Network Monitoring Infrastructures," in *CIT 2010: Proceedings of the 10th IEEE International Conference on Computer and Information Technology*, pp. 1114–1121, IEEE Computer Society, 2010.

[61] G. V. Lioudakis, F. Gogoulos, A. Antonakopoulou, A. S. Mousas, I. S. Venieris, and D. I. Kaklamani, "An access control approach for privacy-preserving passive network monitoring," in *ICITST 2009: Proceedings of the 4th International Conference for Internet Technology and Secured Transactions*, November 2009.

[62] International Telecommunication Union (ITU) – Telecommunication Standardization Sector, "Information technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks," August 2005. ITU-T Recommendation X.509.

[63] The World Wide Web Consortium (W3C), "OWL Web Ontology Language Overview." `http://www.w3.org/TR/owl-features/`, February 2004. W3C Recommendation.

[64] A. Antonakopoulou, F. Gogoulos, G. V. Lioudakis, A. S. Mousas, D. I. Kaklamani, and I. S. Venieris, "Semantic Information Model for Privacy-Aware Access Control," in *PCI 2010: Proceedings of the 14th Panhellenic Conference on Informatics*, (Los Alamitos, CA, USA), pp. 130–134, IEEE Computer Society, 2010.

[65] G. V. Lioudakis, F. Gogoulos, A. Antonakopoulou, D. I. Kaklamani, and I. S. Venieris, "Privacy Protection in Passive Network Monitoring: An Access Control Approach," in *WAINA 2009: Proceedings of the 2009 International Conference on Advanced Information Networking and Applications Workshops*, pp. 109–116, IEEE Computer Society, 2009.

[66] S. Ayed, N. Cuppens-Boulahia, and F. Cuppens, "Deploying Security Policy in Intra and Inter Workflow Management Systems," *Reliability and Security, International Conference on Availability*, pp. 58–65, 2009.

[67] G. Russello, C. Dong, and N. Dulay, "A Workflow-Based Access Control Framework for e-Health Applications," in *WAINA 2008: Proceedings of the 22nd International Conference on Advanced Information Networking and Applications Workshops*, (Washington, DC, USA), pp. 111–120, IEEE Computer Society, 2008.

[68] M. Alam, M. Hafner, and R. Breu, "Constraint based role based access control in the SECTET-framework A model-driven approach," *Journal of Computer Security*, vol. 16, no. 2, pp. 223–260, 2008.

[69] M. Menzel and C. Meinel, "SecureSOA Modelling Security Requirements for Service-Oriented Architectures," in *Services Computing (SCC), 2010 IEEE International Conference on*, pp. 146–153, 2010.

[70] P. Samarati and S. D. C. di Vimercati, "Access Control: Policies, Models, and Mechanisms," in *FOSAD 2000: Foundations of Security Analysis and Design*, vol. 2171 of *Lecture Notes in Computer Science*, (Berlin, Heidelberg), pp. 137–196, Springer, 2001.

[71] G. Tonti, J. Bradshaw, R. Jeffers, R. Montanari, N. Suri, and A. Uszok, "Semantic Web Languages for Policy Representation and Reasoning: A Comparison of KAoS, Rei, and Ponder," in *The SemanticWeb - ISWC 2003*, vol. 2870 of *Lecture Notes in Computer Science*, pp. 419–437, Springer Berlin / Heidelberg, 2003.

[72] P. Mitra, C.-C. Pan, P. Liu, and V. Atluri, "Privacy-preserving semantic interoperation and access control of heterogeneous databases," in *ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, pp. 66–77, ACM, 2006.

[73] C.-C. Pan, P. Mitra, and P. Liu, "Semantic access control for information interoperation," in *SACMAT '06: Proceedings of the 11th ACM Symposium on Access Control Models And Technologies*, (New York, NY, USA), pp. 237–246, ACM, 2006.

[74] Y. Sun, P. Pan, H.-f. Leung, and B. Shi, "Ontology Based Hybrid Access Control for Automatic Interoperation," in *Autonomic and Trusted Computing* (B. Xiao, L. Yang, J. Ma, C. Muller-Schloer, and Y. Hua, eds.), vol. 4610 of *Lecture Notes in Computer Science*, pp. 323–332, Springer Berlin / Heidelberg, 2007.

[75] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Leveraging Semantic Web Technologies for Access Control," in *Emerging Trends in Information and Communication Technologies Security* (B. Akhgar and H. Arabnia, eds.), pp. 493–506, Morgan Kaufmann, 2014.

[76] T. W. Finin, A. Joshi, L. Kagal, J. Niu, R. S. Sandhu, W. H. Winsborough, and B. M. Thuraisingham, "R*OWL*BAC: representing role based access control in *OWL*," in *SACMAT '08: Proceedings of the 13th ACM Symposium on Access Control Models And Technologies*, pp. 73–82, ACM, 2008.

[77] R. Ferrini and E. Bertino, "Supporting RBAC with xacml+OWL," in *SACMAT '09: Proceedings of the 14th ACM Symposium on Access Control Models And Technologies*, pp. 145–154, ACM, 2009.

[78] Z. He, K. Huang, L. Wu, H. Li, and H. Lai, "Using Semantic Web Techniques to Implement Access Control for Web Service," in *Information Computing and Applications* (R. Zhu, Y. Zhang, B. Liu, and C. Liu, eds.), vol. 105 of *Communications in Computer and Information Science*, pp. 258–266, Springer Berlin Heidelberg, 2011.

[79] B. Parsia, E. Sirin, B. C. Grau, E. Ruckhaus, and D. Hewlett, "Cautiously Approaching SWRL," tech. rep., University of Maryland, 2005.

[80] L. Cirio, I. Cruz, and R. Tamassia, "A Role and Attribute Based Access Control System Using Semantic Web Technologies," in *On the Move to Meaningful Internet Systems 2007: OTM 2007 Workshops* (R. Meersman, Z. Tari, and P. Herrero, eds.), vol. 4806 of *Lecture Notes in Computer Science*, pp. 1256–1266, Springer Berlin / Heidelberg, 2007.

[81] I. F. Cruz, R. Gjomemo, B. Lin, and M. Orsini, "A Constraint and Attribute Based Security Framework for Dynamic Role Assignment in Collaborative Environments," in *CollaborateCom 2008: Collaborative Computing: Networking, Applications and Worksharing* (E. Bertino and J. B. D. Joshi, eds.), vol. 10 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 322–339, Springer, 2008.

[82] The World Wide Web Consortium (W3C), "SPARQL Query Language for RDF." `http://www.w3.org/TR/rdf-sparql-query/`, January 2008. W3C Recommendation.

[83] T. Priebe, W. Dobmeier, and N. Kamprath, "Supporting Attribute-based Access Control with Ontologies," in *ARES 2006: Proceedings of the The First International Conference on Availability, Reliability and Security*, pp. 465–472, IEEE Computer Society, 2006.

[84] I. Ching Hsu, "Extensible access control markup language integrated with Semantic Web technologies," *Information Sciences*, vol. 238, no. 0, pp. 33 – 51, 2013.

[85] A. Rota, S. Short, and M. A. Rahaman, "XML secure views using semantic access control," in *Proceedings of the 2010 EDBT/ICDT Workshops*, EDBT '10, (New York, NY, USA), pp. 5:1–5:10, ACM, 2010.

[86] D. Abi Haidar, N. Cuppens-Boulahia, F. Cuppens, and H. Debar, "An extended RBAC profile of XACML," in *Proceedings of the 3rd ACM workshop on Secure web services*, SWS '06, (New York, NY, USA), pp. 13–22, ACM, 2006.

[87] A. Ravari, M. Amini, R. Jalili, and J. Jafarian, "A history based semantic aware access control model using logical time," in *Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on*, pp. 43–50, December 2008.

[88] S. Javanmardi, M. Amini, and R. Jalili, "An Access Control Model for Protecting Semantic Web Resources," in *Web policy workshop*, pp. 32–46, 2006.

[89] S. Javanmardi, A. Amini, R. Jalili, and Y. Ganjisafar, "SBAC: "A Semantic-Based Access Control Model"," in *NORDSEC-2006*, 2006.

[90] A. Ravari, J. Jafarian, M. Amini, and R. Jalili, "GTHBAC: A Generalized Temporal History Based Access Control Model," *Telecommunication Systems*, vol. 45, pp. 111–125, 2010.

[91] H. Debar, D. Curry, and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)." RFC 4765 (Experimental), Mar. 2007.

[92] N. Cuppens-Boulahia, F. Cuppens, F. Autrel, and H. Debar, "An ontology-based approach to react to network attacks," *International Journal of Information and Computer Security*, vol. 3, no. 3, pp. 280–305, 2009.

[93] A. Antonakopoulou, F. I. Gogoulos, G. V. Lioudakis, A. Mousas, D. I. Kaklamani, and I. S. Venieris, "An Ontology for Privacy-aware Access Control in Network Monitoring Environments," *Journal of Research and Practice in Information Technology*, 2013. (to appear).

[94] G. V. Lioudakis, G. Tropea, I. S. Venieris, D. I. Kaklamani, and N. Blefari-Melazzi, "Combining monitoring and privacy-protection perspectives in a semantic model for ip traffic measurements," in *Computer and Information Sciences: Proceedings of the 25th International Symposium on Computer and Information Sciences* (E. Gelenbe, R. Lent, G. Sakellari, A. Sacan, H. Toroslu, and A. Yazici, eds.), vol. 62 of *Lecture Notes in Electrical Engineering*, pp. 187–190, Springer Netherlands, 2010.

[95] G. Tropea, G. V. Lioudakis, N. Blefari-Melazzi, D. I. Kaklamani, and I. S. Venieris, "Introducing Privacy-Awareness in Network Monitoring Ontologies," in *Trustworthy Internet* (N. B.-M. L. Salgarelli, G. Bianchi, ed.), pp. 317–331, Springer Verlag, 2011.

[96] The World Wide Web Consortium (W3C), "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification." `http://www.w3.org/TR/P3P11/`, November 2006.

[97] The World Wide Web Consortium (W3C), "A P3P Preference Exchange Language 1.0 (APPEL1.0)." `http://www.w3.org/TR/2002/WD-P3P-preferences-20020415`, April 2002.

[98] P. Bodorik, D. Jutla, and M. X. Wang, "Consistent privacy preferences (CPP): model, semantics, and properties," in *SAC 2008: Proceedings of the 2008 ACM Symposium on Applied Computing*, pp. 2368–2375, ACM, 2008.

[99] O. Sacco, A. Passant, and S. Decker, "An Access Control Framework for the Web of Data," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pp. 456–463, 2011.

[100] Y.-J. Hu, H.-Y. Guo, and Guang-DeLin, "Semantic Enforcement of Privacy Protection Policies via the Combination of Ontologies and Rules," in *Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC '08. IEEE International Conference on*, pp. 400–407, June 2008.

[101] C. Ardagna, E. Damiani, S. De Capitani di Vimercati, C. Fugazza, and P. Samarati, "Offline Expansion of XACML Policies Based on P3P Metadata," in *Web Engineering* (D. Lowe and M. Gaedke, eds.), vol. 3579 of *Lecture Notes in Computer Science*, pp. 363–374, Springer Berlin / Heidelberg, 2005.

[102] F. Giunchiglia, R. Zhang, and B. Crispo, "Ontology driven community access control," in *In SPOT2009 - Trust and Privacy on the Social and Semantic Web*, 2009.

[103] N. Elahi, M. Chowdhury, and J. Noll, "Semantic Access Control in Web Based Communities," in *ICCGI 2008: Proceedings of the Third International Multi-Conference on Computing in the Global Information Technology*, pp. 131–136, IEEE Computer Society, August 2008.

[104] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "A semantic web based framework for social network access control," in *SACMAT '09: Proceedings of the 14th ACM Symposium on Access Control Models And Technologies*, pp. 177–186, ACM, 2009.

[105] A. Masoumzadeh and J. Joshi, "OSNAC: An Ontology-based Access Control Model for Social Networking Systems," in *Proceedings of the 2010 IEEE Second International Conference on Social Computing*, SOCIALCOM '10, (Washington, DC, USA), pp. 751–759, IEEE Computer Society, 2010.

[106] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, and S. Waldbusser, "Terminology for Policy-Based Management." RFC 3198 (Informational), November 2001.

[107] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "An Ontology-Based Approach towards Comprehensive Workflow Modelling," *IET Software*, 2013. (to appear).

[108] D. J. Solove, "A Brief History of Information Privacy Law," in *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age* (C. Wolf, ed.), ch. 1, pp. 1–46, New York, NY, USA: Practising Law Institute, 2006.

[109] S. Gutwirth, P. De Hert, and Y. Poullet, *Reinventing Data Protection?* Berlin: Springer, 2009.

[110] S. Gutwirth, P. De Hert, and Y. Poullet, *European Data Protection: Coming of Age*. Berlin: Springer, 2013.

[111] G. V. Lioudakis, F. Gaudino, E. Boschi, G. Bianchi, D. I. Kaklamani, and I. S. Venieris, "Legislation-Aware Privacy Protection in Passive Network Monitoring," in *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues* (I. M. Portela and M. M. Cruz-Cunha, eds.), ch. 22, pp. 363–383, IGI Global, 2010.

[112] J. B. D. Joshi, B. Shafiq, A. Ghafoor, and E. Bertino, "Dependencies and separation of duty constraints in GTRBAC," in *Proceedings of the 8th ACM Symposium on Access Control Models And Technologies*, SACMAT '03, (New York, NY, USA), pp. 51–64, ACM, 2003.

[113] M. Hilty, D. Basin, and A. Pretschner, "On obligations," in *Proceedings of the 10th European Symposium On Research In Computer Security*, ESORICS'05, (Berlin, Heidelberg), pp. 98–117, Springer-Verlag, 2005.

[114] G. M. Kapitsaki, G. V. Lioudakis, D. I. Kaklamani, and I. S. Venieris, "Privacy Protection in Context-Aware Web Services: Challenges and Solutions," in *Enabling Context-Aware Web Services: Methods, Architectures, and Technologies* (S. D. Quan Z. Sheng, Jian Yu, ed.), pp. 393–420, Chapman and Hall/CRC, 2010.

[115] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, J. Garcia-Alfaro, D. I. Kaklamani, and I. S. Venieris, "A Contextual Privacy-Aware Access Control Model for Network Monitoring Workflows: Work in Progress," in *Proceedings of the 4th MITACS Workshop on Foundations & Practice of Security (FPS 2011)* (J. Garcia-Alfaro and P. Lafourcade, eds.), vol. 6888 of *Lecture Notes in Computer Science*, pp. 208–217, Springer Berlin / Heidelberg, 2012.

[116] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, J. Garcia-Alfaro, D. I. Kaklamani, I. S. Venieris, F. Cuppens, and N. Cuppens-Boulahia, "A Privacy-Aware Access Control Model for Distributed Network Monitoring," *Computers & Electrical Engineering*, vol. 39, pp. 2263–2281, October 2013.

[117] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, "Handbook for computer security incident response teams (CSIRTs)," Tech. Rep. CMU/SEI-2003-HB-002, Carnegie Mellon University, Software Engineering Institute, 2003.

[118] M. Adams, A. ter Hofstede, D. Edmond, and W. van der Aalst, "Worklets: A Service-Oriented Implementation of Dynamic Flexibility in Workflows," in *On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE* (R. Meersman and Z. Tari, eds.), vol. 4275 of *Lecture Notes in Computer Science*, pp. 291–308, Springer Berlin / Heidelberg, 2006.

[119] C. Ardagna, S. De Capitani di Vimercati, and P. Samarati, "Privacy Models and Languages: Access Control and Data Handling Policies," in *Digital Privacy* (J. Camenisch, R. Leenes, and D. Sommer, eds.), vol. 6545 of *Lecture Notes in Computer Science*, pp. 309–329, Springer Berlin / Heidelberg, 2011.

[120] F. Cuppens, N. Cuppens-Boulahia, and C. Coma, "O2O: Virtual Private Organizations to Manage Security Policy Interoperability," in *Information Systems Security* (A. Bagchi and V. Atluri, eds.), vol. 4332 of *Lecture Notes in Computer Science*, pp. 101–115, Springer Berlin / Heidelberg, 2006.

[121] N. Russell, A. H. M. Ter Hofstede, W. M. van der Aalst, and N. Mulyar, "Workflow Control-Flow Patterns: A Revised View," Tech. Rep. BPM-06-22, BPM Center, 2006.

[122] R. A. Botha and J. H. P. Eloff, "Separation of duties for access control enforcement in workflow environments," *IBM Systems Journal*, vol. 40, no. 3, pp. 666–682, 2001.

[123] R. Simon and M. E. Zurko, "Separation of Duty in Role-based Environments," in *CSFW '97: Proceedings of the 10th IEEE workshop on Computer Security Foundations*, (Washington, DC, USA), IEEE Computer Society, 1997.

[124] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, J. Garcia-Alfaro, D. I. Kaklamani, I. S. Venieris, N. Cuppens-Boulahia, and F. Cuppens, "Leveraging Ontologies upon a Holistic Privacy-aware Access Control Model," in *Proceedings of the 6th International Symposium on Foundations & Practice of Security (FPS 2013)*, vol. 8352 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 2013. (in press).

[125] Data Protection Commissioner of Ireland, "Data Protection Guidelines on research in the Health Sector," 2007.

[126] J. F. Allen, "Towards a General Theory of Action and Time," *Artif. Intell.*, vol. 23, pp. 123–154, July 1984.

[127] A. Cavoukian, *Privacy by Design*. `http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf`, 2009.

[128] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, D. I. Kaklamani, and I. S. Venieris, "A Workflow Checking Approach for Inherent Privacy Awareness in Network Monitoring," in *Proceedings of the 6th International Workshop on Data Privacy Management (DPM 2011)* (J. Garcia-Alfaro, G. Navarro-Arribas, N. Cuppens-Boulahia, and S. De Capitani di Vimercati, eds.), vol. 7122 of *Lecture Notes in Computer Science*, pp. 295–302, Springer Berlin / Heidelberg, 2012.

[129] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy-Aware Workflows: Challenges and Requirements," in *Proceedings of the 1st International Conference on Information and Communication Technologies and Law (ICT LAW 2013)* (I. Portela, P. Gonçalves, M. M. Cruz Cunha, and V. Carvalho, eds.), Cambridge Scholars, 2013.

[130] M. N. Κουκοβίνη, "Εγγενής Ενσωμάτωση Ιδιωτικότητας σε Τεχνολογίες Λογισμικού Προσανατολισμένου σε Υπηρεσίες." Διδακτορική Διατριβή, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Εθνικό Μετσόβιο Πολυτεχνείο, 2013.

[131] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy Compliance Requirements in Workflow Environments," in *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (M. M. Cruz Cunha, ed.), IGI Global, 2014.

[132] M. Ehrig, *Ontology alignment: bridging the semantic gap*, vol. 4. Springer, 2007.

[133] N. Choi, I.-Y. Song, and H. Han, "A survey on ontology mapping," *ACM Sigmod Record*, vol. 35, no. 3, pp. 34–41, 2006.

[134] Y. Elrakaiby, F. Cuppens, and N. Cuppens-Boulahia, "Formal enforcement and management of obligation policies," *Data Knowl. Eng.*, vol. 71, no. 1, pp. 127–147, 2012.

[135] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, SP '07, (Washington, DC, USA), pp. 321–334, IEEE Computer Society, 2007.

[136] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT'05, (Berlin, Heidelberg), pp. 457–473, Springer-Verlag, 2005.

# Δημοσιεύσεις

## Διεθνή Επιστημονικά Περιοδικά

[1] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, J. Garcia-Alfaro, D. I. Kaklamani, I. S. Venieris, F. Cuppens, and N. Cuppens-Boulahia, "A Privacy-Aware Access Control Model for Distributed Network Monitoring," *Computers & Electrical Engineering*, vol. 39(7), pp. 2263–2281, October 2013.

[2] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "An Ontology-Based Approach towards Comprehensive Workflow Modelling," *IET Software*, 2013. (to appear).

## Κεφάλαια Βιβλίων

[1] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy Compliance Requirements in Workflow Environments," in *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (M. M. Cruz Cunha, ed.), IGI Global, 2014.

[2] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Leveraging Semantic Web Technologies for Access Control," in *Emerging Trends in Information and Communication Technologies Security* (B. Akhgar and H. Arabnia, eds.), pp. 493–506, Morgan Kaufmann, 2014.

## Πρακτικά Διεθνών Επιστημονικών Συνεδρίων

[1] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, J. Garcia-Alfaro, D. I. Kaklamani, I. S. Venieris, N. Cuppens-Boulahia, and F. Cuppens, "Leveraging Ontologies upon a Holistic Privacy-aware Access Control Model," in *Proceedings of the 6th International Symposium on Foundations & Practice of Security (FPS 2013)*, vol. 8352 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 2013. (in press).

[2] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy-Aware Workflows: Challenges and Requirements," in *Proceedings of the 1st International Conference on Information and Communication Technologies and Law (ICT LAW 2013)* (I. Portela, P. Gonçalves, M. M. Cruz Cunha, and V. Carvalho, eds.), Cambridge Scholars, 2013.

[3] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, D. I. Kaklamani, and I. S. Venieris, "A Workflow Checking Approach for Inherent Privacy Awareness in Network Monitoring," in *Proceedings of the 6th International Workshop on Data Privacy Management (DPM 2011)* (J. Garcia-Alfaro, G. Navarro-Arribas, N. Cuppens-Boulahia, and S. De Capitani di Vimercati, eds.), vol. 7122 of *Lecture Notes in Computer Science*, pp. 295–302, Springer Berlin / Heidelberg, 2012.

[4] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, J. Garcia-Alfaro, D. I. Kaklamani, and I. S. Venieris, "A Contextual Privacy-Aware Access Control Model for Network Monitoring Workflows: Work in Progress," in *Proceedings of the 4th MITACS Workshop on Foundations & Practice of Security (FPS 2011)* (J. Garcia-Alfaro and P. Lafourcade, eds.), vol. 6888 of *Lecture Notes in Computer Science*, pp. 208–217, Springer Berlin / Heidelberg, 2012.

[5] S. Rao, G. Bianchi, J. Garcia-Alfaro, F. Romero, B. Trammell, A. Berger, G. V. Lioudakis, E. I. Papagianakopoulou, M. N. Koukovini, and K. Mittig, "System Architecture for Collaborative Security and Privacy Monitoring in Multi-Domain Networks," in *Proceedings of the 3rd IEEE Workshop on Collaborative Security Technologies (CoSec 2011)*, IEEE Press, 2011.

## Δημοσιεύσεις υπό Κρίση

[1] E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Privacy-Aware Access Control," in *Encyclopedia of Information Science and Technology* (M. Khosrow-Pour, ed.), IGI Global, 2014. (under review).

[2] M. N. Koukovini, E. I. Papagiannakopoulou, G. V. Lioudakis, N. M. Dellas, D. I. Kaklamani, and I. S. Venieris, "Workflow Modeling Technologies," in *Encyclopedia of Information Science and Technology* (M. Khosrow-Pour, ed.), IGI Global, 2014. (under review).

# Συνοπτικό Βιογραφικό Σημείωμα

Η κ. Ευγενία Ι. Παπαγιαννακοπούλου γεννήθηκε στην Αθήνα το 1983. Αποφοίτησε από το 5ο Λύκειο Βύρωνα το 2001, με βαθμό "Άριστα. Το ίδιο έτος εισήχθη στη Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του ΕΜΠ, απ' όπου και αποφοίτησε το 2007 με γενικό βαθμό "Λίαν καλώς" (8,10/10). Το 2008 έγινε δεκτή ως υποψήφια διδάκτορας της ίδιας σχολής. Κατά τη διάρκεια της εκπόνησης της διδακτορικής της διατριβής είχε ενεργή συμμετοχή σε ευρωπαϊκά ερευνητικά προγράμματα, ιδιαιτέρως δε στο FP7 ICT DEMONS, το αντικείμενο του οποίου ήταν συναφές με αυτό της διατριβής. Στο πλαίσιο της ερευνητικής της εργασίας μελέτησε, σχεδίασε και ανέπτυξε πρωτότυπο μοντέλο ελέγχου πρόσβασης και χρήσης σε κατανεμημένα συστήματα, με στόχο την προστασία των υποκείμενων πόρων, δίνοντας ιδιαίτερο βάρος στην προστασία προσωπικών δεδομένων και τη διασφάλιση της ιδιωτικότητας.

Η κ. Παπαγιαννακοπούλου, κατά τη διάρκεια των μεταπτυχιακών της σπουδών, έλαβε μέρος σε διεθνή συνέδρια, στα οποία παρουσίασε το ερευνητικό της έργο και δημοσίευσε τις εργασίες της στα πρακτικά τους. Παράλληλα, έχει δημοσιεύσει εργασίες της σε συλλογικούς τόμους, καθώς και στα διεθνώς αναγνωρισμένα επιστημονικά περιοδικά *Computer & Electrical Engineering* (Elsevier) και *Software* (IET). Επιπλέον, έχει συνεισφέρει στις δραστηριότητες προτυποποίησης του οργανισμού European Telecommunications Standards Institute (ETSI), μέσω της συμμετοχής της στις ομάδες εργασίας Measurement Ontology for IP traffic (MOI) και Identity and access management for Networks and Services (INS).

Η κ. Παπαγιαννακοπούλου έχει εργασθεί στον ιδιωτικό τομέα ως Μηχανικός Λογισμικού, συμμετέχοντας σε πληθώρα αναπτυξιακών έργων, και είναι μέλος του Τεχνικού Επιμελητηρίου Ελλάδος (Τ.Ε.Ε.).