

Ατομική Διπλωματική Εργασία

**ΕΠΕΚΤΑΣΗ ΤΥΠΙΚΗΣ ΓΛΩΣΣΑΣ ΜΟΤΕΛΟΠΟΙΗΣΗΣ
ΣΥΣΤΗΜΑΤΩΝ ΜΕ ΡΟΛΟΥΣ ΚΑΙ ΔΥΝΑΜΙΚΟΥΣ
ΠΕΡΙΟΡΙΣΜΟΥΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ**

Άντρια Παπαδημητρίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2013

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΠΕΚΤΑΣΗ ΤΥΠΙΚΗΣ ΓΛΩΣΣΑΣ ΜΟΤΕΛΟΠΟΙΗΣΗΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕ ΡΟΛΟΥΣ ΚΑΙ ΔΥΝΑΜΙΚΟΥΣ ΠΕΡΙΟΡΙΣΜΟΥΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Άντρια Παπαδημητρίου

Επιβλέπουσα Καθηγήτρια

Άννα Φιλίππου

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των
απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του
Πανεπιστημίου Κύπρου

Μάιος 2013

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτή μου κ. Άννα Φιλίππου, για την υποστήριξη και καθοδήγηση που μου προσέφερε κατά την διάρκεια έρευνας και υλοποίησης της παρούσας εργασίας, καθώς και για την επίτευξη μιας άψογης συνεργασίας. Επίσης, να την ευχαριστήσω για την κατανόηση και την βοήθεια στα όποια προβλήματα προέκυψαν στη πορεία.

Εν τέλη, θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου, για τη στήριξη που μου έδιναν κατά τη διάρκεια εκπόνησης της πτυχιακής μου εργασίας, αλλά και καθ' όλη τη διάρκεια των σπουδών μου στο Πανεπιστήμιο Κύπρου.

Ευχαριστώ

Άντρια Παπαδημητρίου

Περίληψη

Η ραγδαία ανάπτυξη της τεχνολογίας απειλεί καθημερινά την ασφάλεια της ιδιωτικής ζωής του κάθε ατόμου. Η διαφύλαξη των προσωπικών όσο και των επαγγελματικών πληροφοριών είναι απαραίτητη γι' αυτό και οι νομοθέτες και οι κυβερνήσεις κάνουν προσπάθειες για σύνταξη και επιβολή αυστηρών κανονισμών. Ταυτόχρονα υπάρχει η ανάγκη για εξεύρεση μηχανισμών που προέρχονται από την ίδια την τεχνολογία για τη διασφάλιση του προσωπικού χώρου και της ιδιωτικότητας του ατόμου.

Στη διπλωματική εργασία αυτή μελετήθηκε η έννοια της ιδιωτικότητας και πώς απαιτήσεις που σχετίζονται με ιδιωτικότητα μπορούν να διατυπωθούν και να αναπτυχθούν χρησιμοποιώντας το πρότυπο των αλγεβρών διεργασιών. Οι άλγεβρες διεργασιών χρησιμοποιούνται για προδιαγραφή, επαλήθευση και μοντελοποίηση παράλληλων συστημάτων.

Στόχος της διπλωματικής εργασίας είναι η επέκταση της άλγεβρας διεργασιών PARWAL. Οι δύο επεκτάσεις που έχουν γίνει αφορούν τα δικαιώματα πρόσβασης που έχουν οι χρήστες. Κάθε αντικείμενο όταν δημιουργηθεί από κάποιο χρήστη ορίζονται τα δικαιώματα για ανάγνωση και γραφή στα περιεχόμενα του. Η πρώτη επέκταση αναφέρεται σε δυναμική αλλαγή των δικαιωμάτων του αντικειμένου από τον δημιουργό του. Κάθε χρήστης από την στιγμή που είναι ο δημιουργός του αντικειμένου έχει δικαίωμα επεξεργασίας των λιστών δικαιωμάτων του αντικειμένου και μπορεί να προσθέσει ή να αφαιρέσει χρήστες από αυτές.

Η δεύτερη επέκταση είναι μια παραλλαγή της γλώσσας PARWAL όπου οι χρήστες είναι χωρισμένοι σε ομάδες ανάλογα με το ρόλο που έχουν στο σύστημα. Κάθε χρήστης που δημιουργεί ένα αντικείμενο σε αυτή τη περίπτωση δηλώνει ποιες ομάδες χρηστών έχουν δικαιώματα ανάγνωσης και γραφής στο αντικείμενο. Από την στιγμή που μια ομάδα βρίσκεται στις λίστες δικαιωμάτων του αντικειμένου τότε όλοι οι χρήστες που ανήκουν σε αυτή την ομάδα έχουν αυτά τα δικαιώματα στο συγκεκριμένο αντικείμενο.

Τέλος οι δύο επεκτάσεις θα χρησιμοποιηθούν για τη μοντελοποίηση ενός ρεαλιστικού συστήματος με απαιτήσεις ιδιωτικότητας.

Περιεχόμενα

Κεφάλαιο 1	Εισαγωγή.....	1
	1.1 Κίνητρα	1
	1.2 Σκοπός	2
	1.3 Δομή Εργασίας	3
Κεφάλαιο 2	Ιδιωτικότητα.....	4
	2.1 Εισαγωγή στην Ιδιωτικότητα	4
	2.2 Samuel Warren και Louis Brandeis	6
	2.3 Κατηγοριοποίηση της Ιδιωτικότητας	7
	2.3.1 William Prosser	8
	2.3.2 Alan F. Westin	8
	2.4 Διασφάλιση Ιδιωτικότητας	9
	2.5 Ταξινόμηση Ιδιωτικότητας	9
	2.6 Απαιτήσεις Ιδιωτικότητας	11
	2.7 Ανάπτυξη της Τεχνολογίας	11
Κεφάλαιο 3	Άλγεβρες Διεργασιών και η Γλώσσα PARWAL.....	14
	3.1 Εισαγωγή στις τυπικές μεθόδους	14
	3.2 Προκλήσεις που δημιουργούνται	15
	3.3 Προηγούμενες Εργασίες	16
	3.3.1 Τυπική Μέθοδος Διασφάλισης Ιδιωτικότητας-EPAL	16
	3.2 Πλατφόρμα για Προτιμήσεις Ιδιωτικότητας – P3P	17
	3.4 Άλγεβρες Διεργασιών	16
	3.4.1 Άλγεβρα Διεργασιών CCS	18
	3.4.2 Άλγεβρα Διεργασιών π -calculus	19
	3.4.3 Τυπική Γλώσσα PARWAL	19
Κεφάλαιο 4	Σύνταξη και Σημασιολογία της γλώσσας D-PARWAL.....	22
	4.1 Γενική Περιγραφή γλώσσας	22

4.2	Σύνταξη	22
4.3	Σημασιολογία	27
4.4	Παράδειγμα	32
Κεφάλαιο 5	Σύνταξη και Σημασιολογία της γλώσσας G-PARWAL.....	37
5.1	Γενική Περιγραφή γλώσσας	37
5.2	Σύνταξη	38
5.3	Σημασιολογία	41
Κεφάλαιο 6	Παράδειγμα Μελέτης.....	46
6.1	Παρουσίαση Παραδείγματος	46
6.2	Γράφος παραδείγματος	47
6.3	Σύνταξη Διεργασιών D-PARWAL	50
6.3.1	Παρουσίαση Παραδείγματος	51
6.3.2	Αξιολόγηση Παραδείγματος	54
6.4	Παρουσίαση Παραδείγματος G-PARWAL	54
6.4.1	Τι προβλήματα Ιδιωτικότητας προκύπτουν και γιατί	53
ΚΕΦΑΛΑΙΟ 7	Συμπεράσματα	57
7.1	Συμπεράσματα	57
7.2	Μελλοντική Εργασία	58
Βιβλιογραφία		59

ΚΑΤΑΛΟΓΟΣ ΜΕ ΕΙΚΟΝΕΣ

ΕΙΚΟΝΑ 1: 25 ΠΙΟ ΚΟΙΝΟΙ ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ ΑΝΑ ΤΟ ΠΑΓΚΟΣΜΙΟ	13
ΕΙΚΟΝΑ 2: ΓΡΑΦΟΣ ΣΕΝΑΡΙΟΥ 1	49
ΕΙΚΟΝΑ 3: ΓΡΑΦΟΣ ΣΕΝΑΡΙΟΥ 2	49

ΚΑΤΑΛΟΓΟΣ ΜΕ ΠΙΝΑΚΕΣ

ΠΙΝΑΚΑΣ 1: ΣΥΝΤΑΞΗ ΓΛΩΣΣΑΣ D-PARWAL – ΠΡΟΘΕΜΑΤΑ	25
ΠΙΝΑΚΑΣ 2: ΣΥΝΤΑΞΗ ΓΛΩΣΣΑΣ D-PARWAL – ΔΙΕΡΓΑΣΙΕΣ	26
ΠΙΝΑΚΑΣ 3: ΚΑΝΟΝΕΣ ΜΕΤΑΒΑΣΗΣ ΓΙΑ ΑΝΤΙΚΕΙΜΕΝΑ ΤΥΠΟΥ USER	28
ΠΙΝΑΚΑΣ 4: ΚΑΝΟΝΕΣ ΜΕΤΑΒΑΣΗΣ ΓΙΑ ΑΝΤΙΚΕΙΜΕΝΑ	29
ΠΙΝΑΚΑΣ 5: ΚΑΝΟΝΕΣ ΜΕΤΑΒΑΣΗΣ ΓΙΑ ΣΥΣΤΗΜΑΤΑ	30
ΠΙΝΑΚΑΣ 6: ΣΥΝΤΑΞΗ ΓΛΩΣΣΑΣ G-PARWAL – ΠΡΟΘΕΜΑΤΑ	40
ΠΙΝΑΚΑΣ 7: ΣΥΝΤΑΞΗ ΓΛΩΣΣΑΣ G-PARWAL – ΔΙΕΡΓΑΣΙΕΣ	40
ΠΙΝΑΚΑΣ 8: ΚΑΝΟΝΕΣ ΜΕΤΑΒΑΣΗΣ ΓΙΑ ΑΝΤΙΚΕΙΜΕΝΑ ΤΥΠΟΥ USER	42
ΠΙΝΑΚΑΣ 9: ΚΑΝΟΝΕΣ ΜΕΤΑΒΑΣΗΣ ΓΙΑ ΑΝΤΙΚΕΙΜΕΝΑ	42
ΠΙΝΑΚΑΣ 10: ΚΑΝΟΝΕΣ ΜΕΤΑΒΑΣΗΣ ΓΙΑ ΣΥΣΤΗΜΑΤΑ	43

Κεφάλαιο 1

Εισαγωγή

1.1 Κίνητρα	1
1.2 Σκοπός	2
1.3 Δομή Εργασίας	3

1.1 Κίνητρα

Το κυριότερο κίνητρο για τη μελέτη της ιδιωτικότητας στα υπολογιστικά συστήματα μπορεί να θεωρηθεί η ραγδαία ανάπτυξη της τεχνολογίας όπου εγκυμονεί κινδύνους που πρέπει να αντιμετωπιστούν. Παρατηρείται ότι καθημερινά πάρα πολλοί χρήστες χρησιμοποιούν τις υπηρεσίες κοινωνικής δικτύωσης που αν και εμφανίστηκαν ξαφνικά έγιναν εθισμός για τους χρήστες και διατηρώντας το δικό τους προφίλ δημοσιεύοντας προσωπικές πληροφορίες. Αφήνουν γνωστούς και άγνωστους, να μπορούν να μάθουν συνήθειες και ιστορικό της ζωής τους. Η διαφύλαξη των προσωπικών όσο και των επαγγελματικών πληροφοριών είναι απαραίτητη ειδικά σήμερα που η τεχνολογία αναπτύσσεται συνεχώς.

Η τεχνολογία εισβάλλει όλο και περισσότερο στη ζωή μας. Παρατηρούμε ότι αρκετοί χρήστες χρησιμοποιούν το Διαδίκτυο για να εκτελέσουν διάφορες αγορές, γνωρίζοντας τις απειλές που μπορεί να προκύψουν δίνουν τα προσωπικά τους στοιχεία όπως ονοματεπώνυμο, διεύθυνση και αριθμό πιστωτικής κάρτας.

Οι επιθέσεις στο κυβερνοχώρο αυξάνονται μέρα με τη μέρα με αποτέλεσμα είτε άθελα είτε σκόπιμα σημαντικές πληροφορίες να κινδυνεύουν. Οι παραβιάσεις σε προσωπικά δεδομένα και πληροφορίες αυξάνονται καθημερινά έχοντας αποτέλεσμα την

αποκάλυψη λεπτών προσωπικών δεδομένων. Το κάθε άτομο έχει το δικαίωμα της ιδιωτικότητας και για να γίνει αυτό θα πρέπει να οριστούν κανόνες όπου θα είναι σεβαστοί από όλους.

Με τη ραγδαία ανάπτυξη της τεχνολογίας προέκυψαν ανάγκες για προστασία της ιδιωτικότητας του χρήστη σε συστήματα. Ο κάθε χρήστης έχει το δικαίωμα να μπορεί να καθορίσει σε ποιους δίνει την ελευθερία να δουν και να επεξεργαστούν πληροφορίες που τον αφορούν. Θα πρέπει να έχει την δυνατότητα να δηλώνει ποιοι έχο Ψ δικαιώματα και τι δικαιώματα σε αντικείμενα που σχετίζονται με αυτόν. Επίσης θα πρέπει να του παρέχεται και η δυνατότητα να μπορεί να αλλάξει αυτά τα δικαιώματα όποτε επιθυμεί. Αυτός είναι ένας τρόπος να προστατευτεί η ιδιωτικότητα ενός χρήστη όσο αυτός το επιθυμεί σε ένα υπολογιστικό σύστημα.

Συνειδητοποιώντας το Ψ κινδύνους που μπορεί να προκύψο Ψ από τα πιο πάνω παραδείγματα χρειάζεται να προταθούν νέα μοντέλα, λογικές, γλώσσες όπως και εργαλεία για διασφάλιση της ιδιωτικότητας σε συστήματα. Αυτή η ανάγκη δημιούργησε νέες προκλήσεις στο πεδίο της ιδιωτικότητας και νέες ερευνητικές ευκαιρίες στο πεδίο των τυπικών μεθόδων. Έτσι σε αυτή τη διπλωματική εργασία θα επικεντρωθούμε στη μελέτη της ιδιωτικότητας και πώς μπορεί να διασφαλιστεί μέσα σε ένα σύστημα.

1.2 Σκοπός

Στη διπλωματική εργασία αυτή θα μελετηθεί η έννοια της ιδιωτικότητας και πώς διασφαλίζεται σε ένα υπολογιστικό σύστημα χρησιμοποιώντας τυπικές μεθόδους που περιγράφουν τη λειτουργία συστημάτων και ικανοποιούν απαιτήσεις που υπάρχουν σε θέματα ιδιωτικότητας. Οι τυπικές μέθοδοι χρησιμοποιούνται για τη προδιαγραφή, ανάπτυξη και επαλήθευση συστημάτων με συστηματικό τρόπο. Για τη μοντελοποίηση του συστήματος χρησιμοποιείται η μέθοδος των αλγεβρών διεργασιών. Οι άλγεβρες διεργασιών χρησιμοποιούνται για προδιαγραφή, επαλήθευση και μοντελοποίηση παράλληλων συστημάτων.

Στόχος μας είναι δύο επεκτάσεις της σύνταξης και της σημασιολογίας της τυπικής γλώσσας PARWAL, που όρισε η Βερόνικα Ιωάννου στα πλαίσια της διατριβής της το 2011 [12]. Η πρώτη επέκταση της γλώσσας είναι σε μια τυπική γλώσσα όπου η διαχείριση των δικαιωμάτων πρόσβασης στα αντικείμενα θα γίνεται δυναμικά. Οι ιδιοκτήτες των αντικειμένων θα μπορούν να αλλάζουν τα δικαιώματα πρόσβασης καθώς το σύστημα θα εκτελείται. Έτσι μια διεργασία θα έχει πρόσβαση σε ένα αντικείμενο εάν ο ιδιοκτήτης του αντικειμένου το επιτρέπει τη συγκεκριμένη στιγμή. Η δεύτερη επέκταση της γλώσσας PARWAL, σε μια τυπική γλώσσα όπου η διαχείριση των δικαιωμάτων πρόσβασης στα αντικείμενα θα αφορά ομάδες χρηστών και όχι τον κάθε χρήστη ατομικά ανάλογα με το ρόλο που έχουν στο σύστημα.

1.3 Δομή Εργασίας

Η παρούσα πτυχιακή εργασία αποτελείται από 7 κεφάλαια. Στο Κεφάλαιο 2 γίνεται αναφορά στην έννοια της ιδιωτικότητας. Παρουσιάζεται μία ιστορική αναδρομή για το πώς προσεγγίστηκε η σημαντικότητα της ιδιωτικότητας και γίνεται μία παρουσίαση της ανάπτυξης της τεχνολογίας και πώς επηρεάζει την ιδιωτικότητα του κάθε ατόμου. Στο Κεφάλαιο 3 γίνεται μια γενική περιγραφή στις τυπικές μεθόδους και στις άλγεβρες διεργασιών. Στη συνέχεια παρουσιάζονται οι άλγεβρες διεργασιών CCS, π -calculus και PARWAL. Στο Κεφάλαιο 4 παρουσιάζεται η γλώσσα D-PARWAL, όπου είναι η πρώτη κύρια συνεισφορά αυτής της ατομικής διπλωματικής εργασίας, η οποία επεκτείνει την γλώσσα PARWAL για δυναμική αλλαγή των δικαιωμάτων των αντικειμένων. Στο Κεφάλαιο 5 παρουσιάζεται η γλώσσα G-PARWAL, όπου είναι η δεύτερη επέκταση της γλώσσας PARWAL, η οποία αναφέρεται στους χρήστες ως ομάδες ανάλογα με το ρόλο που έχουν στο σύστημα. Στο Κεφάλαιο 6 επιδεικνύεται η χρησιμότητα των δύο επεκτάσεων που έχουν αναπτυχθεί μέσω μιας μελέτης εφαρμογής από τον πραγματικό κόσμο. Τέλος στο Κεφάλαιο 7 υπάρχουν τα συμπεράσματα και η μελλοντική εργασία που μπορεί να γίνει στις δύο επεκτάσεις της γλώσσας.

Κεφάλαιο 2

Ιδιωτικότητα

2.1 Εισαγωγή στην Ιδιωτικότητα	4
2.2 Samuel Warren και Louis Brandeis	5
2.3 Κατηγοριοποίηση της Ιδιωτικότητας	6
2.3.1 William Prosser	7
2.3.2 Alan F. Westin	7
2.4 Διασφάλιση Ιδιωτικότητας	7
2.5 Ταξινόμηση Ιδιωτικότητας	8
2.6 Απαιτήσεις Ιδιωτικότητας	9
2.7 Ανάπτυξη της Τεχνολογίας	10

2.1 Εισαγωγή στην Ιδιωτικότητα

Στην ερώτηση τι είναι ιδιωτικότητα (privacy) μπορείς να λάβεις πολλές και διαφορετικές απαντήσεις γιατί είναι μια έννοια που το κάθε άτομο την αντιλαμβάνεται διαφορετικά. Η ιδιωτικότητα δεν αποτελεί μια ανθρωπολογική σταθερά. Προσδιορίζεται σε σχέση με το ν κοινωνικό περίγυρο του από μόνον. Η εμβέλεια της ιδιωτικότητας ορίζεται από τις αντιλήψεις και τα ήθη μιας εποχής και κοινωνικής οργάνωσης τα οποία υπόκεινται σε διαρκή αλλαγή. Οι αλλαγές στο μέγεθος στη δομή και στη φύση της οικογένειας, η ανάδειξη νέων κοινωνικών χώρων και πεδίων δραστηριότητας, η διάκριση χώρου εργασίας και χώρου κατοικίας, οι νέες τεχνολογίες επικοινωνίας μεταλλάσσουν την πραγματικότητα και τις αντιλήψεις σχετικά με το τι είναι «ιδιωτικό» και τι «δημόσιο». Προέρχεται από τη λατινική λέξη “privatus” και αναφέρεται στη προάσπιση των προσωπικών δεδομένων των χρηστών.

Η ιδιωτικότητα προσεγγίστηκε μέσω τριών εννοιών, την εδαφική ιδιωτικότητα όπου αναφέρεται στην προστασία του στενού φυσικού χώρου που περιλαμβάνει το άτομο

είτε είναι χώρος εργασίας, είτε ο χώρος του σπιτιού του, την ιδιωτικότητα του ατόμου που αναφέρεται στην προστασία του ατόμου από αναίτιες παρεμβάσεις τρίτων στην προσωπική του ζωή, και την ιδιωτικότητα της πληροφορίας όπου αναφέρεται στο δικαίωμα κάθε ατόμου να ελέγχει κατά πόσο προστατεύονται τα προσωπικά του δεδομένα.

Τα προσωπικά δεδομένα είναι κάθε πληροφορία που προσδιορίζει την προσωπικότητα ενός ατόμου και η προστασία αυτών των δεδομένων έχει σκοπό τη διαφύλαξη της ιδιωτικότητας και αποτελεί μέρος της γενικής έννοιας της ιδιωτικότητας. Η ιδιωτική ζωή του καθενός είναι πολύτιμη και πρέπει να είναι σεβαστή από τον καθένα μας. Είναι η πνευματική, σωματική και ψυχική ελευθερία του κάθε ατόμου.

Η προστασία των προσωπικών δεδομένων εγείρεται ως αίτημα συνδεδεμένο με την τεχνολογική εξέλιξη, καθώς αξιολογείται πως οι υφιστάμενες ρυθμίσεις δεν προσφέρουν επαρκή προστασία έναντι των κινδύνων. Λαμβάνοντας υπόψη τις ιδιαίτερες δυνατότητες και επιπτώσεις της ηλεκτρονικής επεξεργασίας προσωπικής πληροφορίας, η προστασία προσωπικών δεδομένων δεν περιορίζεται στη ρύθμιση και προστασία της πληροφορίας που το άτομο θεωρεί ιδιωτική και ευαίσθητη και για τον λόγο αυτό επιθυμεί να απαγορεύσει ή να περιορίσει τη συλλογή, χρήση και διάδοση της. Αφορά κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο αφού η πληροφοριακή αξία καθορίζεται από την επεξεργασία της, τον συνδυασμό της με άλλες πληροφορίες και την αξιολόγηση της. Στο πλαίσιο της προστασίας προσωπικών δεδομένων δεν είναι μόνο η παρεμπόδιση της μη εξουσιοδοτημένης χρήσης ή αποκάλυψης σε άλλους αλλά ένα σύνολο από αρχές και δικαιώματα.

Μια από τις πιο συνήθεις προσλήψεις της έννοιας της ιδιωτικότητας είναι ότι αυτή συνιστάται στον απόρρητο χαρακτήρα ορισμένων ζητημάτων και υπό αυτή την έννοια η ιδιωτικότητα προσβάλλεται με την αποκάλυψη απόρρητης πληροφορίας. Η έννοια του απορρήτου αναφέρεται στη υποχρέωση προσώπων ή οργανισμών να διαφυλάσσουν πληροφορίες που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας σχέσης εμπιστοσύνης είτε κατέχουν αυτές τις πληροφορίες λόγω της θέσης το υ ή της αρμοδιότητάς τους. Για να είναι μια πληροφορία απόρρητη/εμπιστευτική θα πρέπει να είναι σε μια κατάσταση περιορισμένης πρόσβασης.

Διάφοροι φιλόσοφοι προσδιόρισαν τη σημαντικότητα του απορρήτου της ιδιωτικής ζωής με διαφορετικούς τρόπους. Ο Bloustein [5] υπερασπίζεται ότι το απόρρητο είναι απαραίτητο για την ύπαρξη της ανθρώπινης προσωπικότητας. Οι υπόλοιποι φιλόσοφοι εστιάζονται στο ρόλο του απορρήτου της ιδιωτικής ζωής που επιτρέπει σε προσωπικές σχέσεις ή γενικά στις διαπροσωπικές σχέσεις. Ο Gavison [11] υποστηρίζει ότι το απόρρητο της ιδιωτικής ζωής είναι ένας τρόπος ελέγχου της πρόσβασης σε κάποιο άτομο. Η Thomson [7], αναφέρει ότι κάθε άτομο θα ορίσει διαφορετικά τον όρο της ιδιωτικότητας και κάποια σημεία για κάποιον μπορεί να είναι σημαντικά ενώ για κάποιο άλλο όχι τόσο σημαντικά. Αναφέρει ότι κανείς δεν είναι σε θέση να διατυπώσει έναν ορισμό για τον όρο αυτό.

2.2 Samuel Warren και Louis Brandeis

Δύο πολύ αξιόλογοι νομικοί, ο Samuel Warren και ο Luis D. Brandeis, αποφοίτησαν από το Harvard Law School με άριστα. Ο Luis Brandeis έγινε δικαστής του Αμερικάνικου Ανώτατου Δικαστηρίου. Το 1890 δημοσιεύτηκε το άρθρο τους “The Right to Privacy” [12] , όπου παρουσίασαν το θεμελιώδες δικαίωμα να αφήνεται ήσυχος – the right to be let alone- όπου σε κάθε άτομο πρέπει να προστατεύεται η ιδιοκτησία του είτε αυτή είναι άυλη είτε απτή. Η πλήρη προστασία της ιδιοκτησίας είναι παλιά αρχή αλλά με τον καιρό πρέπει να γίνεται μια νέα έρευνα για τη φύση και την έκταση αυτής της προστασίας.

Η προστασία του ατόμου από τη στέρηση της ελευθερίας, η καταπάτηση των ανθρώπινων δικαιωμάτων και η προστασία της ιδιωτικής περιουσίας ήταν τα βασικότερα δικαιώματα. Κατά τη διάρκεια των χρόνων στην προστασία του ατόμου αναγνωρίστηκε και η πνευματική φύση του ανθρώπου, των συναισθημάτων και της διάνοια του. Σήμερα το κάθε άτομο έχει το δικαίωμα να βρίσκεται σε ένα πλαίσιο στο οποίο να έχει προσωπικές στιγμές και να μπορεί να ζει τη ζωή του όπως αυτό θέλει.

Η προστασία της σωματικής βλάβης ήταν αναγκαίο να επεκταθεί και στη προστασία από τυχόν εκφοβισμούς ενάντια στην σωματική βλάβη. Πολύ αργότερα ήρθε στην επιφάνεια και η προστασία του ατόμου από θορύβους, οσμές, σκόνη και καπνό. Έτσι η προστασία του ατόμου επεκτάθηκε πέρα από τη σωματική στη συναισθηματική. Η

διασφάλιση της θέσης του ατόμου μεταξύ των συνανθρώπων του ήταν η αιτία να συνταχθεί ο νόμος για συκοφαντική δυσφήμιση. Στις μέρες μας το κουτσομπολιό όπως ονομάζεται είναι πλέον μόδα, ανάγκη και εμπόριο που τη ζούμε καθημερινά μέσα από εφημερίδες, περιοδικά, τηλεοπτικά και ραδιοφωνικά μέσα. Θεωρείται ως κοινωνικό σχόλιο και ενδιαφέρον. Οι δύο νομικοί τονίζουν ότι οι σκέψεις, τα συναισθήματα και οι αισθήσεις χρειάζονται την απαιτούμενη προστασία.

Ακόμη ο Samuel Warren και ο Luis Brandeis έχοντας σκοπό να εξετάσουν κατά πόσο η υπάρχουσα νομοθεσία παρέχει κανόνες όπου λαμβάνουν υπόψη τους την προστασία της ιδιωτικής ζωής του ατόμου. Και αν υπάρχουν τέτοιοι κανόνες τότε σε πιο βαθμό είναι ικανοποιητικοί αφού θα πρέπει να αναβαθμίζονται ανάλογα με την ανάπτυξη της τεχνολογίας και τις ανάγκες της κοινωνίας.

Οι σύγχρονοι νομικοί μελετώντας το άρθρο αυτό παρατήρησαν δύο μειονεκτήματα. Αρχικά αναφέρονται αρκετές παραβιάσεις ιδιωτικότητας ως αδικήματα που στην πραγματικότητα δεν είναι όπως για παράδειγμα η βλάβη της σωματικής ακεραιότητας. Και δεύτερο μειονέκτημα είναι ότι δεν κατηγοριοποιεί τις παραβιάσεις ιδιωτικότητας και δεν διαχωρίζει την παραβίαση της ιδιωτικότητας από την απειλή της σωματικής ακεραιότητας του ατόμου. Ο Samuel Warren και ο Luis Brandeis έκαναν προσπάθειες για να αναγνωριστεί το δικαίωμα της ιδιωτικότητας, κάτι όμως που δεν έγινε εφικτό. Χρόνια μετά και υπό την μεγάλη επίδραση της τεχνολογικής επανάστασης η αντίληψη της ιδιωτικότητας έχει εμπλουτιστεί με επιμέρους δικαιώματα, όπως το δικαίωμα σε ιδιωτική ζωή, ο περιορισμός της προσβασιμότητας, ο αποκλειστικός έλεγχος της πρόσβασης στον ιδιωτικό χώρο, το δικαίωμα στο απόρρητο και το δικαίωμα στην απόλαυση της μοναξιάς της ιδιωτικότητας, της ανωνυμίας και της απόσυρσης.

2.3 Κατηγοριοποίηση της Ιδιωτικότητας

Η νομοθεσία διαχωρίζει και αναγνωρίζει αδικήματα παραβίασης ιδιωτικότητας έτσι κάθε άτομο που έχει υποστεί κάποια ζημιά μπορεί να επικαλεστεί αυτό το νόμο και να λάβει αποζημίωση από το άτομο που είναι υπεύθυνος για την ζημιά που έχει υποστεί. Ακολουθούν δύο κατηγοριοποιήσεις την ιδιωτικότητας από το λόγιο William Prosser και το νομικό Alain Westin.

2.3.1 William Prosser

Ο λόγιος William Prosser [13] στο σύγγραμμά του “Privacy” αναφέρει τέσσερις κατηγορίες “εισβολής” στην ιδιωτική ζωή του ατόμου. Η πρώτη κατηγορία που αναφέρει είναι το αδίκημα της εισβολής είτε της απομόνωσης ή μοναξιάς του ατόμου είτε στις ιδιωτικές του υποθέσεις. Αυτή η κατηγορία προστατεύει το άτομο από ανεπιθύμητες εισβολές στο προσωπικό και ιδιωτικό του χώρο. Η δεύτερη κατηγορία είναι το αδίκημα της δημοσιοποίησης ιδιωτικών και προσβλητικών δεδομένων του ατόμου. Προστατεύει τα προσωπικά και ιδιωτικά ζητήματα του ατόμου από ανεπιθύμητες εισβολές, έτσι προστατεύει την πνευματική κατάσταση και διαφυλάσσει την διαβίωση του ατόμου. Η τρίτη κατηγορία αναφέρεται στο αδίκημα της δημοσιοποίησης παραποιημένων πληροφοριών οι οποίες θέτουν το άτομο σε δυσχερή θέση απέναντι στο κοινωνικό περίγυρο και προστατεύει τη διανοητική και συναισθηματική ευεξία του ατόμου. Και τέλος η τέταρτη κατηγορία είναι το αδίκημα της οικειοποίησης του ονόματος ή της ομοιότητας του ατόμου με κάποιο άλλο. Προστατεύει το άτομο από το να δημοσιεύονται πληροφορίες χωρίς να του ζητηθεί η συγκατάθεση του για να επωφεληθούν κάποια άλλα άτομα. Μέσα από αυτό στο σύγγραμμά του διευκρινίστηκαν ασάφειες και παραλείψεις της μελέτης των Samuel Warren και Luis Brandeis.

2.3.2 Alan F. Westin

Ο δικηγόρος, Alain Westin [2], έγραψε το βιβλίο “Privacy and Freedom” το οποίο θεωρείται το σημαντικότερο βιβλίο του 20^{ου} αιώνα αφού μέσω της τεχνολογίας η εισβολή στη προσωπική ζωή του ατόμου είναι καθημερινή. Στον ορισμό που μας δίνει ο Westin για την ιδιωτικότητα αναφέρει ότι η ιδιωτικότητα καταπατείται μέσω διάφορων μορφών παρακολούθησης που αρχικά καταγράφονται προσωπικές πληροφορίες και στη συνέχεια δημοσιεύονται χωρίς τη συγκατάθεση του ατόμου. Ακόμη αναφέρει ο κάθε άνθρωπος έχει την ανάγκη για ιδιωτική ζωή και αναφέρεται σε διάφορες μεθόδους που χρησιμοποιούν τα άτομα για να αποτρέψουν την παραβίαση της ιδιωτικής τους ζωής.

2.4 Διασφάλιση Ιδιωτικότητας

Τα άτομα για να αποφύγουν την παραβίαση της ιδιωτικής τους ζωής καταλήγουν να ανήκουν σε μία από τις παρακάτω κατηγορίες. Υπάρχουν άτομα που καταλήγουν στην μοναχικότητα και απομονώνονται στους εαυτούς τους και με αυτό το ν τρόπο αποφεύγουν την κριτική και τις παρατηρήσεις. Άλλα άτομα διασφαλίζουν την ιδιωτικότητα τους μέσω της οικειότητας όπου δημιουργούν ομάδες ατόμων, των οποίων τα άτομα είναι αποκλειστικά μέλη, και έτσι δημιουργούν μια σχέση ειλικρινή, ήρεμη και στενή. Μια άλλη κατηγορία που καταλήγουν τα άτομα είναι η ανωνυμία όπου τα άτομα δραστηριοποιούνται ελεύθερα σε δημόσιους χώρους χωρίς να αναγνωρίζονται και να παρακολουθούνται από περαστικούς. Και η τελευταία κατηγορία είναι η επιφυλακτικότητα όπου το άτομο είναι επιφυλακτικό και προσεκτικό στις συνομιλίες με τρίτους ώστε να αποφύγει παραβίαση της ιδιωτικότητας του.

Ο Westin προσδιορίζει το λόγο που επιτυγχάνεται η διασφάλιση της ιδιωτικότητας μέσω τεσσάρων διαδικασιών που είναι οι εξής: *Προσωπική Αυτονομία* που αναφέρεται στην επιθυμία του ατόμου να μην πέσει θύμα εκμετάλλευσης και κακομεταχείρισης. *Συναισθηματική Απελευθέρωση* όπου το άτομο αποφεύγει τις εντάσεις που θα του προκαλέσουν συναναστροφή με το κοινωνικό περιβάλλον. *Αυτό-αξιολόγηση* όπου το άτομο κάνει πιο ουσιαστικά και αυτόνομα βήματα για να έχει πιο ενεργή συμμετοχή στη διεκπεραίωση μίας εργασίας. Και *Περιορισμένη και Προστατευμένη Επικοινωνία* όπου το άτομο θέτει τα όρια στις διαπροσωπικές σχέσεις και την επιλογή που κάνει το κάθε άτομο να αναφέρει προσωπικές πληροφορίες σε άτομα εμπιστοσύνης.

Το βιβλίο του Alain Westin είχε παρουσιαστεί το 1967 και αυτό θεωρείται το μόνο μειονέκτημα της θεωρίας του γιατί η τεχνολογία δεν είχε αναπτυχθεί όπως είναι σήμερα και οι προσωπικές πληροφορίες προστατεύονταν πιο εύκολα.

2.5 Ταξινόμηση Ιδιωτικότητας

Η ταξινόμηση της ιδιωτικότητας κατά τον Daniel Solove [4] αποτελείται από 4 ομάδες. Με αυτή την ταξινόμηση επιχειρεί την καλύτερη κατανόηση των παραβιάσεων στην

ιδιωτικότητα και τονίζει ότι η νομοθεσία πρέπει να εναρμονιστεί και τα αδικήματα που αφορούν την ιδιωτικότητα δεν διαφοροποιούνται από την κοινωνία.

Η πρώτη ομάδα είναι η συλλογή πληροφοριών που μπορεί να προκαλέσει αρκετά προβλήματα έστω και αν αυτές οι πληροφορίες δεν αποκαλυφθούν σε άλλα άτομα. Η συλλογή πληροφοριών μπορεί να γίνει είτε με παρακολούθηση όπου είναι μια συνεχής επιτήρηση του ατόμου, είτε με ανάκριση όπου γίνονται διάφορες ερωτήσεις στο άτομο για να ανακτηθούν οι πληροφορίες.

Η δεύτερη ομάδα είναι η επεξεργασία της πληροφορίας όπου χρησιμοποιούνται οι πληροφορίες που ανακτήθηκαν από την πρώτη ομάδα και αποθηκεύονται, επεξεργάζονται και χρησιμοποιούνται. Μια μορφή επεξεργασίας πληροφορίας είναι η συσσωμάτωση όπου συνδυάζονται διάφορα στοιχεία για ένα άτομο. Μια άλλη μορφή είναι η ταύτιση όπου συσχετίζονται οι πληροφορίες με συγκεκριμένο τρόπο. Ακόμη μια μορφή είναι η μη επαρκής παροχή ασφάλειας που αναφέρεται στην αφελή προστασία αποθηκευμένων δεδομένων από την πιθανότητα απώλειας πληροφοριών. Η δευτερογενής χρήση είναι μια μορφή όπου στοιχεία που έχουν συλλεχθεί για ένα σκοπό στο τέλος χρησιμοποιούνται για κάποιο άλλο σκοπό χωρίς τη συγκατάθεση του εμπλεκόμενου ατόμου. Και τελευταία μορφή είναι ο αποκλεισμός όπου το εμπλεκόμενο άτομο δεν είναι ενήμερο για την συλλογή των πληροφοριών του και δεν συμμετέχει στη διαχείριση και χρησιμοποίησή τους.

Η τρίτη ομάδα είναι η μεταβίβαση της πληροφορίας όπου παραβιάζει και προκαλεί επιβλαβές συνέπειες στην ιδιωτικότητα του κάθε ατόμου. Με την *παραβίαση του απορρήτου* δεν διατηρούνται οι προσωπικές πληροφορίες του ατόμου εμπιστευτικές. Μέσω της *παράθεσης* αποκαλύπτονται αληθοφανείς πληροφορίες με επιπτώσεις στον τρόπο που αντιμετωπίζεται το άτομο. Η διαδικασία *αποκάλυψης* προσωπικών πληροφοριών και με σκοπό να εκτεθεί ένα άτομο λέγεται *έκθεση*. Η δυνατότητα πρόσβασης σε αυστηρώς προσωπικά δεδομένα ενισχύεται με την αυξημένη προσβασιμότητα. Με τη μέθοδο του εκβιασμού δέχονται απειλητικά μηνύματα για διάδοση αυστηρών προσωπικών πληροφοριών. Και με την αλλοίωση η αλήθεια και τα στοιχεία του ατόμου διαστρεβλώνονται με κάποιο απότομο σκοπό.

Η τέταρτη και τελευταία ομάδα είναι η εισβολή της πληροφορίας όπου αναφέρεται στη παραβίαση των προσωπικών πληροφοριών ενός ατόμου. Γίνεται καταπάτηση έτσι ώστε με κάποιες πράξεις να διαταραχθεί η απομόνωση και η ηρεμία του ατόμου. Με τη παρεμβολή λήψεως αποφάσεων οι κυβερνήσεις εμποδίζουν τα άτομα να πάρουν αποφάσεις για προσωπικά θέματα.

2.6 Απαιτήσεις Ιδιωτικότητας

Για να μπορέσει ένα σύστημα να προσφέρει στο χρήστη ιδιωτικότητα μπορεί να χρησιμοποιήσει τις ακόλουθες απαιτήσεις:

- *Αυθεντικότητα*: η διαδικασία με την οποία επιβεβαιώνεται η ταυτότητα μιας οντότητας και θεωρείται περισσότερο απαίτηση ασφάλειας αλλά η συνεισφορά της στην ικανοποίηση των απαιτήσεων της ιδιωτικότητας είναι σημαντική. Η αυθεντικότητα συνήθως υλοποιείται με τη χρήση κωδικών πρόσβασης.
- *Προστασία Δεδομένων*: αφορά την επεξεργασία των προσωπικών δεδομένων και την ελεύθερη διακίνηση τους.
- *Ανωνυμία*: ένας χρήστης έχει την δυνατότητα να χρησιμοποιεί μια υπηρεσία ή να επικοινωνεί με μια άλλη οντότητα χωρίς να αποκαλύπτει την ταυτότητα του.
- *Εξουσιοδότηση*: είναι η διαδικασία μέσω της οποίας μια οντότητα αποκτά δικαιώματα πρόσβασης σε κάποιο αντικείμενο.
- *Αναγνώριση*: είναι η διαδικασία που ελέγχει σε ποιους χρήστες επιτρέπει την πρόσβαση σε δεδομένα, έτσι ώστε να μην αποκτήσει πρόσβαση κάποιος μη εξουσιοδοτημένος χρήστης προφυλάσσοντας με αυτό τον τρόπο την ιδιωτικότητα των κατόχων των δεδομένων.
- *Ψευδωνυμία*: μέσω αυτής προστατεύεται η αναγνώριση των χρηστών αφού οι χρήστες χρησιμοποιούν ψευδώνυμα για να προστατέψουν την αποκάλυψη της ταυτότητας τους.

2.7 Ανάπτυξη της Τεχνολογίας

Τα τελευταία χρόνια έχει σημειωθεί ραγδαία ανάπτυξη της τεχνολογίας η οποία κατάφερε να εισχωρήσει σε όλους τους τομείς της ζωής μας. Στο ξεκίνημα του 21^{ου}

αιώνα, είμαστε όλοι μάρτυρες μιας τεχνολογικής επανάστασης που με ταχύτατους ρυθμούς επιφέρει τεράστιες αλλαγές. Σίγουρα η ανάπτυξη της τεχνολογίας έχει διευκολύνει τις ζωές των ανθρώπων όμως επιφέρει και πολλούς κινδύνους.

Οι εξελίξεις στην πληροφορική τεχνολογία έχουν ως συνέπεια ότι δεν υπάρχει πλέον όριο στην πληροφορία που μπορεί να καταχωριστεί, στην ανάλυση που μπορεί να γίνει, στο χρονικό διάστημα για το οποίο μπορεί να τηρηθεί. Ο χρήστης εθίζεται στην αναγκαιότητα να παρέχει πληροφορία. Ο πολλαπλασιασμός της διατιθέμενης πληροφορίας, η απώλεια της ανωνυμίας είναι το αντίτιμο της δυνατότητας διεκπεραίωσης διαδικτυακών συναλλαγών, εργασιών και υποχρεώσεων, όπως η ηλεκτρονική αγορά και πληρωμή προϊόντων και υπηρεσιών

Μια αξιοσημείωτη εξέλιξη συνιστά η εκρηκτική ανάπτυξη της κοινωνικής δικτύωσης. Οι χρήστες καταχωρώντας και δημοσιεύοντας προσωπικά στοιχεία στα κοινωνικά δίκτυα γίνονται ευάλωτοι σε μεγαλύτερο αριθμό ατόμων. Η κλοπή της ταυτότητας του χρήστη δεν είναι απίθανο αφού πολλές εφαρμογές ή υπηρεσίες μπορεί να κρύβουν ηλεκτρονικές απάτες. Ένα από τα μεγαλύτερα μειονεκτήματα των κοινωνικών δικτύων είναι η κλοπή των προσωπικών δεδομένων ή η απειλή της ασφάλειας αυτών των δεδομένων του χρήστη.

Μέχρι στιγμής λαμβάνονται κάποια μέτρα για προστασία της ιδιωτικής ζωής όπως τα usernames που είναι μοναδικά για τον κάθε χρήστη και οι κωδικοί πρόσβασης που είναι ένας μυστικός κωδικός που χρησιμοποιεί ο χρήστης για να έχει πρόσβαση στα δεδομένα του. Αυτά όμως δεν αρκούν αφού πλέον είναι πολύ εύκολο για τους χάκερς «σπάσουν» αυτούς τους κωδικούς αφού οι χρήστες χρησιμοποιούν εύκολους και αδύναμους κωδικούς γιατί δεν ενδιαφέρονται πως λειτουργεί ένας κωδικός σε ένα υπολογιστικό σύστημα αλλά να κάνουν εύκολα και γρήγορα την δουλειά τους. Μέσα από έρευνα της εταιρίας Splashdata, η οποία αναπτύσσει ένα από τα πιο γνωστά εργαλεία ασφάλειας για κινητά, παρουσιάζει τους 2 5 πιο κοινούς κωδικούς που χρησιμοποιούν οι χρήστες ανά το παγκόσμιο.

1. password	13. iloveyou
2. 123456	14. master
3. 12345678	15. sunshine
4. qwerty	16. ashley
5. abc123	17. bailey
6. monkey	18. passw0rd
7. 1234567	19. shadow
8. letmein	20. 123123
9. trustno1	21. 654321
10. dragon	22. superman
11. baseball	23. qazwsx
12. 111111	24. michael
	25. football

Εικόνα 1: 25 πιο κοινοί κωδικοί πρόσβασης ανά το παγκόσμιο

Κάποια άλλη τεχνική που χρησιμοποιείται είναι η κρυπτογραφία όπου για να μπορέσει να υπάρξει επικοινωνία μεταξύ δύο χρηστών χρησιμοποιείται ένα μυστικό κλειδί το οποίο γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης. Ο αποστολέας το χρησιμοποιεί για να κρυπτογραφήσει το μήνυμα και ο αποστολέας για να το αποκρυπτογραφήσει. Το μειονέκτημα αυτής της τεχνικής είναι ότι η ανταλλαγή αυτού του κλειδιού θα πρέπει να γίνει χωρίς κάποιος τρίτος να μάθει για αυτό και να αποκτήσει πρόσβαση. Η μετάδοση του μέσω διαδικτύου δεν είναι ασφαλής αφού για κάποιο που γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει την επικοινωνία και να αποκτήσει το κλειδί.

Η τεχνολογία και οι πολιτικοί εμπειρογνώμονες θα πρέπει να συνεργαστούν έτσι ώστε να διασφαλίσουν το απόρρητο της ιδιωτικής ζωής. Οι επιστήμονες και οι μηχανικοί θα πρέπει να καταλάβουν τι μπορεί να γίνει από τεχνική άποψη δηλαδή τι είναι πρακτικά δυνατό ή αδύνατο. Και τέλος η κοινωνία θα πρέπει να δημιουργήσει ένα περιβάλλον στο οποίο οι νέοι κανονισμοί για τη διατήρηση του απορρήτου θα μπορούν να ανταποκριθούν όταν τεθούν σε εφαρμογή.

Κεφάλαιο 3

Τυπικές Μέθοδοι

3.1 Εισαγωγή στις τυπικές μεθόδους	14
3.2 Προκλήσεις που δημιουργούνται	15
3.3 Προηγούμενες εργασίες	16
3.3.1 Τυπική Μέθοδος Διασφάλισης Ιδιωτικότητας – EPAL	16
3.3.2 Πλατφόρμα για Προτιμήσεις Ιδιωτικότητας – P3P	17
3.4 Άλγεβρες Διεργασιών	17
3.4.1 Άλγεβρα Διεργασιών CCS	18
3.4.2 Άλγεβρα Διεργασιών π -calculus	19
3.4.3 Τυπική γλώσσα PARWAL	20

3.1 Εισαγωγή στις τυπικές μεθόδους

3.3.2 Πλατφόρμα για Προτιμήσεις Ιδιωτικότητας – P3P

Οι τυπικές μέθοδοι είναι μια συλλογή από σημειογραφίες και τεχνικές οι οποίες χρησιμοποιούνται για τη περιγραφή και ανάλυση συστημάτων. Αυτές οι μέθοδοι είναι τυπικές με την έννοια ότι στηρίζονται πάνω σε μαθηματικές θεωρίες όπως η λογική, τα αυτόματα ή η θεωρία γράφων και στόχο έχουν να βελτιστοποιήσουν την ποιότητα του συστήματος.

Η τυπική προδιαγραφή ξεκινά από μια ακριβή περιγραφή του συστήματος, που είναι πολύ σημαντική στο να συγκεκριμενοποιηθεί η συμπεριφορά του και να καταστεί δυνατή η σωστή ανάλυση του. Μπορεί να χρησιμοποιηθεί από τις αρχικές φάσεις κατασκευής του συστήματος, όπως για παράδειγμα, τη φάση του σχεδιασμού, και να χρησιμοποιηθεί για επαλήθευση των απαιτήσεων του συστήματος, στη συστηματική

αναζήτηση περιπτώσεων όπου το σύστημα αποτυγχάνει να τις ικανοποιήσει, ή ακόμα στην αξιολόγηση της ποιότητας υπηρεσιών που μπορεί να προσφέρει.

Οι αρχικές έρευνες πάνω στις τυπικές μεθόδους επικεντρώνονται στην επιβεβαίωση της ορθότητας των συστημάτων. Με τον τρόπο αυτό εννοούμε ότι το σύστημα θα ικανοποιεί τις προτεινόμενες προδιαγραφές. Η επαλήθευση λογισμικού ήταν από τις κυριότερες τυπικές μεθόδους που μελετήθηκαν. Αρχικός στόχος τέτοιων τεχνικών ήταν η τυπική επαλήθευση συστημάτων κριτικής ασφάλειας. Στην συνέχεια, προτάθηκε όπως αυτές οι μέθοδοι επαλήθευσης χρησιμοποιηθούν στο να βοηθήσουν την ανάπτυξη λογισμικών και υλικών συστημάτων. Σύμφωνα λοιπόν με την εισήγηση αυτή, τα προγράμματα έπρεπε να εκλεπυνθούν με τέτοιο τρόπο ώστε ο έλεγχος να γίνεται βήμα-βήμα, ξεκινώντας από τις προδιαγραφές και τελειώνοντας με τον κυρίως κώδικα.

Τα πλεονεκτήματα των τυπικών μεθόδων τα οποία υποβοήθησαν στην επικράτηση τους για την ανάλυση συστημάτων περιλαμβάνουν τη δυνατότητα μοντελοποίησης συστημάτων και την ύπαρξη κοινής μεθοδολογίας για μελέτη της ορθότητας και της αξιοπιστίας που τα χαρακτηρίζει. Οι τυπικές μέθοδοι έχουν ιδιαίτερη χρησιμότητα σε συστήματα όπου πολλαπλές διεργασίες ενεργούν ταυτόχρονα και κατά συνέπεια δυνατόν να παρουσιάσουν μη-ντετερμινισμό και περισσότερες από μια διαφορετικές συμπεριφορές [9].

3.2 Προκλήσεις που δημιουργούνται

Η ιδιωτικότητα προσφέρει στον τομέα των τυπικών μεθόδων πρόκληση για νέες μελέτες αφού τα δικαιώματα ιδιωτικότητας απειλούνται όλο και περισσότερο όσο η τεχνολογική ανάπτυξη αυξάνεται.

Μπορούμε να χρησιμοποιήσουμε τις τυπικές γλώσσες και την τυπική λογική για να δηλώσουμε τις διάφορες πτυχές της ιδιωτικότητας, τις ιδιότητες των συστημάτων και την πολιτική της προστασίας των προσωπικών δεδομένων, έτσι ώστε να μπορούμε να καταλάβουμε πότε ένα μοντέλο ικανοποιεί την πολιτική της ιδιωτικότητας και για να εντοπίζουμε τις διαφορές ανάμεσα στις πολιτικές ιδιωτικότητας. Εμφανίστηκαν

προκλήσεις για δημιουργία νέων τυπικών λογικών που θα καθορίζουν και θα αιτιολογούν ιδιότητες για ιδιωτικότητα.

Η τεχνολογία των τυπικών μεθόδων μπορεί να βοηθήσει στην διασφάλιση της ιδιωτικότητας παρέχοντας από φορμαλισμούς της ιδιωτικής ζωής σε πρακτικά εργαλεία για τον έλεγχο παραβίασης της ιδιωτικής ζωής.

3.3 Προηγούμενες Εργασίες

3.3.1 Τυπική Μέθοδος Διασφάλισης Ιδιωτικότητας - EPAL

Η EPAL [9][8] (Enterprise Privacy Authorization Language) είναι μια τυπική γλώσσα που χρησιμοποιείται για καταγραφή πολιτικών ιδιωτικότητας και επιβάλλει κανόνες για τη σωστή διαχείριση των δεδομένων. Οι κανόνες αυτοί ορίζονται ως λίστα ιεραρχιών *τις κατηγορίες δεδομένων* που μπορούν να δημιουργηθούν με βάση τα δεδομένα που έχουμε και η κάθε κατηγορία έχει διαφορετικό χειρισμό ως προς την ιδιωτικότητα, τους *χρήστες δεδομένων* που είναι οι ομάδες που χρησιμοποιούν τα δεδομένα αυτά, τις *προθέσεις* που μοντελοποιούν την υπηρεσία που θα χειριστεί τα δεδομένα ανάλογα με τα δεδομένα που έχουν καταγραφεί και τα σύνολα των *ενεργειών*, των *υποχρεώσεων* και των *προϋποθέσεων*.

Αφού έχουν προσδιοριστεί τα πιο πάνω στοιχεία τότε μπορούν να τυποποιηθούν για την δημιουργία των κανόνων ιδιωτικότητας για να επιτρέπεται ή όχι η εκτέλεση ενεργειών στις κατηγορίες δεδομένων για συγκεκριμένες προθέσεις δεδομένου ότι ισχύουν οι ζητούμενες προϋποθέσεις και διατηρούνται οι υποχρεώσεις.

Η EPAL *απαρτίζεται από ένα σύνολο από κανόνες ιδιωτικότητας* για να προσδιοριστεί κατά πόσον μπορεί ένα αίτημα να επιτραπεί ή να απορριφθεί. Κάθε κανόνας είναι μια πρόταση που περιλαμβάνει ένα ορισμό εκτέλεσης και έχει ένα επίπεδο προτεραιότητας

3.3.2 Πλατφόρμα για Προτιμήσεις Ιδιωτικότητας – P3P

Η Πλατφόρμα για Προτιμήσεις Ιδιωτικότητας ενημερώνει τους επισκέπτες μιας ιστοσελίδας για την πολιτική που έχει όσο αφορά την διατήρηση της εμπιστευτικότητας των προσωπικών τους δεδομένων.

Οι χρήστες έχουν την δυνατότητα να επιλέξουν τις δικές τους προτιμήσεις ιδιωτικότητας και όταν μια ιστοσελίδα δεν ανταποκρίνεται στις προτιμήσεις του χρήστη τότε είτε θα ειδοποιηθεί ο χρήστης ότι η συγκεκριμένη ιστοσελίδα δεν ικανοποιεί τις προτιμήσεις του είτε θα μπλοκάρει το περιεχόμενο.

3.4 Άλγεβρες Διεργασιών

Ο Milner [10] και ο Hoare ήταν οι πρώτοι ερευνητές που έθεσαν τα θεμέλια της άλγεβρας διεργασιών.

Οι άλγεβρες διεργασιών εντάσσονται κάτω από την ομπρέλα των τυπικών μεθόδων και στο επιστημονικό πεδίο της Πληροφορικής είναι μια οικογένεια μαθηματικών formalismών που χρησιμεύουν στην μοντελοποίηση της συμπεριφοράς παράλληλων συστημάτων. Η μοντελοποίηση επιτυγχάνεται κάνοντας χρήση τελεστών, ονομάτων, αλγεβρικών κανόνων και αλγορίθμων.

Ο formalismός κάθε άλγεβρας διεργασιών αποτελείται από τη σύνταξη και τη σημασιολογία, τα οποία μας επιτρέπουν να μοντελοποιήσουμε τις διεργασίες που απαρτίζουν κάποιο σύστημα, τους τρόπους επικοινωνίας μεταξύ των διεργασιών και τους κανόνες με τους οποίους μπορούν να μοντελοποιηθούν οι ενέργειες που εκτελούν οι διεργασίες.

Για τον ορισμό μιας άλγεβρας διεργασιών αρχικά πρέπει να ορίσουμε τα κανάλια του συστήματος, δίνοντας τους ένα όνομα, για την επικοινωνία των οντοτήτων του συστήματος. Μετά ορίζουμε τους βασικούς τελεστές που χρησιμοποιούνται για τον ορισμό των βασικών κανόνων της άλγεβρας διεργασιών που είναι:

- ο τελεστής επιλογής ενός εκ των δύο διαθέσιμων διεργασιών για να προχωρήσει στην εκτέλεση της (+) γράφεται ως $P+Q$,
- ο τελεστής για παράλληλη σύνθεση των διεργασιών επιτρέπει στις διεργασίες να προχωρήσουν στην εκτέλεση τους παράλληλα και ανεξάρτητα η μια από την άλλη ($|$) και γράφεται ως $P|Q$,
- ο τελεστής για διαδοχική εκτέλεση ενεργειών πρώτα επιτρέπει την εκτέλεση της ενέργειας 'α' και μετά η διεργασία συμπεριφέρεται όπως η διεργασία P ($.$) γράφεται ως $\alpha. P$

Οι βασικοί κανόνες που προκύπτουν από τους πιο πάνω τελεστές είναι :

- *Αντιμεταθετική ιδιότητα* ($x+y = y+x$)
- *Προσεταιριστική ιδιότητα* ($x+(y+z) = (x+y)+z$)
- *Ταυτοδυναμία* ($x+x = x$)
- *Αντιμεταθετική ιδιότητα για παράλληλη σύνθεση* ($x|y = y|x$)
- *Προσεταιριστική ιδιότητα για παράλληλη σύνθεση* ($x|(y|z) = (x|y)|z$)

Στη θεωρία της άλγεβρας διεργασιών βασικός άξονας είναι η επικοινωνία μεταξύ των διεργασιών του συστήματος και γι' αυτό χρειάζεται να ορίσουμε τις ενέργειες εισόδου και εξόδου. Χρησιμοποιούμε τον τελεστή $x(y)$ για την ενέργεια εισόδου και δείχνουμε ότι το όνομα y λαμβάνεται μέσω του καναλιού x . Για την ενέργεια εξόδου χρησιμοποιούμε τον τελεστή $x<y>$ και δείχνουμε ότι το όνομα y αποστέλλεται μέσω του καναλιού x .

Οι άλγεβρες διεργασιών θα μας βοηθήσουν να κατανοήσουμε πως λειτουργεί η γλώσσα PARWAL που είναι μια άλγεβρα διεργασιών και να επεκτείνουμε τη σύνταξη και σημασιολογία της έτσι ώστε να ικανοποιούνται οι κανόνες ιδιωτικότητας σε ένα σύστημα.

3.4.1 Άλγεβρα Διεργασιών CCS

Ο Robin Milner ασχολήθηκε με την άλγεβρα διεργασιών CCS (Calculus of Communicating Systems) [6]. Σε αυτή τη θεωρία παρουσιάζει τον δυαδικό

συγχρονισμό ως τη βασική μέθοδο για επικοινωνία και εστιάζει στις ενέργειες που πρέπει να εκτελεστούν για να επιτευχθεί η δυαδική επικοινωνία. Ορίζει μια τυπική γλώσσα η οποία περιγράφει τη παράλληλη σύνθεση, την επιλογή μεταξύ διεργασιών και την δήλωση περιορισμών. Η άλγεβρα διεργασιών CCS χρησιμοποιείται για αξιολόγηση συστημάτων κατά πόσο καταλήγουν σε αδιέξοδο ή σε αποκλεισμό διεργασιών.

Η σύνταξη της CCS ακολουθεί την πιο κάτω γραμματική:

$$\begin{aligned}
 E ::= & 0 \\
 & | a.E \\
 & | E_1 + E_2 \\
 & | E_1 \setminus E_2 \\
 & | E \setminus L \\
 & | E[f] \\
 & | C
 \end{aligned}$$

Η σημασιολογία της ορίζεται ως τη μαθηματική σχέση $\rightarrow \subseteq Proc \times Act \times Proc$, όπου γράφοντας $\langle E, a, F \rangle \in \rightarrow$ σημαίνει ότι η διεργασία E μπορεί να εκτελέσει την ενέργεια a και ακολούθως να συμπεριφέρεται όπως η διεργασία F . Το γράφουμε ως $E \xrightarrow{a} F$. Η ενέργεια αυτή μπορεί να είναι ενέργεια εισόδου, ενέργεια εξόδου ή εσωτερική ενέργεια.

3.4.2 Άλγεβρα Διεργασιών π -calculus

Ο Robin Milner, ο Joachim Parrow και ο David Walker επεκτείνοντας την άλγεβρα διεργασιών CCS δημιούργησαν την άλγεβρα διεργασιών π -calculus [9]. Η π -calculus επιτρέπει στα ονόματα των καναλιών να είναι τα αντικείμενα επικοινωνίας και να μεταφέρονται μέσα στα κανάλια. Οι διεργασίες επικοινωνούν εφόσον χρησιμοποιούν το ίδιο όνομα καναλιού. Ο ρόλος ενός καναλιού είναι διπλός, από τη μια ένα κανάλι επικοινωνίας λειτουργεί ως αντικείμενο που ανταλλάσσεται μεταξύ των διεργασιών, και από την άλλη αποτελεί διάδρομο επικοινωνίας μεταξύ διεργασιών. Αυτός ο διπλός ρόλος είναι και το πλεονέκτημα αυτής της άλγεβρας διεργασιών

Η σύνταξη της π -calculus κτίζεται εφαρμόζοντας την σύνταξη BNF όπου:

$P ::= 0$	τερματισμός ή αδιέξοδο
$ x(y).P$	το μήνυμα y παραλαμβάνεται μέσω του καναλιού x και ακολούθως συνεχίζει ως η διεργασία P
$ \bar{x}(y).P$	το μήνυμα y στέλνεται μέσω του καναλιού x και ακολούθως συνεχίζει ως η διεργασία P
$ P P$	παράλληλη εκτέλεση των διεργασιών
$ (v x)P$	δημιουργία ενός νέου αντικειμένου
$!P$	δημιουργία αντιγράφων της διεργασία P

3.4.3 Τυπική Γλώσσα PARWAL

Θα παρουσιάσουμε τη τυπική γλώσσα μοντελοποίησης συστημάτων που περιλαμβάνει περιορισμούς ιδιωτικότητας, PARWAL [15]. Στη γλώσσα PARWAL τα κανάλια χρησιμοποιούνται για την επικοινωνία ανάμεσα στις διεργασίες όπου κάθε διεργασία μπορεί να στείλει ή να διαβάσει κάποιο μήνυμα μέσω κάποιου καναλιού και για απόδοση ταυτότητας στις οντότητες του συστήματος όπου η κάθε διεργασία έχει ένα μοναδικό αναγνωριστικό που την χαρακτηρίζει και το οποίο υλοποιείται ως ένα κανάλι.

Η γλώσσα PARWAL σε αντίθεση από τη άλγεβρα διεργασιών CCS τα κανάλια έχουν διπλό ρόλο στη γλώσσα. Χρησιμοποιούνται για την επικοινωνία ανάμεσα στις διεργασίες και στην απόδοση ταυτότητας στις οντότητες του συστήματος. Η ταυτότητα αυτή είναι ένα μοναδικό χαρακτηριστικό το οποίο υλοποιείται ως κανάλι και για να το χρησιμοποιήσει ένας χρήστης για ανάγνωση και γραφή θα πρέπει πρώτα να αποκτήσει πρόσβαση στο αναγνωριστικό του. Οι οντότητες της PARWAL είναι τα αντικείμενα, οι χρήστες και το σύστημα.

Βασικό στοιχείο της πολιτικής της γλώσσας αυτής είναι οι λίστες δικαιωμάτων οι οποίες αρχικοποιούνται κατά τη δημιουργία του αντικειμένου από το δημιουργό του. Οι λίστες δικαιωμάτων περιλαμβάνουν τα αναγνωριστικά των χρηστών που έχουν δικαίωμα γραφής ή ανάγνωσης.

Ο κύριος στόχος για την κατασκευή της γλώσσας αυτής ήταν να περιορίζεται η πρόσβαση στα περιεχόμενα των αντικειμένων από τον δημιουργό του αντικειμένου, δηλαδή να ορίζει κατά τη δημιουργία του αντικείμενου ποιοι χρήστες έχουν δικαίωμα πρόσβασης στα περιεχόμενα του για ανάγνωση ή γραφή.

Η σύνταξη της PARWAL κτίζεται εφαρμόζοντας την σύνταξη π -calculus και δίνεται σε τρία επίπεδα, αντικειμένων, χρηστών και συστημάτων, που είναι βασισμένα σε ένα σύνολο από προθέματα και τελεστές.

Τα προθέματα έχουν την εξής σύνταξη:

$\alpha ::= \bar{a}(y)$	έξοδος σε κανάλι αντικειμένου
$ \quad a(y)$	είσοδος σε κανάλι αντικειμένου
$\beta ::= \bar{\beta}(y)$	έξοδος σε τυχαίο κανάλι
$ \quad \beta(y)$	είσοδος σε τυχαίο κανάλι
$ \quad \beta(v \ a) \ \bar{m} \ (a, wr, rr)$	δημιουργία νέου αντικειμένου

Οι διεργασίες έχουν την εξής σύνταξη:

$E ::= 0$	τερματισμός
$ \quad \alpha.E$	εκτέλεση προθέματος α και στη συνέχεια λειτουργεί ως το αντικείμενο E
$ \quad E + E$	μη ντετερμινιστική επιλογή

$P ::= 0$	τερματισμός
$ \quad \beta.P$	εκτέλεση προθέματος β και στη συνέχεια λειτουργεί ως τον χρήστη P
$ \quad P + P$	μη ντετερμινιστική επιλογή

$S ::= E^{a,wr,rr}$	αντικείμενο με αναγνωριστικό a δικαιώματα γραφής και ανάγνωσης wr και rr .
$ \quad P^u$	χρήστης με αναγνωριστικό u

$S \mid S$	παράλληλη σύνθεση διεργασιών
$(\nu a) S$	το κανάλι a είναι περιορισμένο για χρήση αποκλειστικά εντός του συστήματος S
$! m(a, wr, rr). E^{a, wr, rr}$	δημιουργία καινούργιου αντικειμένου

Η σημασιολογία περιγράφει τη λειτουργία της κάθε διεργασίας του συστήματος, μέσω ενός συνόλου από κανόνες οι οποίοι διατυπώνουν τα βήματα/μεταβάσεις που μπορεί να εκτελέσει κάθε τελεστής της γλώσσας.

Η σημασιολογία ορίζεται μέσω ενός συνόλου από κανόνες για κάθε επίπεδο της γλώσσας (αντικείμενο/ χρήστης/ σύστημα). Σε αυτούς τους κανόνες βασιστήκαμε για να δημιουργήσουμε την σημασιολογία και της δικής μας επέκτασης της PARWAL που παρουσιάζεται στο επόμενο κεφάλαιο.

Κεφάλαιο 4

Σύνταξη και Σημασιολογία της γλώσσας PARWAL

4.1 Γενική Περιγραφή γλώσσας	23
4.2 Σύνταξη	24
4.3 Σημασιολογία	28
4.4 Παράδειγμα	33

4.1 Γενική Περιγραφή Γλώσσας

Στο κεφάλαιο αυτό θα παρουσιάσουμε την πρώτη κύρια συνεισφορά της διπλωματικής αυτής εργασίας, που είναι η επέκταση της άλγεβρας διεργασιών PARWAL για δυναμική διαχείριση των δικαιωμάτων πρόσβασης στα αντικείμενα. Δηλαδή οι ιδιοκτήτες των αντικειμένων, αφού το κρίνουν σκόπιμο να έχουν την δυνατότητα να αλλάζουν τα δικαιώματα πρόσβασης για γραφή ή ανάγνωση κατά την διάρκεια της εκτέλεσης του συστήματος δυναμικά. Με αυτό τον τρόπο μια διεργασία/χρήστης θα μπορεί να αποκτήσει ή να χάσει πρόσβαση σε ένα αντικείμενο εφόσον το θεωρεί αναγκαίο ο ιδιοκτήτης/δημιουργός του αντικειμένου. Αυτή τη νέα γλώσσα την ονομάζουμε D-PARWAL.

Ένα σύστημα αποτελείται από ένα σύνολο από διεργασίες, τα αντικείμενα και τους χρήστες που έχουν τη δυνατότητα να επικοινωνήσουν μεταξύ τους, να δημιουργήσουν αντικείμενα, να στείλουν αντικείμενα σε άλλους χρήστες, να διαβάσουν το περιεχόμενο κάποιου αντικειμένου και να αλλάζουν το περιεχόμενο κάποιου αντικειμένου.

4.2 Σύνταξη

Σε αυτή την υποενότητα θα παρουσιάσουμε τη σύνταξη της γλώσσας D-PARWAL και θα επισημάνουμε τις διαφορές της από την PARWAL. Το σύνολο των αναγνωριστικών των χρηστών είναι το U και το σύνολο των αναγνωριστικών των αντικειμένων είναι το A . Για αντικείμενα του U γράφουμε $u, v, u_1, u_2 \dots$ και για αντικείμενα του A γράφουμε $a, b, a_1, a_2 \dots$. Το σύνολο των καναλιών για δημιουργία νέων αντικειμένων είναι το M και για τα αντικείμενα του γράφουμε $m, m_1, m_2 \dots$. Επιπρόσθετα υπάρχει ένα κανάλι με τα κανάλια των χρηστών που έχουν δικαίωμα αφαίρεσης χρηστών από τις λίστες wr και pr των αντικειμένων, Remove. Και τέλος υπάρχει ένα κανάλι με τα κανάλια των χρηστών που έχουν δικαίωμα πρόσθεσης χρηστών στις λίστες wr και pr των αντικειμένων, Add. Η ένωση των συνόλων U, A, M , Add και Remove είναι το σύνολο N των καναλιών ή ονομάτων της γλώσσας. Γράφουμε x, y, z για τα στοιχεία του N . Οι βασικές οντότητες της γλώσσας είναι τα κανάλια και χρησιμοποιούνται στις θέσεις εισόδου και εξόδου ή για να περαστούν ως αντικείμενα μέσω άλλων καναλιών.

Κάθε αντικείμενο έχει δύο λίστες δικαιωμάτων. Η μία λίστα δικαιωμάτων του κάθε αντικειμένου είναι για ανάγνωση (pr) και αναφέρεται στους χρήστες που έχουν το δικαίωμα για ανάγνωση των περιεχομένων του αντικειμένου. Η άλλη λίστα δικαιωμάτων του αντικειμένου είναι για γραφή (wr) και αναφέρεται στους χρήστες που έχουν το δικαίωμα για γραφή στα περιεχόμενα του αντικειμένου.

Για $x \in N$ γράφουμε

x : δηλώνοντας ότι το κανάλι χρησιμοποιείται σε θέση εισόδου,

$\bar{x}$: δηλώνοντας ότι το κανάλι χρησιμοποιείται σε θέση εξόδου,

$(v\ x)$: δηλώνοντας τη δημιουργία ενός νέου καναλιού με το όνομα x . Για να δημιουργηθεί αυτό το νέο κανάλι το όνομα x δεν πρέπει να χρησιμοποιείται ήδη στο σύστημα.

Για τη σύνταξη της γλώσσας χρησιμοποιούμε τρία επίπεδα, των αντικειμένων E , των χρηστών P και των συστημάτων S . Αυτά τα επίπεδα ορίζονται μέσω γραμματικών και βασίζονται στα εξής προθέματα:

- Τα προθέματα a αναφέρονται σε είσοδο, έξοδο και επεξεργασία πάνω σε κανάλια $a \in A$. Αυτά τα προθέματα χρησιμοποιούνται στο επίπεδο των

αντικειμένων E και περιλαμβάνουν προθέματα της μορφής $\bar{a}(y)$ που δηλώνουν την αποστολή του ονόματος $y \in N$ μέσω του καναλιού $a \in A$ και της μορφής $a(y)$ που δηλώνουν τη παραλαβή ενός ονόματος πάνω στο κανάλι $a \in A$ το οποίο θα αποθηκευτεί ως τιμή της μεταβλητής y . Επίσης περιλαμβάνουν και προθέματα της μορφής $add(x, wr', rr')$ και $remove(x, wr', rr')$ τα οποία χρησιμοποιούνται για πρόσθεση και αφαίρεση, αντίστοιχα, χρηστών στις λίστες δικαιωμάτων των αντικειμένων $wr, rr \subseteq U$.

- Τα προθέματα β αναφέρονται σε είσοδο και έξοδο πάνω σε οποιοδήποτε κανάλι $x \in N$. Αυτά τα προθέματα χρησιμοποιούνται στο επίπεδο των χρηστών και περιλαμβάνουν προθέματα της μορφής $\bar{m}(wr, rr)$ που χρησιμοποιούνται για τη δημιουργία νέων αντικειμένων και προσδιορίζουν τις λίστες δικαιωμάτων $wr, rr \subseteq U$. Επίσης περιλαμβάνουν και προθέματα της μορφής $\overline{add}(x, wr', rr')$ και $\overline{remove}(x, wr', rr')$ τα οποία χρησιμοποιούνται για πρόσθεση και αφαίρεση, αντίστοιχα, χρηστών στις λίστες δικαιωμάτων των αντικειμένων $wr, rr \subseteq U$.
- Το πρόθεμα "τ" είναι πρόθεμα της εσωτερικής ενέργειας.

Η γραμματική του επιπέδου των αντικειμένων E βασίζεται στις διεργασίες:

- Αδρανές αντικείμενο – 0
- Η διεργασία η οποία εκτελεί πρώτα το πρόθεμα a και στη συνέχεια λειτουργεί ως το αντικείμενο E , χρησιμοποιώντας τον τελεστή διαδοχής “.” – $a.E$
- Η διεργασία στην οποία εκτελείται μη-ντετερμινιστικά μια από τις επιλογές $E1$ και $E2$ – $E1 + E2$

Η γραμματική του επιπέδου των χρηστών P βασίζεται στις διεργασίες:

- Αδρανής χρήστης – 0
- Η διεργασία η οποία εκτελεί πρώτα το πρόθεμα β και στη συνέχεια λειτουργεί ως τον χρήστη P , χρησιμοποιώντας τον τελεστή διαδοχής “.” – $\beta.P$

Η γραμματική του επιπέδου του συστήματος ορίζεται ως εξής:

- Ένα αντικείμενο με αναγνωριστικό a , δημιουργό του αντικειμένου o , δικαιώματα γραφής wr και δικαιώματα ανάγνωσης rr , $E^{a,o,wr,rr}$

- Ένας χρήστης με αναγνωριστικό u , P^u
- Η παράλληλη σύνθεση πολλών τέτοιων διεργασιών $\text{System}|\text{System}$
- Η διεργασία $(\nu a)\text{System}$ στην οποία το κανάλι a είναι περιορισμένο για χρήση αποκλειστικά εντός του συστήματος System
- Η διεργασία $!m(a,wr,rr).E^{a,o,wr,rr}$, η οποία δημιουργεί καινούρια αντικείμενα κάθε φορά που λαμβάνει κατάλληλο μήνυμα στο κανάλι m

Στους πίνακες που ακολουθούν παρουσιάζεται η σύνταξη της γλώσσας.

Πίνακας 1: Σύνταξη γλώσσας D-PARWAL –Προθέματα

ΠΡΟΘΕΜΑΤΑ:		
$\alpha ::= \bar{a}(y)$		έξοδος σε κανάλι αντικειμένου
$a(y)$		είσοδος σε κανάλι αντικειμένου
$add(a, wr', rr')$		πρόσθεση σε κανάλι αντικειμένου
$remove(a, wr', rr')$		αφαίρεση σε κανάλι αντικειμένου
$\beta ::= \bar{x}(y)$		έξοδος σε τυχαίο κανάλι
$x(y)$		είσοδος σε τυχαίο κανάλι
$\overline{add}(a, wr', rr')$		πρόσθεση σε τυχαίο κανάλι
$\overline{remove}(a, wr', rr')$		αφαίρεση σε τυχαίο κανάλι
$(\nu a) \bar{m}(a, wr, rr)$		δημιουργία νέου αντικειμένου

Πίνακας 2: Σύνταξη γλώσσας D-PARWAL –Διεργασίες

Διεργασίες:		
$E ::= 0$		τερματισμός
$\alpha.E$		διαδοχή
$E + E$		επιλογή

$P ::= 0$	τερματισμός
$ \quad \beta.P$	διαδοχή
$S ::= E^{a,o,wr,rr}$	Αντικείμενο με αναγνωριστικό a
$ \quad P^u$	Χρήστης με αναγνωριστικό u
$ \quad S \mid S$	Παράλληλη σύνθεση διεργασιών
$ \quad (v \ a)S$	περιορισμός
$ \quad ! m(a, wr, rr). E^{a,o,wr,rr}$	Δημιουργία νέου αντικειμένου

Θα ορίσουμε κάποιες έννοιες τις οποίες θα χρησιμοποιήσουμε στη συνέχεια:

- Χρησιμοποιώντας το πρόθεμα εισόδου $x(y).P$ το όνομα y είναι αντικείμενο και δεσμεύεται για χρήση από τη διεργασία P και το x είναι το υποκείμενο. Στο πρόθεμα εξόδου $\bar{x}(y).P$ το όνομα y είναι αντικείμενο και δεν δεσμεύεται για χρήση από τη διεργασία P και το x είναι το υποκείμενο. Στο πρόθεμα της εσωτερικής ενέργειας δεν υπάρχει αντικείμενο και υποκείμενο. Στη περίπτωση του τελεστή για το περιορισμό $(v \ a)S$ το όνομα a δεσμεύεται για χρήση από τη διεργασία S . Ορίζουμε ένα σύνολο από δεσμευμένα ονόματα για τη διεργασία P που δεσμεύονται από το πρόθεμα εισόδου, $\text{bn}(P)$ και ένα σύνολο με τα ελεύθερα ονόματα της διεργασίας P , $\text{fn}(P)$. Αντίστοιχα ορίζουμε τα σύνολα για το τελεστή περιορισμού, $\text{bn}(a)$ και $\text{fn}(a)$ για τα δεσμευμένα και ελεύθερα ονόματα για το a .
- Για να συσχετίσουμε ένα όνομα/αναγνωριστικό με κάποιο άλλο χρησιμοποιούμε τη συνάρτηση αντικατάστασης. Γράφοντας $\{x/y\}$ ισχύει ότι αντικαθιστάται το όνομα y από το αναγνωριστικό x . Η αντικατάσταση μπορεί να εφαρμοστεί και σε ένα σύνολο $\{x_1 \dots x_n / y_1 \dots y_n\}$, και ισχύει ότι κάθε στοιχείο του συνόλου y_i συσχετίζεται με το αντίστοιχο στοιχείο του συνόλου x_i . Η εκτέλεση της αντικατάστασης όταν διενεργηθεί μια ενέργεια εισόδου από μία διεργασία του συστήματος, οπότε και οι τιμές που εισήχθησαν κατά την είσοδο αντικαθιστούνται κατάλληλα στις κατάλληλες μεταβλητές και διεργασίες.

4.3 Σημασιολογία

Σε αυτό το υποκεφάλαιο θα διατυπώσουμε τυπικά τη συμπεριφορά των τελεστών μέσω μιας αυστηρής σημασιολογίας η οποία θα περιγράφει τη λειτουργικότητα της κάθε διεργασίας του συστήματος, μέσω ενός συνόλου από κανόνες οι οποίοι διατυπώνουν τα βήματα/μεταβάσεις που ο κάθε τελεστής της γλώσσας D-PARWAL μπορεί να εκτελέσει.

Η σχέση μεταβάσεων της γλώσσας ορίζεται από τη σχέση $\rightarrow \subseteq S \times Act \times S$, όπου S το σύνολο όλων των διεργασιών που μπορούν να διατυπωθούν στη γλώσσα και Act το σύνολο όλων των ενεργειών που μπορούν να εκτελεστούν από τα συστήματα. Αντί να γράφουμε $(S, a, S') \in \rightarrow$ γράφουμε $S \xrightarrow{a} S'$ και το ερμηνεύουμε ως το σύστημα S μπορεί να εκτελέσει την ενέργεια a και μετά να εξελιχθεί στο σύστημα S' . Η ενέργεια $a \in Act$ μπορεί να έχει μία από τις ακόλουθες μορφές:

- $\bar{x}(id, y)$: η αποστολή του μηνύματος y μέσω του καναλιού x , προς το χρήστη με το αναγνωριστικό id .
- $x(id, y)$: η παραλαβή του μηνύματος y μέσω του καναλιού x , από το χρήστη με το αναγνωριστικό id .
- $add(y, id, wr', rr')$: η πρόσθεση των υποσυνόλων wr' και rr' στις λίστες δικαιωμάτων του αντικειμένου y μέσω του καναλιού add , από το δημιουργό του αντικειμένου με αναγνωριστικό id .
- $remove(y, id, wr', rr')$: η αφαίρεση των υποσυνόλων wr' και rr' από τις λίστες δικαιωμάτων του αντικειμένου y μέσω του καναλιού $remove$, από το δημιουργό του αντικειμένου με αναγνωριστικό id .
- $m(a, u, wr, rr)$: η δημιουργία νέου αντικειμένου με αναγνωριστικό a δημιουργό το χρήστη με αναγνωριστικό u και λίστες δικαιωμάτων wr και rr .
- τ : η εσωτερική ενέργεια η οποία εμφανίζεται όταν εκτελεστεί ταυτόχρονα μία είσοδος και μία έξοδος στο ίδιο κανάλι ή όταν δημιουργείται ένα καινούριο αντικείμενο.

Για διεργασίες χρηστών (αντικείμενα τύπου User) με αναγνωριστικά P^u ισχύουν οι ακόλουθοι κανόνες μετάβασης:

Πίνακας 3: Κανόνες Μετάβασης για αντικείμενα τύπου User

U ₁ :	$[x(y).P]^u \xrightarrow{x(u,z)} P\{z/y\}^u$
U ₂ :	$[\bar{x}(y).P]^u \xrightarrow{\bar{x}(u,y)} P^u$
U ₃ :	$[(va)\bar{m}(a,wr,rr).P]^u \xrightarrow{(va)\bar{m}(a,u,wr,rr)} P^u$
U ₄ :	$[\overline{add}(a,wr',rr').P]^u \xrightarrow{\overline{add}(a,u,wr',rr')} P^u$
U ₅ :	$[\overline{remove}(a,wr',rr').P]^u \xrightarrow{\overline{remove}(a,u,wr',rr')} P^u$

U₁: Η διεργασία $[x(y).P]^u$ μπορεί να εκτελέσει την ενέργεια $x(u, z)$ και να εξελιχθεί στη διεργασία $P\{z/y\}^u$ όπου η τιμή z που λήφθηκε μέσω της ενέργειας αντικατασταθείτε όπου y στη διεργασία P .

U₂: Η διεργασία $[\bar{x}(y).P]^u$ μπορεί να στείλει μέσω του καναλιού x την τιμή y σε οποιαδήποτε διεργασία για οποιοδήποτε αναγνωριστικό $v \in U$.

U₃: Η διεργασία $[(va)\bar{m}(a,wr,rr).P]^u$ δημιουργεί ένα καινούριο κανάλι αντικειμένου a το οποίο χρησιμοποιείται ως το όνομα ενός νέου αντικειμένου $E^{a,u,wr,rr}$. Το αντικείμενο αυτό είναι γνωστό μόνο στο δημιουργό του ο οποίος είναι ο χρήστης με αναγνωριστικό u που υλοποιείται μέσω του περιορισμού (va) .

U₄: Η διεργασία $[\overline{add}(a,wr',rr').P]^u$ προσθέτει τα σύνολα wr' και rr' στις λίστες δικαιωμάτων γραφής και ανάγνωσης, αντίστοιχα, του αντικειμένου a .

U₅: Η διεργασία $[\overline{remove}(a,wr',rr').P]^u$ αφαιρεί τα σύνολα wr και rr από τις λίστες δικαιωμάτων γραφής και ανάγνωσης, αντίστοιχα, του αντικειμένου a .

Για τις διεργασίες αντικειμένων ισχύουν οι ακόλουθοι κανόνες μετάβασης:

Πίνακας 4: Κανόνες Μετάβασης για Αντικείμενα

O₁:	$[a(x).E]^{a,o,wr,rr} \xrightarrow{a(id,z)} E\{z/x\}^{a,o,wr,rr}, \text{ if } id \in wr$
O₂:	$[\bar{a}(x).E]^{a,o,wr,rr} \xrightarrow{\bar{a}(id,x)} E^{a,o,wr,rr}, \text{ if } id \in rr$
O₃:	$[y(x).E]^{a,o,wr,rr} \xrightarrow{y(id,z)} E\{z/x\}^{a,o,wr,rr}, \text{ if } y \neq a$
O₄:	$[\bar{y}(x).E]^{a,o,wr,rr} \xrightarrow{\bar{y}(id,x)} E^{a,o,wr,rr}, \text{ if } y \neq a$
O₅:	$[add(a, wr', rr').E]^{a,o,wr,rr} \xrightarrow{add(a,o,wr',rr')} E^{a,o,(wr \cup wr'),(rr \cup rr')}$
O₆:	$[remove(a, wr', rr').E]^{a,o,wr,rr} \xrightarrow{remove(a,o,wr',rr')} E^{a,o,(wr - wr'),(rr - rr')}$
O₇:	$\frac{E_1^{a,o,wr,rr} \xrightarrow{\beta} (E_1')^{a,o,wr',rr'}}{(E_1 + E_2)^{a,o,wr,rr} \xrightarrow{\beta} (E_1')^{a,o,wr',rr'}}$
O₈:	$\frac{E_2^{a,o,wr,rr} \xrightarrow{\beta} (E_2')^{a,o,wr',rr'}}{(E_1 + E_2)^{a,o,wr,rr} \xrightarrow{\beta} (E_2')^{a,o,wr',rr'}}$

O₁,O₂: Αυτοί οι δύο κανόνες μετάβασης προσδιορίζουν ότι ένα αντικείμενο με αναγνωριστικό **a** μπορεί είτε να αλλοιωθεί είτε να διαβαστεί από οποιοδήποτε χρήστη έχει αναγνωριστικό **id** το οποίο ανήκει στα σύνολα δικαιωμάτων **wr** και **rr**.

O₃,O₄: Αυτοί οι δύο κανόνες δηλώνουν ότι όταν η επικοινωνία διενεργείται σε κανάλι διάφορο του αναγνωριστικού του αντικειμένου, τότε υλοποιείται χωρίς τους προαναφερθέντες περιορισμούς.

O₅,O₆: Αυτοί οι δύο κανόνες δηλώνουν ότι ένας χρήστης με αναγνωριστικό **o** μπορεί είτε να προσθέσει είτε να αφαιρέσει χρήστες από τις λίστες δικαιωμάτων του αντικειμένου **a**.

O₇, O₈: Οι δύο τελευταίοι κανόνες ερμηνεύουν ότι ο τελεστής + σε μια μη-ντετερμινιστική επιλογή, μπορεί να επιλεγθεί οποιαδήποτε από τις δύο συνιστώσες.

Και τέλος για τα συστήματα ισχύουν οι ακόλουθοι κανόνες μετάβασης:

Πίνακας 5: Κανόνες Μετάβασης για Συστήματα

$$\text{Res: } \frac{S \xrightarrow{(v a) \alpha} S'}{(v a) S \xrightarrow{\alpha} (v a) S'}, \text{ if } \text{subj}(\alpha) \neq a$$

$$\text{Rep: } ! m(a, wr, rr). E^{a, o, wr, rr} \xrightarrow{m(a', o', wr', rr')} E^{a', o', wr', rr'} \mid ! m(a, wr, rr). E^{a, o, wr, rr}$$

$$\text{P}_1: \frac{S_1 \xrightarrow{a} S_1'}{S_1 \mid S_2 \xrightarrow{a} S_1' \mid S_2}$$

$$\text{P}_2: \frac{S_2 \xrightarrow{a} S_2'}{S_1 \mid S_2 \xrightarrow{a} S_1 \mid S_2'}$$

$$\text{P}_3: \frac{S_1 \xrightarrow{a(id, y)} S_1' \quad S_2 \xrightarrow{\bar{a}(id, y)} S_2'}{S_1 \mid S_2 \xrightarrow{\tau} S_1' \mid S_2'}$$

$$\text{P}_4: \frac{S_1 \xrightarrow{x(u, y)} S_1' \quad S_2 \xrightarrow{\bar{x}(u, y)} S_2'}{S_1 \mid S_2 \xrightarrow{\tau} S_1' \mid S_2'} \text{ if } x \notin A$$

$$\text{P}_5: \frac{S_1 \xrightarrow{a(id, b)} S_1' \quad S_2 \xrightarrow{(v b) \bar{a}(id, b)} S_2'}{S_1 \mid S_2 \xrightarrow{\tau} (v b)(S_1' \mid S_2')}$$

$$\begin{array}{l}
\mathbf{P}_6: \frac{S_1 \xrightarrow{m(a,o,wr,rr)} S_1' \quad S_2 \xrightarrow{(v a) \bar{m}(a,o,wr,rr)} S_2'}{S_1 \mid S_2 \xrightarrow{\tau} (v a) (S_1' \mid S_2')} \\
\mathbf{P}_7: \frac{S_1 \xrightarrow{add(a,o,o,wr',rr')} S_1' \quad S_2 \xrightarrow{\overline{add}(a,o,wr',rr')} S_2'}{S_1 \mid S_2 \xrightarrow{\tau} S_1' \mid S_2'} \\
\mathbf{P}_8: \frac{S_1 \xrightarrow{remove(a,o,wr',rr')} S_1' \quad S_2 \xrightarrow{\overline{remove}(a,o,wr',rr')} S_2'}{S_1 \mid S_2 \xrightarrow{\tau} S_1' \mid S_2'}
\end{array}$$

Res: Ο κανόνας αυτός στη περίπτωση του τελεστή περιορισμού δηλώνει ότι αν ένα σύστημα S μπορεί να εκτελέσει τη μετάβαση $S \xrightarrow{\alpha} S'$, τότε το σύστημα με περιορισμένο το κανάλι a μπορεί να εκτελέσει την ενέργεια $(v a)\alpha$ μόνο αν η ενέργεια α δεν αφορά είσοδο ή έξοδο στο κανάλι a . Δηλαδή αν ισχύει ότι $subj(\alpha) \neq a$. Αν το κανάλι a δεν εμφανίζεται καθόλου μέσα στην ενέργεια α , τότε $(v a)\alpha = \alpha$.

Rep: Ο κανόνας αυτός στη περίπτωση του τελεστή δημιουργία αντικειμένου δηλώνει ότι κάθε φορά που η διεργασία $!m(a,wr,rr).E^{a,o,wr,rr}$ λαμβάνει κάποιο μήνυμα στο κανάλι m , τότε δημιουργεί ένα καινούριο αντικείμενο το οποίο συμπεριφέρεται ως τη συνέχεια E με τις παραμέτρους που λήφθηκαν στο μήνυμα.

Οι υπόλοιποι κανόνες ορίζουν πως λειτουργεί η σύνθεση δύο παράλληλων διεργασιών.

P₁, P₂: Αυτοί οι κανόνες δηλώνουν ότι αν μια από τις δύο διεργασίες μπορεί να εκτελέσει μια ενέργεια τότε η ίδια ενέργεια μπορεί να εκτελεστεί και από τη παράλληλη σύνθεση όπου η διεργασία που εκτέλεσε την ενέργεια εξελίσσεται κατάλληλα.

P₃, P₄: Αυτός ο κανόνας υλοποιεί την επικοινωνία ανάμεσα σε δύο διεργασίες στην περίπτωση όπου μια από αυτές λαμβάνει μήνυμα και η άλλη στέλλει μήνυμα στο ίδιο κανάλι. Το αποτέλεσμα αυτής της επικοινωνίας είναι η ενέργεια τ .

P₅, P₆: Αυτοί οι κανόνες ορίζουν τον τρόπο με τον οποίο το εύρος του περιορισμού ενός καναλιού μπορεί να διευρυνθεί όταν αυτό σταλεί ως μήνυμα σε μία διεργασία που δεν το γνωρίζει.

P₇, P₈: Αυτοί οι τελευταίοι κανόνες ορίζουν τον τρόπο με τον οποίο δύο διεργασίες, όπου η μία στέλνει μήνυμα επεξεργασίας στο κανάλι a και η άλλη λαμβάνει μήνυμα επεξεργασίας από το κανάλι a , επικοινωνούν μέσω της ενέργεια τ .

4.4 Παράδειγμα

Αφού παρουσιάσαμε τη σύνταξη και τη σημασιολογία της γλώσσας, θα δώσουμε ένα παράδειγμα για να εξηγηθεί καλύτερα η γλώσσα.

Το παράδειγμα αποτελείται από τον ορισμό μιας διεργασίας αντικειμένου $E^{a,o,wr,rr}\langle x \rangle$, τον ορισμό τριών διεργασιών χρήστη τους P^u , Q^v και R^w και τον ορισμό της διεργασίας του συστήματος.

Για τη κάθε διεργασία δίνουμε τις ενέργειες εισόδου, εξόδου, δημιουργίας νέου αντικειμένου, πρόσθεσης αλλά και αφαίρεσης χρηστών από τις λίστες δικαιωμάτων του αντικειμένου που έχουν δημιουργήσει. Οι διεργασίες για να προχωρήσουν στην εκτέλεση τους μπορούν να εκτελέσουν αυτές τις ενέργειες.

Στο παράδειγμα αυτό στόχος του συστήματος είναι να γίνει εφικτή η επικοινωνία μεταξύ των τριών διεργασιών και να διαβάσουν, να γράψουν και να προσθέσουν ή να αφαιρέσουν στις λίστες δικαιωμάτων στα δύο νέα αντικείμενα a και b που δημιουργούνται στο σύστημα. Θα μελετήσουμε κατά πόσον η διεργασία R^w θα μπορέσει να αποκτήσει πρόσβαση στα περιεχόμενα του αντικειμένου b για γραφή, με βάση τα δικαιώματα που του έχουν δοθεί όταν η διεργασία Q^v δημιουργήσει το νέο αντικείμενο b . Επίσης θα μελετήσουμε κατά πόσον η διεργασία R^w θα μπορέσει να αποκτήσει πρόσβαση στις λίστες δικαιωμάτων του αντικειμένου a και να αφαιρέσει χρήστες από αυτές, με βάση τα δικαιώματα επεξεργασίας που του έχουν δοθεί όταν η διεργασία P^u δημιούργησε το νέο αντικείμενο a .

$$C \stackrel{\text{def}}{=} !m(a, wr, rr). E^{a,o,wr,rr}\langle - \rangle$$

$$E\langle x \rangle \stackrel{\text{def}}{=} a(y).E\langle y \rangle + \bar{a}(x).E\langle x \rangle + add(x, wr', rr').E\langle x \rangle + remove(x, wr', rr').E\langle x \rangle$$

$$P \stackrel{\text{def}}{=} (v a)\bar{m}(a, \{u, v, w\}, \{u, v, w\}).u(b).\bar{a}(b).\bar{w}(a).0$$

$$Q \stackrel{\text{def}}{=} (v\ b)\bar{m}(b, \{u, v\}, \{u, v\}).\bar{b}(c).\bar{u}(b).\overline{add}(b, \{w\}, \{w\}).0$$

$$R \stackrel{\text{def}}{=} w(a)a(y).\bar{y}(z).\overline{remove}(a, \{v\}, \{v\}).0$$

$$\text{System} \stackrel{\text{def}}{=} (v\ u, v, w, m, add, remove)(C|P^u|Q^v|R^w)$$

Η διεργασία C δημιουργεί το νέο αντικείμενο με τα χαρακτηριστικά που θα λάβει από τη διεργασία τύπου χρήστη. Η διεργασία P^u είναι διεργασία τύπου χρήστη όπου αρχικά δημιουργεί νέο αντικείμενο με χαρακτηριστικό a . Αυτή η διεργασία έχει δικαίωμα να προσθέσει ή να αφαιρέσει χρήστες από τις λίστες δικαιωμάτων του αντικειμένου a , αφού ο χρήστης u είναι ο δημιουργός/ιδιοκτήτης του αντικειμένου. Επίσης μπορεί να διαβάσει τα περιεχόμενα των αντικειμένων a και b αλλά και να γράψει σε αυτά αφού το αναγνωριστικό του ανήκει στις λίστες δικαιωμάτων των δύο αντικειμένων. Η διεργασία Q^v είναι τύπου χρήστη που δημιουργεί ένα νέο αντικείμενο με χαρακτηριστικό b . Αυτή η διεργασία έχει δικαίωμα να προσθέσει ή να αφαιρέσει χρήστες από τις λίστες δικαιωμάτων του αντικειμένου b , αφού ο χρήστης v είναι ο δημιουργός/ιδιοκτήτης του αντικειμένου. Και αυτή η διεργασία μπορεί να διαβάσει τα περιεχόμενα των αντικειμένων a και b αλλά και να γράψει σε αυτά αφού το αναγνωριστικό του ανήκει στις λίστες δικαιωμάτων των δύο αντικειμένων. Η διεργασία R^w μπορεί να διαβάσει ή να γράψει στα περιεχόμενα του αντικειμένου a ενώ στα περιεχόμενα του αντικειμένου b δεν μπορεί να τα διαβάσει ή να γράψει γιατί δεν ανήκει στο σύνολο των λιστών του αντικειμένου b . Αν ο ιδιοκτήτης του αντικειμένου b δηλαδή ο χρήστης με αναγνωριστικό v προσθέσει τον χρήστη με αναγνωριστικό w στις λίστες δικαιωμάτων του αντικειμένου b .

Εκτελώντας τη εσωτερική ενέργεια ‘τ’ η διεργασία του συστήματος System μπορεί να εκτελέσει δύο πιθανές ενέργειες:

- Είτε η διεργασία $[(v\ a)\bar{m}(a, \{u, v, w\}, \{u, v, w\})]^u$ να επικοινωνήσει με τη διεργασία C μέσω του καναλιού a , με τη δημιουργία ενός νέου αντικειμένου $E^{a,u,\{u,v,w\},\{u,v,w\}}$ στο σύστημα.

$$C \mid [(v\ a)\bar{m}(a, \{u, v, w\}, \{u, v, w\}).u(b).\bar{a}(b).\bar{w}(a).0]^u \xrightarrow{\tau} (v\ a)(E_1 \mid [u(b).\bar{a}(b).\bar{w}(a).0]^u)$$

- Είτε η διεργασία $[(v\ b)\bar{m}(b, \{u, v\}, \{u, v\})]^v$ να επικοινωνήσει με τη διεργασία C μέσω του καναλιού b , με τη δημιουργία ενός νέου αντικειμένου $E^{b,v,\{u,v\},\{u,v\}}$ στο σύστημα.

$$C \mid [(v \ b)\overline{m}(b, \{u, v\}, \{u, v\}).\overline{b}(c).\overline{u}(b).0]^v \\ \xrightarrow{\tau} (v \ b)(E_2 \mid [\overline{b}(c).\overline{u}(b).\overline{add}(b, \{w\}, \{w\}).0]^v)$$

Με τις πιο πάνω μεταβάσεις δημιουργούνται δύο αντικείμενα τα E_1 και E_2 όπου $E_1 = E^{a,u,\{u,v,w\},\{u,v,w\}}\langle - \rangle$ και $E_2 = E^{b,v,\{u,v\},\{u,v\}}\langle - \rangle$. Το αντικείμενο E_1 έχει ως αναγνωριστικό το a , δημιουργό/ιδιοκτήτη το u και τις δύο λίστες με τα αναγνωριστικά των χρηστών με δικαίωμα γραφής και ανάγνωσης που αποτελούνται από τα αναγνωριστικά των διεργασιών $\{u,v,w\}$. Στο αντικείμενο a έχουν πρόσβαση για γραφή και ανάγνωση όλες οι διεργασίες του συστήματος με τα αναγνωριστικά u,v,w δηλαδή P , Q και R . Το αντικείμενο E_2 έχει ως αναγνωριστικό το b , δημιουργό ή ιδιοκτήτη το v και τις δύο λίστες με τα αναγνωριστικά των χρηστών με δικαίωμα γραφής και ανάγνωσης που αποτελούνται από τα αναγνωριστικά των διεργασιών $\{u,v\}$. Στο αντικείμενο b έχουν πρόσβαση για γραφή και ανάγνωση όλες οι διεργασίες του συστήματος με τα αναγνωριστικά u,v δηλαδή P και Q . Σε αυτό το αντικείμενο η διεργασία R δεν έχει δικαίωμα πρόσβασης.

Η εσωτερική ενέργεια τ εκτελείται κατά την επικοινωνία μεταξύ $(vb)(E_2\langle - \rangle \mid [\overline{b}(c).\overline{u}(b).\overline{add}(b, \{w\}, \{w\}).0]^v)$, όπου η τιμή c στέλνεται ως έξοδος μέσω του καναλιού b στη διεργασία με το αναγνωριστικό v . Το αντικείμενο b που έχει δημιουργηθεί θα μπορέσει να διαβάσει τα περιεχόμενα του c εφόσον το αναγνωριστικό v υπάρχει στη λίστα δικαιωμάτων για ανάγνωση του b , και αφού $v \in \{u, v\}$ θα μπορεί να διαβάσει τα περιεχόμενα του c . Τότε προκύπτει η ακόλουθη μετάβαση:

$$(v \ b)(E_2\langle - \rangle \mid [\overline{b}(c).\overline{u}(b).\overline{add}(b, \{w\}, \{w\}).0]^v) \\ \xrightarrow{\tau} (v \ b)(E_2\langle c \rangle \mid \overline{u}(b).\overline{add}(b, \{w\}, \{w\}).0)$$

Η διεργασία $[u(b).\overline{a}(b).\overline{w}(a).0]^u$ λαμβάνει ένα δεδομένο εισόδου μέσω της ενέργειας $u(u, b)$ όπου μέσω του καναλιού u παραλαμβάνεται το όνομα του αναγνωριστικού b και αφού ισχύει ότι $u \in \{u, v\}$ τότε το αναγνωριστικό της διεργασίας $[u(b).\overline{a}(b).\overline{w}(a).0]^u$ που είναι το u ανήκει στην λίστα wr .

$$(v \ a)(E_1\langle - \rangle \mid [u(b).\overline{a}(b).\overline{w}(a).0]^u) \xrightarrow{u(u,b)} (v \ a)(E_1\langle - \rangle \mid [\overline{a}(b).\overline{w}(a).0]^u)$$

Η διεργασία $[\bar{u}(b). \overline{add}(b, \{w\}, \{w\}). 0]^v$ εξελίσσεται στη διεργασία $[\overline{add}(b, \{w\}, \{w\}). 0]^v$ εκτελώντας την ενέργεια $\bar{u}(u, b)$ με τη μετάβαση:

$$[(v\ b)(E_2\langle c) | [\bar{u}(b). \overline{add}(b, \{w\}, \{w\}). 0]^v] \xrightarrow{\bar{u}(u, b)} (v\ b)(E_2\langle c) | [\overline{add}(b, \{w\}, \{w\}). 0]^v)$$

Στο επίπεδο του συστήματος προκύπτει η ακόλουθη μετάβαση:

$$(v\ a)(E_1\langle -) | [u(b). \bar{a}(b). \bar{w}(a). 0]^u \mid (v\ b)(E_2\langle c) | [\bar{u}(b). \overline{add}(b, \{w\}, \{w\}). 0]^v) \xrightarrow{\tau} (v\ a)(E_1\langle -) | [\bar{a}(b). \bar{w}(a). 0]^u \mid (v\ b)(E_2\langle c) | [\overline{add}(b, \{w\}, \{w\}). 0]^v)$$

Η διεργασία $[\overline{add}(b, \{w\}, \{w\}). 0]^v$ επικοινωνεί με τη διεργασία $E_2\langle c$ μέσω της ενέργειας τ για να αλλάξει τις λίστες δικαιωμάτων του αντικειμένου b και αφού ο χρήστης που επιθυμεί να κάνει αυτή την αλλαγή είναι ο v που είναι και ο δημιουργός του αντικειμένου τότε προκύπτει η διεργασία $E^{b, v, \{u, v, w\}, \{u, v, w\}}\langle c$ και η ανενεργή διεργασία 0 . Η μετάβαση που προκύπτει είναι:

$$(v\ b)(E_2\langle c) | [\overline{add}(b, \{w\}, \{w\}). 0]^v) \xrightarrow{\tau} (v\ b)(E'_2\langle c) | 0)$$

Η τιμή του b στέλνεται μέσω του καναλιού εξόδου a εκτελώντας την ενέργεια $\bar{a}(u, b)$ και προκύπτει η μετάβαση:

$$(v\ a)(E_1\langle -) | [\bar{a}(b). \bar{w}(a). 0]^u) \xrightarrow{\bar{a}(u, b)} (v\ a)(E_1\langle b) | [\bar{w}(a). 0]^u)$$

Επειδή το αναγνωριστικό u της διεργασίας P ανήκει στη λίστα για διάβασμα, $u \in \{u, v\}$ μπορεί να εκτελεστεί και έτσι προκύπτει η διεργασία:

$$(v\ u, v, w, m) (C | (v\ a)(v\ b)(E_1\langle b) | [\bar{w}(a). 0]^u | E_2\langle c) | 0) | R^w)$$

Εκτελώντας την ενέργεια $\bar{w}(w, a)$ αποστέλλεται το όνομα a μέσω του καναλιού w και η διεργασία τερματίζει. Η μετάβαση είναι:

$$(v\ a)(E_1\langle b) | [\bar{w}(a). 0]^u) \xrightarrow{\bar{a}(u, b)} (v\ a)(E_1\langle b) | 0)$$

Παράλληλα με τις άλλες διεργασίες η διεργασία R , μπορεί να δεχτεί τη τιμή a σαν δεδομένο εισόδου μέσω του καναλιού w . Αυτό φαίνεται από τη μετάβαση:

$$[w(a).a(y).\bar{y}(z).\overline{remove}(a, \{v\}, \{v\}).0]^w \\ \xrightarrow{w(w,a)} [a(y).\bar{y}(z).\overline{remove}(a, \{v\}, \{v\}).0]^w$$

Οι διεργασία του συστήματος εξελίσσεται ως εξής:

$(v\ u, v, w, m, add, remove)$

$$(C|(v\ a)(v\ b)(E_1\langle b\rangle|0|E_2\langle c\rangle|0|[a(y).\bar{y}(z).\overline{remove}(a, \{v\}, \{v\}).0])^w)$$

Στη συνέχεια μέσω της μετάβασης:

$[a(y).\bar{y}(z).\overline{remove}(a, \{v\}, \{v\}).0]^w \xrightarrow{a(w,y)} [\bar{b}(z).\overline{remove}(a, \{v\}, \{v\}).0]^w$, η τιμή y θα παραληφθεί μέσω του καναλιού a , και θα αντικατασταθεί το w από το y και οι διεργασίες θα εξελιχθούν ως εξής:

$(v\ u, v, w, m)$

$$(C|(v\ a)(v\ b)(E_1\langle b\rangle|0|E_1\langle c\rangle|0)|[\bar{b}(z).\overline{remove}(a, \{v\}, \{v\}).0]^w)$$

Από τη μετάβαση: $[\bar{b}(z).\overline{remove}(a, \{v\}, \{v\}).0]^w \xrightarrow{\bar{a}(w,z)} [\overline{remove}(a, \{v\}, \{v\}).0]^w$, η τιμή z αποστέλλεται μέσω του καναλιού a . Το αναγνωριστικό w του R βρίσκεται στις λίστες wr και rr του αντικειμένου a , άρα η διεργασία w μπορεί να διαβάσει ή να γράψει στο αντικείμενο με αναγνωριστικό a .

Και για το αντικείμενο b ισχύει αφού ο δημιουργός/ιδιοκτήτης του αντικειμένου τον έχει προσθέσει στις λίστες του αντικειμένου b . Έτσι η εσωτερική εκτελείται αφού δεν παραβιάζονται τα δικαιώματα του αντικειμένου $E'_2\langle z\rangle$ και οι διεργασίες θα εξελίσσονται ως εξής:

$(v\ u, v, w, m, add, remove)$

$$(C|(v\ a, b)(E_1\langle b\rangle|0|E_2\langle z\rangle|0)|[\overline{remove}(a, \{v\}, \{v\}).0]^w)$$

Τέλος με την επικοινωνία των διεργασιών $[\overline{remove}(a, \{v\}, \{v\}).0]^w$ και $E_1\langle b\rangle$ στην μετάβαση: $[\overline{remove}(a, \{v\}, \{v\}).0]^w \xrightarrow{\tau} 0$, ο χρήστης w μπορεί να αποκτήσει πρόσβαση στο αντικείμενο a αλλά δεν μπορεί να αλλάξει τις λίστες δικαιωμάτων του αφού δεν είναι ο ιδιοκτήτης ή δημιουργός του αντικειμένου a . Έτσι η εσωτερική ενέργεια δεν μπορεί να εκτελεστεί αφού παραβιάζονται τα δικαιώματα του αντικειμένου a .

Κεφάλαιο 5

Σύνταξη και Σημασιολογία της γλώσσας G-PARWAL

5.1 Γενική Περιγραφή γλώσσας	37
5.2 Σύνταξη	38
5.3 Σημασιολογία	41

5.1 Γενική Περιγραφή Γλώσσας

Στο κεφάλαιο αυτό θα παρουσιάσουμε την δεύτερη κύρια συνεισφορά της διπλωματικής αυτής εργασίας, που είναι η επέκταση της άλγεβρας διεργασιών PARWAL για διαχείριση των δικαιωμάτων πρόσβασης στα αντικείμενα μέσω ρόλων. Κάθε χρήστης έχει ένα ρόλο ο οποίος καθορίζει τα δικαιώματα που έχει ο χρήστης μέσα σε ένα σύστημα. Ένα παράδειγμα τέτοιου συστήματος είναι ένα σύστημα στο οποίο έχουμε ρόλους administrator, users και super-users, όπου ο ρόλος αυτών των χρηστών είναι διαφορετικός και όσοι έχουν τον ίδιο ρόλο εκτελούν τις ίδιες ενέργειες. Δηλαδή κάθε δημιουργός αντικειμένου κατά τη δημιουργία του αντικειμένου αποφασίζει πως θα χρησιμοποιείται ορίζοντας δύο λίστες δικαιωμάτων που περιέχουν τα ονόματα των ομάδων των χρηστών του συστήματος. Σε αυτές τις ομάδες επιτρέπεται η εγγραφή ή ανάγνωση στο αντικείμενο. Αυτές οι δύο λίστες είναι η wg (write groups) για τις ομάδες που έχουν δικαίωμα γραφής και rg (read groups) για τις ομάδες που έχουν δικαίωμα ανάγνωσης. Επίσης ο δημιουργός μπορεί οποιαδήποτε στιγμή να αλλάξει τις λίστες δικαιωμάτων του αντικειμένου είτε προσθέτοντας είτε αφαιρώντας ομάδες από τις λίστες αυτές.

Ένα σύστημα αποτελείται από ένα σύνολο από διεργασίες, τα αντικείμενα και τους χρήστες που έχουν τη δυνατότητα να επικοινωνήσουν μεταξύ τους, να δημιουργήσουν

αντικείμενα, να στείλουν αντικείμενα σε άλλους χρήστες και τις ομάδες χρηστών που έχουν τη δυνατότητα οι χρήστες που βρίσκονται σε αυτές τις ομάδες να διαβάσουν περιεχόμενο κάποιου αντικειμένου και να αλλάξουν περιεχόμενο κάποιου αντικειμένου. Αυτές οι ομάδες σχετίζονται με το ρόλο που έχουν οι χρήστες στο σύστημα. Ο ρόλος των χρηστών έχει σχέση με την ιδιότητα των χρηστών στο σύστημα και οι χρήστες χωρίζονται βάσει αυτής. Επίσης οι χρήστες που βρίσκονται σε κάθε ομάδα μπορούν να έχουν πρόσβαση όλοι στο ίδιο αντικείμενο αφού ο χρήστης που δημιούργησε το αντικείμενο έβαλε στις λίστες δικαιωμάτων του το όνομα της ομάδας τους.

5.2 Σύνταξη

Σε αυτή την υποενότητα θα παρουσιάσουμε τη σύνταξη της γλώσσας G-PARWAL. Η σύνταξη αυτής της γλώσσας δεν διαφέρει κατά πολύ από αυτή της γλώσσας PARWAL. Σε αυτή την παραλλαγή της γλώσσας PARWAL προσθέτουμε ένα νέο σύνολο το οποίο είναι οι ρόλοι που χωρίζονται οι χρήστες του συστήματος είναι το G και γράφουμε $g_1, g_2 \dots$. Κάθε χρήστης έχει ένα αναγνωριστικό u . Γράφουμε $u:g$ για να δείξουμε ότι ο χρήστης u έχει τον ρόλο g . Τώρα η ένωση των συνόλων U, A, M και G είναι το σύνολο N των καναλιών ή ονομάτων της γλώσσας. Γράφουμε x, y, z για τα στοιχεία του N . Οι βασικές οντότητες της γλώσσας και εδώ είναι τα κανάλια και τα ονόματα χρησιμοποιούνται στις θέσεις εισόδου, εξόδου, για επεξεργασία των δικαιωμάτων του αντικειμένου ή για να περαστούν ως αντικείμενα μέσω άλλων καναλιών.

Οι δύο λίστες των αντικειμένων αλλάζουν και πλέον αφορούν ομάδες χρηστών και όχι ατομικά τον κάθε χρήστη. Κάθε χρήστης με την είσοδο του στο σύστημα καταχωρείται σε μία ομάδα και βάση αυτής της ομάδας καθορίζονται τα δικαιώματα του σε κάθε αντικείμενο. Η μία λίστα δικαιωμάτων του κάθε αντικειμένου είναι για ανάγνωση (rg) και αναφέρεται στις ομάδες των χρηστών που έχουν το δικαίωμα για ανάγνωση των περιεχομένων του αντικειμένου και η άλλη λίστα δικαιωμάτων του αντικειμένου είναι για γραφή (wg) και αναφέρεται στις ομάδες των χρηστών που έχουν το δικαίωμα για γραφή στα περιεχόμενα του αντικειμένου.

Για $x \in N$ γράφουμε

x : δηλώνοντας ότι το κανάλι χρησιμοποιείται σε θέση εισόδου

$\bar{x}$: δηλώνοντας ότι το κανάλι χρησιμοποιείται σε θέση εξόδου

Για τη σύνταξη της γλώσσας χρησιμοποιούμε τρία επίπεδα, των αντικειμένων E , των χρηστών P και των συστημάτων S . Αυτά τα επίπεδα ορίζονται μέσω γραμματικών και βασίζονται στα εξής προθέματα που είναι όμοια με αυτά της γλώσσας D-PARWAL:

- Τα προθέματα a αναφέρονται σε είσοδο και έξοδο πάνω σε κανάλια $a \in A$. Αυτά τα προθέματα χρησιμοποιούνται στο επίπεδο των αντικειμένων E και περιλαμβάνουν προθέματα της μορφής $\bar{a}(y)$ που δηλώνουν την αποστολή του ονόματος $y \in N$ μέσω του καναλιού $a \in A$ και της μορφής $a(y)$ που δηλώνουν τη παραλαβή ενός ονόματος πάνω στο κανάλι $a \in A$ το οποίο θα αποθηκευτεί ως τιμή της μεταβλητής y
- Τα προθέματα β αναφέρονται σε είσοδο και έξοδο πάνω σε οποιοδήποτε κανάλι $x \in N$. Αυτά τα προθέματα χρησιμοποιούνται στο επίπεδο των χρηστών και περιλαμβάνουν προθέματα της μορφής $\bar{m}(wg, rg)$ που χρησιμοποιούνται για τη δημιουργία νέων αντικειμένων και προσδιορίζουν τις λίστες δικαιωμάτων $wr, rr \subseteq U$.
- Το πρόθεμα "τ" είναι πρόθεμα της εσωτερικής ενέργειας.

Η γραμματική του επιπέδου των αντικειμένων E βασίζεται στις διεργασίες:

- Αδρανές αντικείμενο – 0
- Η διεργασία η οποία εκτελεί πρώτα το πρόθεμα a και στη συνέχεια λειτουργεί ως το αντικείμενο E , χρησιμοποιώντας τον τελεστή διαδοχής $(.) - a.E$
- Η διεργασία στην οποία εκτελείτε μη-ντετερμινιστικά μια από τις επιλογές $E1$ και $E2$ – $E1+E2$

Η γραμματική του επιπέδου των χρηστών P βασίζεται στις διεργασίες:

- Αδρανής χρήστης – 0
- Η διεργασία η οποία εκτελεί πρώτα το πρόθεμα β και στη συνέχεια λειτουργεί ως τον χρήστη P , χρησιμοποιώντας τον τελεστή διαδοχής $(.) - \beta.P$

Η γραμματική του επιπέδου του συστήματος ορίζεται ως εξής:

- Ένα αντικείμενο με αναγνωριστικό α , δημιουργό του αντικειμένου o , δικαιώματα γραφής wg και δικαιώματα ανάγνωσης rg , $E^{\alpha,o,wg,rg}$
- Ένας χρήστης με αναγνωριστικό u , P^u
- Η παράλληλη σύνθεση πολλών τέτοιων διεργασιών $System \mid System$
- Η διεργασία $(\nu a)System$ στην οποία το κανάλι a είναι περιορισμένο για χρήση αποκλειστικά εντός του συστήματος $System$
- Η διεργασία $!m(a,wg,rg).E^{\alpha,o,wg,rg}$, η οποία δημιουργεί καινούρια αντικείμενα κάθε φορά που λαμβάνει κατάλληλο μήνυμα στο κανάλι m

Στους πίνακες που ακολουθούν παρουσιάζεται η σύνταξη της γλώσσας.

Πίνακας 6: Σύνταξη γλώσσας G-PARWAL –Προθέματα

ΠΡΟΘΕΜΑΤΑ:		
$\alpha ::= \bar{a}(y)$		έξοδος σε κανάλι αντικειμένου
$a(y)$		είσοδος σε κανάλι αντικειμένου
$\beta ::= \bar{x}(y)$		έξοδος σε τυχαίο κανάλι
$x(y)$		είσοδος σε τυχαίο κανάλι
$(\nu a) \bar{m}(a, wg, rg)$		δημιουργία νέου αντικειμένου

Πίνακας 7: Σύνταξη γλώσσας G-PARWAL –Διεργασίες

Διεργασίες:		
$E ::= 0$		τερματισμός
$\alpha.E$		διαδοχή
$E + E$		επιλογή
$P ::= 0$		τερματισμός
$\beta.P$		διαδοχή
$S ::= E^{\alpha,o,wg,rg}$		Αντικείμενο με αναγνωριστικό α
P^u		Χρήστης με αναγνωριστικό u

	$S \mid S$	Παράλληλη σύνθεση διεργασιών
	$(v \ a)S$	περιορισμός
	$! m(a, wg, rg). E^{a,o, wg, rg}$	Δημιουργία νέου αντικειμένου

5.3 Σημασιολογία

Σε αυτό το υποκεφάλαιο θα δώσουμε τη σημασιολογία η οποία περιγράφει τη λειτουργικότητα της κάθε διεργασίας του συστήματος, μέσω ενός συνόλου από κανόνες οι οποίοι διατυπώνουν τα βήματα/μεταβάσεις που ο κάθε τελεστής της γλώσσας G-PARWAL μπορεί να εκτελέσει.

Η σχέση μεταβάσεων της γλώσσας όπως και της γλώσσας PARWAL ορίζεται από τη σχέση $\rightarrow \subseteq S \times Act \times S$, όπου S το σύνολο όλων των διεργασιών που μπορούν να διατυπωθούν στη γλώσσα και Act το σύνολο όλων των ενεργειών που μπορούν να εκτελεστούν από τα συστήματα. Γράφουμε $S \xrightarrow{a} S'$ και το ερμηνεύουμε ως το σύστημα S μπορεί να εκτελέσει την ενέργεια a και μετά να εξελιχθεί στο σύστημα S' . Η ενέργεια $a \in Act$ μπορεί να έχει μία από τις ακόλουθες μορφές:

- $\bar{x}(id, y)$: η αποστολή του μηνύματος y μέσω του καναλιού x , προς όλους τους χρήστες που ανήκουν στην ομάδα με αναγνωριστικό id .
- $x(id, y)$: η παραλαβή του μηνύματος y μέσω του καναλιού x , από τους χρήστες που ανήκουν στην ομάδα με αναγνωριστικό id .
- $m(a, id, wg, rg)$: η δημιουργία νέου αντικειμένου με αναγνωριστικό a , ο χρήστη που δημιουργεί το αντικείμενο είναι ο χρήστης με αναγνωριστικό id και λίστες δικαιωμάτων wg και rg .
- τ : η εσωτερική ενέργεια η οποία εμφανίζεται όταν εκτελεστεί ταυτόχρονα μία είσοδος και μία έξοδος στο ίδιο κανάλι ή όταν δημιουργείται ένα καινούριο αντικείμενο.

Για διεργασίες χρηστών (αντικείμενα τύπου User) με αναγνωριστικά P^u ισχύουν οι ακόλουθοι κανόνες μετάβασης:

Πίνακας 8: Κανόνες Μετάβασης για αντικείμενα τύπου User

$U_1: [x(y).P]^u \xrightarrow{x(u,z)} P\{z/y\}^u$
$U_2: [\bar{x}(y).P]^u \xrightarrow{\bar{x}(u,y)} P^u$
$U_3: [(va)\bar{m}(a, wg, rg).P]^u \xrightarrow{(va)\bar{m}(a,u,wg,rg)} P^u$

U₁: Η διεργασία $[x(y).P]^u$ μπορεί να εκτελέσει την ενέργεια $x(u, z)$ και να εξελιχθεί στη διεργασία $P\{z/y\}^u$ όπου η τιμή z που λήφθηκε μέσω της ενέργειας αντικατασταθείτε όπου y στη διεργασία P .

U₂: Η διεργασία $[\bar{x}(y).P]^u$ μπορεί να στείλει μέσω του καναλιού x την τιμή y σε οποιαδήποτε διεργασία για οποιοδήποτε αναγνωριστικό v .

U₃: Η διεργασία $[(va)\bar{m}(a, wg, rg).P]^u$ δημιουργεί ένα καινούριο κανάλι αντικειμένου a το οποίο χρησιμοποιείται ως το όνομα ενός νέου αντικειμένου $E^{a,u,wg,rg}$. Το αντικείμενο αυτό είναι γνωστό μόνο στο δημιουργό του ο οποίος είναι ο χρήστης u που υλοποιείται μέσω του περιορισμού (va) .

Για τις διεργασίες αντικειμένων ισχύουν οι ακόλουθοι κανόνες μετάβασης:

Πίνακας 9: Κανόνες Μετάβασης για Αντικείμενα

$O_1: [a(x).E]^{a,o,wg,rg} \xrightarrow{a(id,z)} E\{z/x\}^{a,o,wg,rg}, id: R \text{ και } R \in wg \text{ ή } id = o$
$O_2: [\bar{a}(x).E]^{a,o,wg,rg} \xrightarrow{\bar{a}(id,x)} E^{a,o,wg,rg}, id: R \text{ και } R \in rg \text{ ή } id = o$

$$\mathbf{O}_3: [y(x).E]^{a,o,wg,rg} \xrightarrow{y(id,z)} E\{z/x\}^{a,o,wg,rg}, \text{ if } y \neq a$$

$$\mathbf{O}_4: [\bar{y}(x).E]^{a,o,wg,rg} \xrightarrow{\bar{y}(id,x)} E^{a,o,wg,rg}, \text{ if } y \neq a$$

$$\mathbf{O}_5: \frac{E_1^{a,o,wg,rg} \xrightarrow{\beta} (E_1')^{a,o,wg,rg}}{(E_1+E_2)^{a,o,wg,rg} \xrightarrow{\beta} (E_1')^{a,o,wg,rg}}$$

$$\mathbf{O}_6: \frac{E_2^{a,o,wg,rg} \xrightarrow{\beta} (E_2')^{a,o,wg,rg}}{(E_1+E_2)^{a,o,wg,rg} \xrightarrow{\beta} (E_2')^{a,o,wg,rg}}$$

O₁,O₂: Αυτοί οι δύο κανόνες μετάβασης προσδιορίζουν ότι ένα αντικείμενο με αναγνωριστικό a μπορεί είτε να αλλοιωθεί είτε να διαβαστεί από οποιοδήποτε χρήστη που το αναγνωριστικό του id ανήκει σε ομάδα η οποία ανήκει στα σύνολα δικαιωμάτων wg και rg ή είναι ο δημιουργός/ιδιοκτήτης του αντικειμένου.

O₃,O₄: Αυτοί οι δύο κανόνες δηλώνουν ότι όταν η επικοινωνία διενεργείται σε κανάλι διάφορο του αναγνωριστικού του αντικειμένου, τότε υλοποιείται χωρίς τους προαναφερθέντες περιορισμούς.

O₅,O₆: Οι δύο τελευταίοι κανόνες ερμηνεύουν ότι ο τελεστής $+$ σε μια μη-ντετερμινιστική επιλογή, μπορεί να επιλεχθεί οποιαδήποτε από τις δύο συνιστώσες.

Και τέλος για τα συστήματα ισχύουν οι ακόλουθοι κανόνες μετάβασης:

Πίνακας 10: Κανόνες Μετάβασης για Συστήματα

$$\mathbf{Res:} \frac{s \xrightarrow{(v a)\alpha} s'}{(v a)s \xrightarrow{\alpha} (v a)s'}, \text{ if } \text{subj}(\alpha) \neq a$$

Rep:

$$! m(a, wg, rg). E^{a,o,wg,rg} \xrightarrow{m(a',o,wg',rg')} E^{a',o,wg',rg'} \mid ! m(a, wg, rg). E^{a,o,wg,rg}$$

$$\begin{aligned}
\mathbf{P}_1: & \frac{S_1 \xrightarrow{a} S_1'}{S_1 \mid S_2 \xrightarrow{a} S_1' \mid S_2} \\
\mathbf{P}_2: & \frac{S_2 \xrightarrow{a} S_2'}{S_1 \mid S_2 \xrightarrow{a} S_1 \mid S_2'} \\
\mathbf{P}_3: & \frac{S_1 \xrightarrow{x(id,y)} S_1' \quad S_2 \xrightarrow{\bar{x}(id,y)} S_2'}{S_1 \mid S_2 \xrightarrow{\tau} S_1' \mid S_2'} \\
\mathbf{P}_5: & \frac{S_1 \xrightarrow{\alpha(id,b)} S_1' \quad S_2 \xrightarrow{(v b)\bar{a}(id,b)} S_2'}{S_1 \mid S_2 \xrightarrow{\tau} (v b)(S_1' \mid S_2')} \\
\mathbf{P}_6: & \frac{S_1 \xrightarrow{m(a,o,wg,rg)} S_1' \quad S_2 \xrightarrow{(v a)\bar{m}(a,o,wg,rg)} S_2'}{S_1 \mid S_2 \xrightarrow{\tau} (v a)(S_1' \mid S_2')}
\end{aligned}$$

Res: Ο κανόνας αυτός στη περίπτωση του τελεστή περιορισμού δηλώνει ότι αν ένα σύστημα S μπορεί να εκτελέσει τη μετάβαση $S \xrightarrow{\alpha} S'$, τότε το σύστημα με περιορισμένο το κανάλι a μπορεί να εκτελέσει την ενέργεια $(v a)\alpha$ μόνο αν η ενέργεια α δεν αφορά είσοδο ή έξοδο στο κανάλι a . Δηλαδή αν ισχύει ότι $subj(\alpha) \neq a$. Αν το κανάλι a δεν εμφανίζεται καθόλου μέσα στην ενέργεια α , τότε $(v a)\alpha = \alpha$.

Rep: Ο κανόνας αυτός στη περίπτωση του τελεστή δημιουργία αντικειμένου δηλώνει ότι κάθε φορά που η διεργασία $!m(a, wg, rg).E^{a,o,wg,rg}$ λαμβάνει κάποιο μήνυμα στο κανάλι m , τότε δημιουργεί ένα καινούριο αντικείμενο το οποίο συμπεριφέρεται ως τη συνέχεια E με τις παραμέτρους που λήφθηκαν στο μήνυμα.

Οι υπόλοιποι κανόνες ορίζουν πως λειτουργεί η σύνθεση δύο παράλληλων διεργασιών.

P₁, P₂: Αυτοί οι κανόνες δηλώνουν ότι αν μια από τις δύο διεργασίες μπορεί να εκτελέσει μια ενέργεια τότε η ίδια ενέργεια μπορεί να εκτελεστεί και από τη παράλληλη σύνθεση όπου η διεργασία που εκτέλεσε την ενέργεια εξελίσσεται κατάλληλα.

P₃: Αυτός οι κανόνες υλοποιούν την επικοινωνία ανάμεσα σε δύο διεργασίες στην περίπτωση όπου μια από αυτές λαμβάνει μήνυμα και η άλλη στέλλει μήνυμα στο ίδιο κανάλι. Το αποτέλεσμα αυτής της επικοινωνίας είναι η ενέργεια τ .

P₅, P₆: Αυτοί οι τελευταίοι κανόνες ορίζουν τον τρόπο με τον οποίο το εύρος του περιορισμού ενός καναλιού μπορεί να διευρυνθεί όταν αυτό σταλεί ως μήνυμα σε μία διεργασία που δεν το γνωρίζει.

Κεφάλαιο 6

Παράδειγμα Μελέτης

6.1 Παρουσίαση Παραδείγματος	46
6.2 Γράφος παραδείγματος	47
6.3 Σύνταξη Διεργασιών D-PARWAL	50
6.3.1 Παρουσίαση Παραδείγματος	51
6.3.2 Αξιολόγηση Παραδείγματος	54
6.4 Παρουσίαση Παραδείγματος G-PARWAL	54
6.4.1 Τι προβλήματα Ιδιωτικότητας προκύπτουν και γιατί;	55

6.1 Παρουσίαση Παραδείγματος

Στο κεφάλαιο αυτό θα παρουσιάσουμε την εφαρμογή των μεθοδολογιών που αναπτύξαμε στα δύο προηγούμενα κεφάλαια. Το παράδειγμα που θα παρουσιάσουμε είναι μία παραλλαγή του παραδείγματος της διδακτορικής διατριβής του Adam Barth [1], όπου δίνει την δυνατότητα στους ασθενείς και τους γιατρούς να ανταλλάξουν μηνύματα μέσω μίας διαδικτυακής εφαρμογής. Αυτή η εφαρμογή είχε ως στόχο την καλύτερη ιατρική βοήθεια με μειωμένο κόστος και περισσότερη ευκολία στον ασθενή διατηρώντας την ιδιωτικότητα ως προς τα προσωπικά δεδομένα του ασθενή είτε αυτά αφορούν την ερώτηση που θα κάνει στο γιατρό είτε τα στοιχεία του ραντεβού. Μέσω του συστήματος ο ασθενής έχει τη δυνατότητα να κάνει ερωτήσεις στους γιατρούς και να λάβει απαντήσεις, να κλείσει ραντεβού μέσω της γραμματέας και να λάβει τα αποτελέσματα του για κάποια εξέταση.

Στο παράδειγμα μελέτης που θα παρουσιάσουμε στόχος είναι να δίνεται η ευκαιρία στο χρήστη να θέσει ερωτήματα στους γιατρούς και να κλείσει ραντεβού και παράλληλα να ικανοποιούνται οι περιορισμοί ιδιωτικότητας του συστήματος. Κάθε φορά που ο

ασθενής δημιουργεί κάποιο αντικείμενο, δηλαδή μήνυμα, δηλώνει τις δύο λίστες δικαιωμάτων του μηνύματος που περιλαμβάνουν τα αναγνωριστικά των χρηστών που έχουν δικαίωμα ανάγνωσης ή γραφής του αντικειμένου. Επίσης για το Κεφάλαιο 4 και την γλώσσα D-PARWAL ο χρήστης που δημιουργεί το μήνυμα έχει το δικαίωμα να αλλάξει τις δύο λίστες, δηλαδή να προσθέσει ή να αφαιρέσει χρήστες από τις λίστες δυναμικά. Για τη γλώσσα G-PARWAL που παρουσιάζεται στο Κεφάλαιο 5 όλοι οι χρήστες είναι χωρισμένοι σε ομάδες βάσει του ρόλου που έχουν στο σύστημα και οι λίστες δικαιωμάτων δεν αφορούν χρήστες ατομικά αλλά ομάδες χρηστών. Στη G-PARWAL γλώσσα όμως λόγω του ότι οι χρήστες είναι χωρισμένοι σε ομάδες σε αυτό το σύστημα, το οποίο δεν είναι βασισμένο στο ρόλο του κάθε χρήστη, η ιδιωτικότητα του χρήστη δεν διασφαλίζεται απόλυτα.

Μέσω της γλώσσας που αναπτύξαμε στο Κεφάλαιο 4 βεβαιώνουμε ότι κανένα μήνυμα δεν μπορεί να διαβαστεί ή να επεξεργαστεί από κάποιο άτομο του οποίου το αναγνωριστικό του δεν ανήκει στις λίστες δικαιωμάτων του αντικειμένου, αλλά ούτε τα δικαιώματα του αντικειμένου να αλλαχτούν από κάποιο χρήστη ο οποίος δεν είναι ο ιδιοκτήτης/δημιουργός του. Και έτσι διασφαλίζουμε την ιδιωτικότητα των προσωπικών στοιχείων του χρήστη.

6.2 Γράφος Παραδείγματος

Ο γράφος και για τις δύο εκδοχές της γλώσσας αποτελείται από τέσσερις οντότητες/διεργασίες, τον ασθενή, τη νοσοκόμα, την γραμματέα και τον γιατρό και αντικείμενα τα οποία μπορεί να είναι είτε ραντεβού είτε μήνυμα είτε απάντηση.

Ασθενής:

Αρχικά η διεργασία ασθενής θα δημιουργήσει το αντικείμενο που είναι κάποιο μήνυμα και θα καθορίσει τις λίστες δικαιωμάτων του αντικειμένου. Στην περίπτωση που δημιουργήσει κάποιο μήνυμα τότε το προωθεί στη νοσοκόμα ή στη γραμματέα. Στη συνέχεια ο ασθενής θα παραλάβει την απάντηση από τη νοσοκόμα ή από τον γιατρό. Στην περίπτωση που ζητήσει από τη νοσοκόμα να κλείσει ραντεβού τότε θα παραλάβει επιβεβαίωση με τα στοιχεία του ραντεβού από τη γραμματέα. Παράλληλα με την εκτέλεση των πιο πάνω ενεργειών ο ασθενής έχει το δικαίωμα να αλλάξει τα δικαιώματα του αντικειμένου.

Νοσοκόμα:

Η διεργασία νοσοκόμα αφού παραλάβει το μήνυμα από κάποιο ασθενή τότε το προωθεί στο γιατρό για να απαντήσει στον ασθενή ή μπορεί να απαντήσει στον ασθενή και να του στείλει την απάντηση της. Επίσης η νοσοκόμα μπορεί να διαβάσει τα ραντεβού και να αλλάξει κάποια στοιχεία του και να ενημερώσει την γραμματέα.

Γραμματέας:

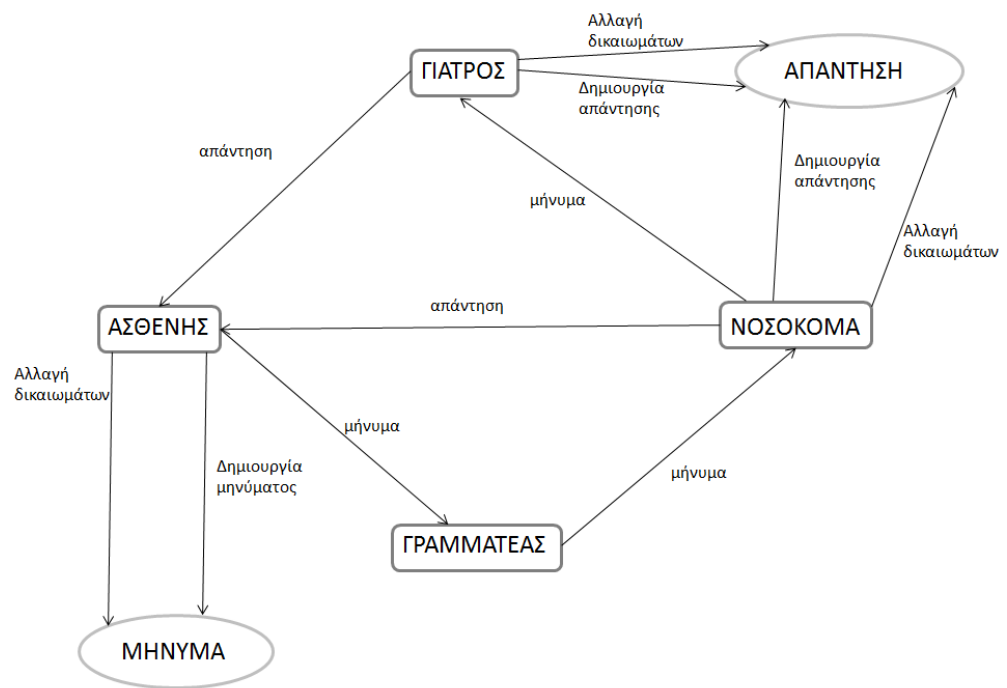
Η διεργασία γραμματέας είναι υπεύθυνη να μεταβιβάζει τα μηνύματα των ασθενών στη νοσοκόμα και να επιβεβαιώνει τα ραντεβού δημιουργώντας ένα αντικείμενο. Στην περίπτωση που λάβει κάποιο αίτηση για ραντεβού τότε δημιουργεί το ραντεβού και στέλνει τα στοιχεία του ραντεβού στον ασθενή.

Γιατρός:

Η διεργασία γιατρός είναι υπεύθυνη μόνο για να απαντά στα ερωτήματα των ασθενών. Αφού λάβει κάποιο μήνυμα από τη νοσοκόμα τότε το απαντά δημιουργώντας το αντικείμενο απάντηση και το στέλνει στον ασθενή.

Για την εκτέλεση του συστήματος ο χρήστης μπορεί να εκτελέσει 2 διαφορετικές πράξεις:

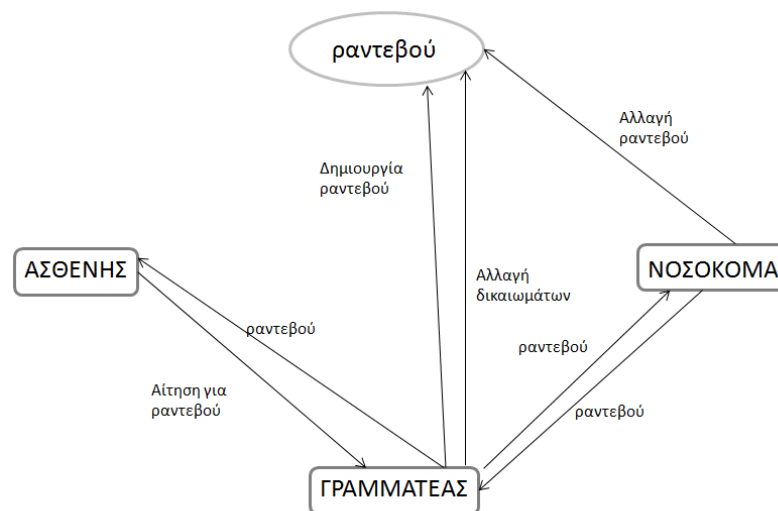
- **Σενάριο 1:** Ο ασθενής δημιουργεί ένα νέο αντικείμενο το οποίο είναι το μήνυμα στο οποίο αναφέρεται η ερώτηση του προς τον γιατρό. Το μήνυμα αυτό μπορούν να το διαβάσουν η νοσοκόμα και η γραμματέας και να το προωθήσουν στο γιατρό. Στο μήνυμα αυτό μπορούν να απαντήσουν είτε ο γιατρός είτε η νοσοκόμα δημιουργώντας ένα νέο αντικείμενο που θα είναι η απάντηση και την προωθούν στον ασθενή. Τις λίστες δικαιωμάτων αυτού του αντικειμένου έχει δικαίωμα μόνο ο ασθενής που το δημιούργησε να προσθέσει ή να αφαιρέσει χρήστες.



Εικόνα 2: Γράφος σεναρίου 1

- Σενάριο 2:** Ο ασθενής θέλει να κλείσει ραντεβού και η γραμματέας δημιουργεί ένα νέο αντικείμενο που είναι το ραντεβού στο οποίο δικαίωμα ανάγνωσης έχει ο χρήστης, η νοσοκόμα και η γραμματέας. Στο αντικείμενο ραντεβού δικαίωμα γραφής έχει η νοσοκόμα και η γραμματέας όπου μπορούν να αλλάξουν κάποια στοιχεία του ραντεβού. Τις λίστες δικαιωμάτων αυτού του αντικειμένου έχει δικαίωμα μόνο η γραμματέας που το δημιούργησε να προσθέσει ή να αφαιρέσει χρήστες.

Εικόνα 3: Γράφος σεναρίου 2



6.3 Σύνταξη Διεργασιών- D-PARWAL

Σε αυτό το υποκεφάλαιο θα δώσουμε τον ορισμό των διεργασιών χρησιμοποιώντας τη γλώσσα D-PARWAL.

Διεργασία Ασθενή (Patient)

Η διεργασία αυτή έχει ως αναγνωριστικό το u για να επικοινωνήσει με άλλες διεργασίες. Χρησιμοποιεί δύο παραμέτρους το t για να δηλώσει την ώρα που θέλει να κλείσει το ραντεβού και το q για να δηλώσει τις πληροφορίες του μηνύματος που θα κάνει.

Η διεργασία $Patient^u \langle t, q \rangle$ μπορεί να επιλέξει είτε να στείλει κάποιο ερώτημα ή να κλείσει ραντεβού με την πιο κάτω διεργασία:

$$Patient^u \langle t, q \rangle \stackrel{\text{def}}{=} Patient_{quest}^u \langle q \rangle | Patient_{app}^u \langle t \rangle$$

Η διεργασία $Patient_{quest}^u \langle q \rangle$ δημιουργεί το ερώτημα, γράφει το μήνυμα του και το στέλνει στη γραμματέα. Τέλος λαμβάνει την απάντηση από τη νοσοκόμα ή το γιατρό.

$$Patient_{quest}^u \langle q \rangle \stackrel{\text{def}}{=} (v \text{ quest}) \overline{m}(quest, \{u, n, d\}, \{u, n, d\}) \overline{quest}(q). \overline{squest}(quest). ans(a). 0$$

Η διεργασία στέλνει την ώρα του ραντεβού στη γραμματέα και λαμβάνει τις πληροφορίες του ραντεβού από τη γραμματέα.

$$Patient_{app}^u \langle t \rangle \stackrel{\text{def}}{=} \overline{sapp}(t). papp(app). 0$$

Διεργασία Γραμματέας (Secretary)

Η διεργασία αυτή χρησιμοποιεί το κανάλι με όνομα s για να επικοινωνήσει με τις άλλες διεργασίες.

$$Secretary^s \stackrel{\text{def}}{=} Secretary_{app}^s | Secretary_{quest}^s$$

Η γραμματέας αν λάβει ένα ερώτημα από τον ασθενή το προωθεί στη νοσοκόμα.

$$Secretary_{quest}^s \stackrel{\text{def}}{=} squest(quest). \overline{nquest}(quest). Secretary^s$$

Αλλιώς αν λάβει αίτηση για ραντεβού δημιουργεί το ραντεβού, γράφει τα στοιχεία του ραντεβού, το στέλνει στη νοσοκόμα για επιβεβαίωση ή αλλαγή της ώρας.

$Secretary_{app}^s$

$\stackrel{\text{def}}{=} sapp(t). (v\ app)\bar{m}(app, \{u, s, n, d\}, \{u, s, n, d\}). \overline{app}(t). \overline{napp}(app). nsapp(app). \overline{papp}(app). Secretary^s$

Διεργασία Νοσοκόμα (Nurse)

Η διεργασία αυτή χρησιμοποιεί το κανάλι με όνομα n για να επικοινωνήσει με άλλες διεργασίες.

$Nurse^n \stackrel{\text{def}}{=} Nurse_{app}^n \mid Nurse_{quest}^n$

Η νοσοκόμα λαμβάνει ένα μήνυμα από τον ασθενή είτε το προωθεί στο γιατρό είτε μπορεί να δημιουργήσει το αντικείμενο απάντηση, να γράψει την απάντηση και να το προωθήσει στον ασθενή.

$Nurse_{quest}^n \stackrel{\text{def}}{=} nquest(quest). (\overline{dquest}(quest). Nurse^n$
 $+ (v\ a)\bar{m}(a, \{n\}, \{u\}). \bar{a}(answer). \overline{ans}(a). Nurse^n)$

Η νοσοκόμα είτε θα αλλάξει την ώρα του ραντεβού που θα λάβει από τη γραμματέα είτε θα αλλάξει την ώρα του και μετά το προωθεί στη γραμματέα.

$Nurse_{app}^n \stackrel{\text{def}}{=} napp(app). (\overline{app}(t'). \overline{nsapp}(app). Nurse^n + \overline{psapp}(app). Nurse^n)$

Διεργασία Γιατρός (Doctor)

Η διεργασία αυτή χρησιμοποιεί το κανάλι με όνομα d για να επικοινωνήσει με άλλες διεργασίες. Ο γιατρός λαμβάνει ένα μήνυμα από νοσοκόμα και ο γιατρός δημιουργήσει το αντικείμενο απάντηση, γράφει την απάντηση και το προωθήσει στον ασθενή.

$Doctor^d \stackrel{\text{def}}{=} dquest(quest). (v\ a)\bar{m}(a, \{d, n\}, \{n, u\}). \bar{a}(answer). \overline{ans}(a). Doctor^d$

6.3.1 Παρουσίαση Παραδείγματος

Σενάριο 1: Αποστολή ερωτήματος

Ο ασθενής P^u αρχικά θα δημιουργήσει ένα αντικείμενο ερώτησης $quest$ και θα γράψει μέσα το ερώτημα του. Στη συνέχεια θα το στείλει στη γραμματεία S^s η οποία θα το προωθήσει στη νοσοκόμα. Η νοσοκόμα N^n θα το προωθήσει στο γιατρό D^d για να το απαντήσει. Ο γιατρός με τη σειρά του θα δημιουργήσει ένα νέο αντικείμενο απάντησης στο οποίο θα γράψει την απάντηση του και θα το προωθήσει στον ασθενή. Σε αυτό το σενάριο θα δείξουμε επίσης ότι ενώ η νοσοκόμα θα προσπαθήσει να αλλάξει τα δικαιώματα ανάγνωσης και γραφής του αντικειμένου ερώτησης που δημιούργησε ο ασθενής δεν θα μπορέσει να το κάνει αφού δεν είναι ο δημιουργός του αντικειμένου.

$$\begin{aligned}
C^{quest} &\stackrel{\text{def}}{=} !m(quest, \{u, n, d\}, \{u, n, d\}).E^{quest}\langle - \rangle \\
E^{quest}\langle - \rangle &\stackrel{\text{def}}{=} quest(q).E^{quest}\langle q \rangle + remove(quest, \{d\}, \{d\}).E^{quest}\langle q \rangle \\
C^a &\stackrel{\text{def}}{=} !m(a, \{n\}, \{u\}).E^a\langle - \rangle \\
E^a\langle - \rangle &\stackrel{\text{def}}{=} a(ans).E^a\langle answer \rangle
\end{aligned}$$

$$\begin{aligned}
P^u\langle q \rangle &\stackrel{\text{def}}{=} (v\ quest)\bar{m}(quest, \{u, n, d\}, \{u, n, d\}).\overline{quest}(q).\overline{squest}(quest).ans(a).0 \\
S^s &\stackrel{\text{def}}{=} squest(quest).\overline{nquest}(quest).0 \\
N^n &\stackrel{\text{def}}{=} nquest(quest).\overline{dquest}(quest).\overline{remove}(quest, \{d\}, \{d\}).0 \\
D^d &\stackrel{\text{def}}{=} dquest(quest).(v\ a)\bar{m}(a, \{n\}, \{u\}).\bar{a}(answer).\overline{ans}(a).0 \\
System &\stackrel{\text{def}}{=} (v\ u, s, n, d)(P^u \mid S^s \mid N^n \mid D^d)
\end{aligned}$$

Εκτελώντας το σύστημα προκύπτουν οι μεταβάσεις.

$$\begin{aligned}
&(v\ u, s, n, d)(P^u \mid S^s \mid N^n \mid D^d) \\
&\xrightarrow{\tau} (v\ u, s, n, d)((E_1\langle - \rangle \mid \overline{quest}(q).\overline{squest}(quest).ans(a).0) \mid S^s \mid N^n \mid D^d) \\
&\xrightarrow{\tau} (v\ u, s, n, d)((E_1\langle q \rangle \mid \overline{squest}(quest).ans(a).0) \mid S^s \mid N^n \mid D^d) \\
&\xrightarrow{\tau} (v\ u, s, n, d)((E_1\langle q \rangle \mid ans(a).0) \mid \overline{nquest}(quest).0 \mid N^n \mid D^d) \\
&\xrightarrow{\tau} (v\ u, s, n, d)((E_1\langle q \rangle \mid ans(a).0) \mid 0 \mid \overline{dquest}(quest).\overline{remove}(quest, \{d\}, \{d\}).0 \mid D^d) \\
&\xrightarrow{\tau} (v\ u, s, n, d)((E_1\langle q \rangle \mid ans(a).0) \mid 0 \mid \overline{remove}(quest, \{d\}, \{d\}).0 \mid (v\ a)\bar{m}(a, \{n\}, \{u\}).\bar{a}(answer).\overline{ans}(a).0) \\
&\xrightarrow{\tau} (v\ u, s, n, d)((E_1\langle q \rangle \mid ans(a).0) \mid 0 \mid \overline{remove}(quest, \{d\}, \{d\}).0 \mid (E_2\langle - \rangle \mid \bar{a}(answer).\overline{ans}(a)).0) \\
&\xrightarrow{\tau} (v\ u, s, n, d)((E_1\langle q \rangle \mid ans(a).0) \mid 0 \mid \overline{remove}(quest, \{d\}, \{d\}).0 \mid (E_2\langle answer \rangle \mid \overline{ans}(a)).0) \\
&\xrightarrow{\tau} (v\ u, s, n, d)((E_1\langle q \rangle \mid 0) \mid 0 \mid \overline{remove}(quest, \{d\}, \{d\}).0 \mid (E_2\langle answer \rangle \mid 0)) \\
&\xrightarrow{\tau} (v\ u, s, n, d)((E'_1\langle q \rangle \mid 0) \mid 0 \mid 0 \mid (E_2\langle answer \rangle \mid 0)), n \neq o_{quest}
\end{aligned}$$

$$\begin{aligned} \text{όπου } E_1\langle q \rangle &= E^{quest,u,\{u,n,d\},\{u,n,d\}}\langle q \rangle, E_2\langle q \rangle = E^{a,d,\{n\},\{u\}}\langle answer \rangle \text{ και } E'_1\langle q \rangle \\ &= E^{quest,u,\{u,n\},\{u,n\}}\langle q \rangle \end{aligned}$$

Η τελευταία εσωτερική ενέργεια δεν μπορεί να εκτελεστεί αφού παραβιάζονται τα δικαιώματα του αντικειμένου για επεξεργασία αφού η νοσοκόμα δεν είναι ο δημιουργός του αντικειμένου αλλά ο ασθενής. Έτσι το σύστημα δεν θα επιτρέψει στη νοσοκόμα να κάνει αυτή την αλλαγή στις λίστες δικαιωμάτων του ερωτήματος.

Σενάριο 2: Κλείσιμο ραντεβού

Ο ασθενής θα κάνει αίτηση για ραντεβού στη γραμματέα και αυτή με τη σειρά της θα δημιουργήσει ένα νέο αντικείμενο ραντεβού στο οποίο θα γράψει τα στοιχεία του ραντεβού και θα το στείλει στη νοσοκόμα η οποία θα αλλάξει την ώρα του ραντεβού και όταν το κάνει θα ενημερώσει την γραμματέα και αυτή τον ασθενή για την αλλαγή του ραντεβού. Στο τέλος η γραμματέας θα αλλάξει τα δικαιώματα του αντικειμένου ραντεβού για να προσθέσει και τον γιατρό.

$$\begin{aligned} C^{app} &\stackrel{\text{def}}{=} !m(app, \{u, s, n\}, \{u, s, n\}).E^{app}\langle - \rangle \\ E^{app}\langle - \rangle &\stackrel{\text{def}}{=} app(t).E^{app}\langle q \rangle + add(app, \{d\}, \{d\}).E^{app}\langle q \rangle \end{aligned}$$

$$\begin{aligned} P^u\langle t \rangle &\stackrel{\text{def}}{=} \overline{sapp}(t).papp(app).0 \\ S^s &\stackrel{\text{def}}{=} sapp(t).(v\ app)\overline{m}(app, \{u, s, n\}, \{u, s, n\}).\overline{app}(t).\overline{napp}(app).nsapp(app). \\ &\quad \overline{papp}(app).\overline{add}(app, \{d\}, \{d\}).0 \\ N^n\langle ap \rangle &\stackrel{\text{def}}{=} napp(app).\overline{app}(t').\overline{nsapp}(app).0 \\ System &\stackrel{\text{def}}{=} (v\ u, s, n, d)(P^u \mid S^s \mid N^n \mid D^d) \end{aligned}$$

Εκτελώντας το σύστημα προκύπτουν οι μεταβάσεις.

$$\begin{aligned} &(v\ u, s, n, d)(P^u \mid S^s \mid N^n \mid D^d) \\ &\xrightarrow{\tau} (v\ u, s, n, d)(papp(app).0 \mid (v\ app)\overline{m}(app, \{u, s, n\}, \{u, s, n\}).\overline{app}(t).\overline{napp}(app).nsapp(app). \\ &\quad \overline{papp}(app).\overline{add}(app, \{d\}, \{d\}).0 \mid N^n \mid D^d) \\ &\xrightarrow{\tau} (v\ u, s, n, d)(papp(app).0 \mid \left(E_1\langle - \rangle \mid \overline{app}(t).\overline{napp}(app).nsapp(app).\overline{papp}(app) \right) \\ &\quad \cdot \overline{add}(app, \{d\}, \{d\}).0 \mid N^n \mid D^d) \end{aligned}$$

$$\begin{aligned}
& \xrightarrow{\tau} (v\ u, s, n, d)(papp(app).0 \mid (E_1\langle t \rangle \mid \overline{napp}(app).nsapp(app).\overline{papp}(app).\overline{add}(app, \{d\}, \{d\}).0) \\
& \mid N^n \mid D^d) \\
& \xrightarrow{\tau} (v\ u, s, n, d)(papp(app).0 \mid (E_1\langle t \rangle \mid nsapp(app).\overline{papp}(app).\overline{add}(app, \{d\}, \{d\}).0) \\
& \mid \overline{app}(t').\overline{nsapp}(app).0 \mid D^d) \\
& \xrightarrow{\tau} (v\ u, s, n, d)(papp(app).0 \mid (E_1\langle t' \rangle \mid nsapp(app).\overline{papp}(app).\overline{add}(app, \{d\}, \{d\}).0) \\
& \mid \overline{nsapp}(app).0 \mid D^d) \\
& \xrightarrow{\tau} (v\ u, s, n, d)(papp(app).0 \mid (E_1\langle t' \rangle \mid \overline{papp}(app).\overline{add}(app, \{d\}, \{d\}).0) \mid 0 \mid D^d) \\
& \xrightarrow{\tau} (v\ u, s, n, d)(0 \mid (E_1\langle t' \rangle \mid \overline{add}(app, \{d\}, \{d\}).0) \mid 0 \mid D^d) \\
& \xrightarrow{\tau} (v\ u, s, n, d)(0 \mid (E'_1\langle t' \rangle \mid 0) \mid 0 \mid D^d) \\
& \text{όπου } E_1\langle t \rangle = E^{app, s, \{u, s, n\}, \{u, s, n\}}\langle t \rangle, \text{ και } E'_1\langle t \rangle = E^{app, s, \{u, s, n, d\}, \{u, s, n, d\}}\langle t \rangle
\end{aligned}$$

6.3.1 Αξιολόγηση Παραδείγματος

Στο παράδειγμα που παρουσιάσαμε πιο πάνω παρατηρούμε ότι ο ασθενής έχει την δυνατότητα να υποβάλει ένα ερώτημα ή να κλείσει ένα ραντεβού διατηρώντας τους κανόνες ιδιωτικότητας που ορίστηκαν στο σύστημα. Καμία διεργασία δεν μπορεί να επεξεργαστεί τις λίστες δικαιωμάτων ενός αντικειμένου εκτός και αν αυτή η διεργασία είναι η δημιουργός το υ αντικειμένου, οπότε το σύστημα σέβεται το ν κανόνα ιδιωτικότητας που έχει οριστεί.

Η γλώσσα D-PARWAL δίνει την δυνατότητα να οριστούν οι διεργασίες του συστήματος αλλά και οι κανόνες ιδιωτικότητας για δυναμική αλλαγή των λιστών δικαιωμάτων μόνο από το δημιουργό του αντικειμένου. Η γραμματική της γλώσσας μέσω των κανόνων στη σημασιολογία της επιτρέπει ή όχι την επεξεργασία των λιστών βάση της ιδιωτικότητας.

6.4 Παρουσίαση Παραδείγματος – G-PARWAL

Σενάριο 1: Αποστολή ερωτήματος

Ο ασθενής θα δημιουργήσει ένα ερώτημα το οποίο θα μπορούν να το διαβάσουν όλες ο νοσοκόμες και όλοι οι γιατροί αφού οι ομάδες τους ανήκουν στις λίστες δικαιωμάτων

του ερωτήματος. Μέχρι αυτό το σημείο δεν υπάρχει κάποιο πρόβλημα στην προστασία της ιδιωτικότητας των προσωπικών δεδομένων του ασθενή αφού ο ίδιος όρισε ποιες ομάδες έχουν δικαιώματα ανάγνωσης του ερωτήματος του. Το πρόβλημα δημιουργείται όταν είτε κάποια νοσοκόμα είτε κάποιος γιατρός δημιουργήσουν την απάντηση τους προς τον ασθενή όπου χρησιμοποιώντας την γλώσσα G-PARWAL δεν μπορούν να βάλουν στα δικαιώματα του αντικειμένου κάποιο χρήστη ατομικά αλλά θα πρέπει να υπάρχει όλη η ομάδα αφού η γλώσσα αυτή αναφέρεται σε ρόλους των χρηστών. Άρα δημιουργώντας το αντικείμενο της απάντησης για να μπορεί ο ασθενής που έκανε την ερώτηση να διαβάσει την απάντηση θα πρέπει να μπορούν όλοι οι ασθενείς να την διαβάσουν.

Σενάριο 2: Κλείσιμο ραντεβού

Ο ασθενής κάνει αίτηση για ραντεβού και η γραμματέας δημιουργεί ένα αντικείμενο ραντεβού στο οποίο καταχωρείται η ώρα του. Στο αντικείμενο αυτό δικαίωμα ανάγνωσης έχουν οι ομάδες των ασθενών, των νοσοκόμων και των γιατρών. Σε αυτό το σενάριο παραβιάζεται η ιδιωτικότητα του ασθενή γιατί μπορούν όλοι οι ασθενείς να μάθουν την ώρα του ραντεβού του αλλά θα μπορούσε να χρησιμοποιηθεί έτσι ώστε οι ασθενείς να μπορούν να ελέγχουν κατά πόσο υπάρχει κάποιο άλλο ραντεβού την συγκεκριμένη ώρα που επιθυμούν αυτοί κάποιο ραντεβού και εφόσον τα περιεχόμενα του ραντεβού είναι μόνο η ώρα του τότε οι υπόλοιποι οι ασθενείς δεν μπορούν να μάθουν περισσότερες πληροφορίες που αφορούν το ραντεβού.

6.4.1 Τι προβλήματα Ιδιωτικότητας προκύπτουν και γιατί;

Χρησιμοποιώντας την γλώσσα G-PARWAL στο παράδειγμα αυτό προκύπτουν προβλήματα ιδιωτικότητας όταν δημιουργείται ένα αντικείμενο το οποίο αφορά μόνο ένα συγκεκριμένο χρήστη και όχι όλους τους χρήστες που έχουν τον ίδιο ρόλο στο σύστημα. Κατά τη δημιουργία του αντικειμένου ορίζονται οι λίστες δικαιωμάτων του αντικειμένου που αφορούν τους ρόλους των χρηστών και όχι τον κάθε χρήστη ατομικά. Η γλώσσα G-PARWAL δεν δίνει την δυνατότητα σε ένα χρήστη ατομικά να έχει πρόσβαση σε ένα αντικείμενο εκτός και αν είναι ο δημιουργός του. Με αυτό τον τρόπο προκύπτουν προβλήματα ιδιωτικότητας γιατί κάποια αντικείμενα περιέχουν

προσωπικές πληροφορίες των ασθενών τις οποίες δεν πρέπει μπορούν να διαβάσουν άλλοι ασθενείς.

Τα προβλήματα αυτά προκύπτουν γιατί το σύστημα αυτό που είναι ένα σύστημα νοσοκομείου δεν βασίζεται μόνο στους ρόλους που έχουν οι χρήστες στο σύστημα αλλά και σαν ατομικές οντότητες. Δηλαδή επειδή τα περιεχόμενα των αντικειμένων είναι προσωπικές πληροφορίες που είναι αυστηρά εμπιστευτικές δεν γίνεται να μπορούν να διαβαστούν από οποιοδήποτε ασθενή. Αν τα αντικείμενα του συστήματος δεν είχαν αυτή την ιδιαιτερότητα, δηλαδή το σύστημα βασιζόταν στους ρόλους των χρηστών του, τότε δεν θα υπήρχε κάποιο πρόβλημα καταπάτησης της ιδιωτικότητας του ασθενή.

Κεφάλαιο 7

Συμπεράσματα

7.1 Συμπεράσματα	57
7.2 Μελλοντική Εργασία	58

7.1 Συμπεράσματα

Σε αυτή τη διπλωματική εργασία στόχος μας ήταν η επέκταση της γλώσσας PARWAL η οποία χρησιμοποιείται για την μοντελοποίηση συστημάτων που περιέχουν περιορισμούς ιδιωτικότητας. Η επέκταση D-PARWAL που έχει γίνει στη γλώσσα αυτή είναι για δυναμική αλλαγή των δικαιωμάτων ιδιωτικότητας των αντικειμένων σε ένα σύστημα όπου οι οντότητες μπορούν να δημιουργούν αντικείμενα να τα ανταλλάζουν μεταξύ τους και να μπορούν να διαβάσουν και να γράψουν στα περιεχόμενα των αντικειμένων. Η αλλαγή στα δικαιώματα ιδιωτικότητας των αντικειμένων θα μπορεί να γίνει μόνο στη περίπτωση που ο δημιουργός του αντικειμένου προσπαθήσει να την κάνει αλλιώς δεν θα ικανοποιούνται οι περιορισμοί ιδιωτικότητας που έχουν οριστεί στο σύστημα.

Η δεύτερη επέκταση G-PARWAL που έχει γίνει στη γλώσσα PARWAL στα πλαίσια της διπλωματικής αυτής ήταν οι χρήστες του συστήματος να είναι χωρισμένοι σε ομάδες ανάλογα του ρόλου τους και βάσει αυτού του ρόλου μπορούν να επικοινωνήσουν και να διαβάσουν ή να γράψουν στα περιεχόμενα του αντικειμένου.

Μέσα από παραδείγματα που μοντελοποιήσαμε με τις δύο επεκτάσεις, καταλήξαμε στο συμπέρασμα ότι η πρώτη επέκταση D-PARWAL είναι ικανή για να ορίσει διεργασίες του συστήματος καθώς και τους κανόνες ιδιωτικότητας. Η δεύτερη επέκταση G-PARWAL είναι ικανή και αυτή να ορίσει διεργασίες συστήματος το οποίο είναι

βασισμένο στους ρόλους των χρηστών μόνο. Δεν μπορούν οι κανόνες ιδιωτικότητας να οριστούν αν το σύστημα δεν είναι βασισμένο μόνο στους ρόλους γιατί θα καταπατώνται οι κανόνες ιδιωτικότητας όπως είδαμε και στο παράδειγμα του Κεφαλαίου 6.

7.2 Μελλοντική Εργασία

Η έρευνα σε ότι αφορά υλοποίηση γλωσσών για την επικοινωνία διεργασιών σε συστήματα που παρέχουν περιορισμούς ιδιωτικότητας δεν σταματά με το τέλος αυτής της διπλωματικής εργασίας.

Μπορούν να υπάρξουν βελτιώσεις όσο αφορά την γραμματική της γλώσσας D-PARWAL για επέκταση έτσι ώστε να υπάρχει έλεγχος για πρόσβαση στο περιεχόμενο του αντικειμένου. Δηλαδή το αντικείμενο θα χωρίζεται σε κομμάτια περιεχομένων τα οποία θα έχουν ένα μοναδικό χαρακτηριστικό και ο χρήστης που επιθυμεί να αποκτήσει πρόσβαση σε συγκεκριμένο κομμάτι του αντικειμένου θα πρέπει να αποκτήσει πρόσβαση στο αναγνωριστικό του συγκεκριμένου κομματιού. Με αυτό τον τρόπο δεν θα μπορεί να έχει πρόσβαση σε όλο το αντικείμενο.

Στη γλώσσα G-PARWAL θα μπορούσε να υπάρξει βελτίωση στη σύνταξη και σημασιολογία της έτσι ώστε να μην χρησιμοποιείται μόνο σε συστήματα που είναι βασισμένα στους ρόλους των χρηστών. Δηλαδή να υπάρχουν οι ομάδες των χρηστών που είναι ανάλογες των ρόλων τους αλλά να μπορούν και οι χρήστες να επικοινωνήσουν και ατομικά εκτός της ομάδας τους. Με αυτό τον τρόπο λύνουμε το πρόβλημα του παραδείγματος στο Κεφάλαιο 6. Ακόμη θα μπορούσε να γίνει και η επέκταση που δείξαμε στη γλώσσα D-PARWAL για δυναμική αλλαγή των δικαιωμάτων του αντικειμένου αλλά και για δυναμική αλλαγή των ρόλων των χρηστών στο σύστημα.

Βιβλιογραφία

- [1] A.Barth, “Design and Analysis of Privacy Policies”, Ph.D. dissertation, Stanford University, 2008.
- [2] A. F. Westin, Privacy and Freedom, 1967.
- [3] C.A. Petri, Kommunikation mit Automaten. English Tranlatio, 1966: Communication with Automata, Technical Report, Rome Air. Dev. Center, New York, 1962.
- [4] D. J. Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review, 2006. <http://ssrn.com/abstract=667622>
- [5] E. Bloustein. Privacy as an aspect of human dignity: An answer to dean prosser. New York University Law Review, 1964.
- [6] J.C.M. Baeten, A Brief History of Process Algebra, Journal Theoretical Computer Science- Process algebra, Volume 335 Issue 2-3, 2005.
- [7] J. J. Thomson, The Right to Privacy, Philosophy and Public Affairs, 1975
- [8] M.C.Tschantz, J.M.Wing, Formal Methods for Privacy, Carnegie Mellon University, 2009
- [9] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter, Enterprise Privacy Authorization Language (EPAL), Research Report, 2003.
- [10] R. Milner, The Polyadic π -calculus: a Tutorial, Laboratory for Foundations of Computer Science Department, University of Edinburgh, October 1991.

[11] Ruth Gavison. Privacy and the limits of law. Yale Law Journal, 1980.

[12] S. D. Warren, and L. D. Brandeis, The Right to Privacy, 1890.

[13] W. L. Posser, Privacy, California Law Review, 1960.

[14] Α. ΦΙΛΙΠΠΟΥ, “Άλγεβρες Διεργασιών”, Σημειώσεις μαθήματος ΕΠΛ 664-Ανάλυση και Επαλήθευση Συστημάτων, Τμήμα Πληροφορικής, Πανεπιστήμιο Κύπρου, 2011.

[15] Β. ΙΩΑΝΝΟΥ, “Ανάπτυξη τυπικής γλώσσας μοντελοποίησης συστημάτων με περιορισμούς ιδιωτικότητας και υλοποίηση εργαλείου προσομοίωσης”, ΔΙΑΤΡΙΒΗ ΜΕΤΑΠΤΥΧΙΑΚΟΥ, Τμήμα πληροφορικής, Πανεπιστήμιο Κύπρου, 2011.