ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΕΦΑΡΜΟΓΗ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ ΜΕ ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΜΕΘΟΔΟΥΣ

ΡΟΤΣΚΑΣ ΚΩΝΣΤΑΝΤΙΝΟΣ
ΑΝΑΝΙΑΔΗΣ ΑΝΤΩΝΙΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

…….. Λιουδάκης Γεώργιος ……..
……Εντεταλμένος Διδάσκων…….

Λαμία 12 Μαρ. 23

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΕΦΑΡΜΟΓΗ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ ΜΕ ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΜΕΘΟΔΟΥΣ

ΡΟΤΣΚΑΣ ΚΩΝΣΤΑΝΤΙΝΟΣ
ΑΝΑΝΙΑΔΗΣ ΑΝΤΩΝΙΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

.....Λιουδάκης Γεώργιος.....
..... Εντεταλμένος Διδάσκων .....

Λαμία 12 Μαρ. 23

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

ACCESS CONTROL ENFORCEMENT WITH CRYPTOGRAPHIC METHODS

ROTSKAS KONSTANTINOS
ANANIADIS ANTONIOS

FINAL THESIS

ADVISOR

……..Lioudakis George……..
……..Adjunct Lecturer…….

Lamia 12 March 2023

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ.), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 12/03/2023

Ο – Η Δηλ.

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Τα μοντέλα ελέγχου πρόσβασης έχουν εξελιχθεί πολύ με τα χρόνια και έχουν φτάσει στον λεγόμενο έλεγχο πρόσβασης βάσει χαρακτηριστικών. Το εγγενές πρόβλημα των μοντέλων ελέγχου πρόσβασης είναι ότι, ενώ είναι σε θέση να πάρουν απόφαση, δεν έχουν τη δυνατότητα να εφαρμόσουν την απόφαση αυτή παρά μόνο τοπικά. Το πλαίσιο αυτό μπορεί να βοηθήσει την κρυπτογραφία βάσει χαρακτηριστικών, αλλά δεν υπάρχουν εργαλεία που να μετατρέπουν από τον έλεγχο πρόσβασης στην κρυπτογραφία. Στο πλαίσιο της παρούσας πτυχιακής εργασίας αναπτύχθηκε εργαλείο το οποίο μετατρέπει από την γλώσσα XACML, σε κρυπτογραφικές δομές. Στην πτυχιακή αυτή παρουσιάζεται, επιπλέον, ο αλγόριθμος μετατροπής καθώς και η υλοποίηση του σε γλώσσα Java.

ABSTRACT

Access control models have evolved a lot over the years and have reached the so-called attribute-based access control. The inherent problem with access control models is that, while they are able to make a decision, they do not have the ability to enforce that decision except locally. This framework can help feature-based cryptography, but there are no tools that convert from access control to cryptography. In this thesis, a tool was developed that converts from the XACML language to cryptographic structures. In this thesis, the conversion algorithm and its implementation in Java language is also presented.

Table of Contents

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Ο έλεγχος πρόσβασης(Access Control) είναι ιδιαίτερα σημαντικός για την ασφάλεια πληροφοριών και την προστασία δεδομένων. Κάθε συμβάν ασφάλειας ή παραβίασης ιδιωτικότητας περιλαμβάνει αθέμιτη πρόσβαση σε κάποιον πόρο είτε σε δεδομένα είτε σε κάποιο σύστημα. Επομένως, ο έλεγχος πρόσβασης διαδραματίζει θεμελιώδη ρόλο στην ασφάλεια και την προστασία των δεδομένων. Στο πλαίσιο αυτό, οι τεχνολογίες ελέγχου πρόσβασης έχουν ωριμάσει και έχουν φτάσει στο απόγειο τους, που χαρακτηριστικά αποκαλείται έλεγχος πρόσβασης βάσει χαρακτηριστικών, δηλαδή Attribute Based Access Control (ABAC). Παρά την ωριμότητα τους, όμως, τα συστήματα αυτά έχουν τον εξής εγγενή περιορισμό: μολονότι ορίζουν επαρκώς «ποιος έχει πρόσβαση που» -μάλιστα με το ABAC γίνεται με πολύ λεπτομερή τρόπο, με χαρακτηριστικά του υποκειμένου, του αντικειμένου, του περιβάλλοντος- από τη στιγμή που τα δεδομένα εξαχθούν από μια βάση δεδομένων (database) χάνεται απολύτως ο έλεγχος πάνω σε αυτά. Συγκεκριμένα, αν κάποια δεδομένα εξαχθούν από μια βάση δεδομένων και σταλούν κάπου, ο έλεγχος πρόσβασης παύει να ισχύει, με άλλα λόγια ο έλεγχος πρόσβασης εφαρμόζεται πάνω σε ένα τοπικό επίπεδο. Σε αυτό το σημείο αναλαμβάνει δράση η κρυπτογραφία βάσει χαρακτηριστικών. Αυτή επιτρέπει τους κανόνες ελέγχου πρόσβασης, δηλαδή ποιος έχει δικαίωμα να προσπελάσει τα δεδομένα και γιατί. Με ποιον τρόπο, λοιπόν, η πολιτική αυτή δύναται να περαστεί μέσα στα δεδομένα. Η παρακάτω πτυχιακή εργασία λύνει το κενό αυτό κατασκευάζοντας ένα σύστημα μετατροπής.

Πιο συγκεκριμένα στο Δεύτερο Κεφαλαίο θα δοθεί έμφαση στο τι είναι ο έλεγχος πρόσβασης και τα διαφορετικά μοντέλα που τον αντιπροσωπεύουν με ιδιαίτερη προσοχή στον Έλεγχο Πρόσβασης Βάσει Χαρακτηριστικών, αλλά και με ποιον τρόπο εφαρμόζεται στα συστήματα. Κατόπιν στο Τρίτο Κεφάλαιο θα παρουσιαστεί η κρυπτογραφία βάσει χαρακτηριστικών και πιο συγκεκριμένα η CP-ABE (Ciphertext Policy-Attribute Based Encryption). Στο Τέταρτο Κεφάλαιο και το πιο σημαντικό από όλα θα δοθεί η θεωρία πίσω από την συνεργασία του Ελέγχου Πρόσβασης Βάσει Χαρακτηριστικών με την Κρυπτογράφηση Βάσει Χαρακτηριστικών, με ιδιαίτερη έμφαση στον αλγόριθμο μετατροπής από το ένα στο άλλο αντίστοιχα. Τέλος στο Πέμπτο Κεφάλαιο παρουσιάζεται ένα βασικό σύστημα υγείας το οποίο χρησιμοποιεί την συνεργασία που αναφέρθηκε πριν με στόχο την προστασία των ιατρικών απορρήτων των ασθενών.

ΚΕΦΑΛΑΙΟ 2 ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ

(2.1 ΕΙΣΑΓΩΓΗ)

Μια από τις πιο σημαντικές απαιτήσεις που χρειάζεται να έχει ένα σύστημα διαχείρισης πληροφοριών είναι να διαθέτει προστασία από κακόβουλους παράγοντες που έχουν ως στόχο την αποκάλυψη ή την τροποποίηση των πληροφοριών του συστήματος[2]. Ο έλεγχος πρόσβασης είναι μια θεμελιώδης τεχνολογία για την προστασία ενός συστήματος. Στην ουσία όπως λέει και ο τίτλος κάνει έλεγχο σε κάθε αίτημα πρόσβασης και καθορίζει αν θα πρέπει να εγκριθεί ή να απορριφθεί. Πιο συγκεκριμένα σε αυτά τα συστήματα ασφάλειας υπάρχει διαφοροποίηση ανάμεσα σε πολιτικές, μοντέλα και σε μηχανισμούς[6]. Αρχικά οι πολιτικές είναι υψηλού επιπέδου συντονιστές που αποφασίζουν τον τρόπο ελέγχων και προσβάσεων. Η πολιτική δημιουργείται μέσω ενός μοντέλου ασφάλειας και καθιερώνεται από τους μηχανισμούς ελέγχου πρόσβασης. Οι συγκεκριμένοι μηχανισμοί λαμβάνουν τις πληροφορίες του χρήστη που προσπαθεί να επιχειρήσει πρόσβαση στο σύστημα ενώ μετά συμβουλεύεται την βάση δεδομένων και ελέγχει αν υπάρχει ταύτιση στα στοιχεία μεταξύ τους με αποτέλεσμα να δοθεί ή όχι η εξουσιοδότηση για κάποια συγκεκριμένη λειτουργία του χρήστη πάνω στο σύστημα[2]. Σύμφωνα με την ταυτότητα των χρηστών φτιάχνονται και τα δεδομένα του κάθε χρήστη στην βάση. Αυτό με λίγα λόγια δηλώνει ότι ο έλεγχος πρόσβασης έχεις ως προϋπόθεση την αυθεντικοποιηση ή οποία γίνεται μέσω της εγγραφής του χρήστη με παράδοση ενός αναγνωριστικού και ενός κωδικού πρόσβασης. Οι εξουσιοδοτήσεις διαχειρίζονται από έναν διαχειριστή ασφάλειας ο οποίος τις ορίζει με βάσει την πολιτική ασφάλεια του οργανισμού. Βέβαια η χρήστες έχουν την δυνατότητα και αυτοί να τροποποιήσουν την βάση με τις εξουσιοδοτήσει αλλά μόνο ένα μέρος της, όπως για παράδειγμα τα προσωπικά τους αρχεία[6] .

Η πληθώρα και η συνθετότητα των απαιτήσεων προστασίας που μπορεί να χρειαστεί να εφαρμοστούν στα σημερινά συστήματα δεν είναι καθόλου εύκολη διαδικασία. Για παράδειγμα μια υπηρεσία μπορεί να μην χρειαστεί την πραγματική ταυτότητα ενός χρήστη αλλά μόνο κάποιες από τις ιδιότητες του (π.χ. ο χρήστης να σπουδάζει στην Ελλάδα). Τα πιο δημοφιλής συστήματα ελέγχου πρόσβασης είναι τα εξής.

Διακριτικός Έλεγχος Πρόσβασης (Discretionary Access Control - DAC): Δημιουργήθηκε από το Τμήμα Άμυνας της Αμερικής (Department of Defense - DoD) την δεκαετία 1960-70[6]. Στο συγκεκριμένο μοντέλο οι πολιτικές ελέγχου πρόσβασης ελέγχουν την είσοδο των χρηστών με βάση την ταυτότητα τους και τους κανόνες οι οποίοι καθορίζονται για κάθε υποκείμενο και αντικείμενο. Κάθε αίτημα ενός χρήστη για να πάρει άδεια πάνω σε ένα αντικείμενο εξετάζεται με βάση τις καθορισμένες εξουσιοδοτήσεις. Σε περίπτωση που υπάρχει τέτοια εξουσιοδότηση που να δίνει πρόσβαση στο αντικείμενο με συγκεκριμένη λειτουργία τότε η πρόσβαση πραγματοποιείται επιτυχώς, αλλιώς αποτυγχάνει. Ένα από τα σημαντικά προνομία που παρέχει το συγκεκριμένο μοντέλο ελέγχου πρόσβασης είναι ότι έχει την ικανότητα ένα υποκείμενο να μεταβιβάσει την άδεια σε ένα άλλο υποκείμενο για ένα συγκεκριμένο αντικείμενο[6].

Επιτακτικός Έλεγχος Πρόσβασης (Mandatory Access Control – MAC): Δημιουργήθηκε από το Τμήμα Άμυνας της Αμερικής (Department of Defense - DoD) την δεκαετία 1960-70[6]. Οι εν λόγω πολιτικές ρυθμίζουν την πρόσβαση με βάση την ταξινόμηση των υποκείμενων και των αντικειμένων στο σύστημα. Μια διαφορά αναμεσά στο συγκεκριμένο μοντέλο σε σχέση με το μοντέλο DAC είναι ότι τα υποκείμενα έχουν διαφορετική έννοια. Στο DAC τα υποκείμενα είναι εξουσιοδοτήσεις οι οποίες συμπίπτουν με χρήστες ή ομάδες χρηστών, ενώ στο MAC τα υποκείμενα είναι διεργασίες οι οποίες εκτελούνται για λογαριασμό των χρηστών. Κάθε αντικείμενο είναι συνδεδεμένο με ένα

υποκείμενο και αποθηκεύεται σαν μια κλάση αναφοράς. Πολλές κλάσεις αναφοράς δημιουργούν ένα διατεταγμένο σύνολο το οποίο έχει μια ιεραρχία. Συνήθως η ιεραρχία γίνεται με βάση το τελείως απόρρητο, το απόρρητο ,το εμπιστευτικό και τέλος το μη απόρρητο[6]. Στον διακριτό έλεγχο (DAC) πρόσβασης όπως προαναφέραμε πιο πάνω μπορεί να έχει την δυνατότητα να μοιράζει τις άδειες και να γίνεται πιο ευέλικτο σε σχέση με τον υποχρεωτικό έλεγχο πρόσβασης (MAC), γεγονός που το κάνει όμως και πιο εύκολο να παραβιαστεί. Για παράδειγμα ένα υποκείμενο το οποίο έχει την άδεια να διαγράφει δεδομένα μέσα στον οργανισμό, μπορεί να μοιράσει αυτή την άδεια σε άλλους χρήστες οι οποίοι δεν είναι εξουσιοδοτημένοι χωρίς να το ξέρει ο ιδιοκτήτης[6][2].

Έλεγχος Πρόσβασης Βάσει Ρόλου (Role Based Access Control – RBAC): Δημιουργήθηκε από τους D.F. Ferraiolo and D.R. Kuhn το 1992[6]. Η πρόσβαση ελέγχου βάσει ρόλου (RBAC) έχει την δυνατότητα να παρέχει εξουσιοδοτήσεις σε υποκείμενα τα οποία διαθέτουν έναν συγκεκριμένο ρόλο στο σύστημα[1][3]. Για να είναι λειτουργικό αυτό το μοντέλο απαιτεί να υπάρχουν 3 προϋποθέσεις. Πρώτη προϋπόθεση είναι ότι κάθε υποκείμενο υποχρεούται να διαθέτει έναν ρόλο είτε τον επιλέξει είτε του το αναθέσει κάποιο άλλο υποκείμενο[6]. Η σύνδεση στο σύστημα δεν αποτελεί λειτουργία η οποία ελέγχεται από το συγκεκριμένο μοντέλο. Δεύτερη προϋπόθεση είναι ότι κάθε ρόλος υποχρεούται να είναι έγκυρος για κάθε υποκείμενο[6]. Τρίτη προϋπόθεση και τελευταία είναι ότι ένα υποκείμενο για να εκτελέσει μια πράξη είναι αναγκαίο η πράξη να είναι εξουσιοδοτημένη μέσω των μελών ρόλων[6]. Αυτό έχει ως αποτέλεσμα να απλοποιεί σε μεγάλο βαθμό την διαδικασία διαχείρισης ελέγχου.

Έλεγχος Πρόσβασης Βάσει Χαρακτηριστικών (Attribute Based Access Control – ABAC): Η πρόσβαση ελέγχου βάσει χαρακτηριστικών είναι ένα καινούριο μοντέλο ελέγχου πρόσβασης σε σχέση με τα προαναφερθέντα μοντέλα. Παρακάτω σε αυτή την ενότητα θα αναλυθεί η λειτουργία του και ποια είναι τα οφέλη σε σχέση με τα προηγούμενα μοντέλα.

Access Control	**DAC**	**MAC**	**RBAC**	**ABAC**
Ευκολία Χρήστη	Υψηλή	Ανάλογα το σύστημα	Υψηλή	Υψηλή
Performance	Χαμηλή	Ανάλογα το σύστημα	Υψηλή	Υψηλή
Επαναχρησιμοποίηση	Πολλαπλή	-	Πολλαπλή	Πολλαπλή
Ανάθεση ρόλου	-	Εκχώρηση ενός Ρόλου	Πολλαπλή	-
Αποτυχία Ελέγχου Ταυτότητας	Μικρή	Ανάλογα το σύστημα	Με βάση την ανάθεση ρόλων εργασίας	Μικρή
Ιδιότητα	Το υποκείμενο με μια συγκεκριμένη άδεια έχει την δυνατότητα να μεταβιβάσει την άδεια αυτή σε ένα άλλο υποκείμενο.	Το υποκείμενο έχει πρόσβαση μόνο σε μια λειτουργία και δεν μπορεί να την μεταβιβάσει αλλού	Οι πολίτικες βασίζονται σε συγκεκριμένες ιδιότητες/ρόλους του υποκειμένου	Οι πολίτικες βασίζονται στα χαρακτηριστικά του υποκειμένου, αντικειμένου, δράσης, περιβάλλοντος

Πίνακας 2.1 Λειτουργικές Διαφορές Μοντέλων Πρόσβασης[22]

Επιπλέον σε αυτό τον κεφάλαιο θα διατυπωθεί η XACML (eXtensible Access Control Markup Language) γλώσσα η οποία είναι βασισμένη στην XML και λειτουργεί για να παράγει εξουσιοδοτήσεις ανάμεσα σε έναν οργανισμό.

(2.2 ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΒΑΣΕΙ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ - ABAC)

(2.2.1 ΤΑ ΒΑΣΙΚΑ ΤΟΥ ABAC)

Ο έλεγχος πρόσβασης βάσει χαρακτηριστικών είναι ένα μοντέλο εξουσιοδότησης με βάσει τα χαρακτηριστικά μιας οντότητας(Χαρακτηριστικά περιβάλλοντος, δράσης, αντικειμένων και χρηστών)[4]. Δημιουργήθηκε από τον οργανισμό Organization for the Advancement of Structured Information Standards (OASIS) το 2003.Τα χαρακτηριστικά χρηστών περιγράφουν τον χρήστη που επιχειρεί την πρόσβαση (π.χ. ηλικία, όνομα, βαθμό κλπ.).Τα χαρακτηριστικά δράσης δηλώνουν την ενέργεια που επιχειρείται(π.χ. διαγραφή, επεξεργασία, ανάγνωση κλπ.).Τα χαρακτηριστικά αντικειμένου είναι αυτά που περιγράφουν το αντικείμενο στο οποίο θα έχει πρόσβαση το υποκείμενο(π.χ. αρχείο ασθενή, τραπεζικός λογαριασμός κλπ.) και τέλος τα χαρακτηριστικά περιβάλλοντος τα οποία καθορίζουν την ώρα την τοποθεσία κτλ. [6][2]. Το ABAC για την αξιολόγηση κανόνων χρησιμοποιεί την δυαδική λογική Boolean, και στην συνέχεια αυτοί οι κανόνες ορίζουν το υποκείμενο το αίτημα και την ενέργεια. Για παράδειγμα αν το υποκείμενο είναι καρδιολόγος στο Γενικό Νοσοκομείο Λάμιας τότε επέτρεψε του να διαβάσει ή να επεξεργαστεί αρχεία ασθενών στο συγκεκριμένο τομέα και νοσοκομείο. Η κυβέρνηση των ΗΠΑ πλέον το έχει σαν υποχρεωτικό στόχο πάνω στην ασφάλεια των δεδομένων τους[4][6].

Παρακάτω παρουσιάζονται τα κυριότερα πλεονεκτήματα του συγκεκριμένου μοντέλου αλλά και το βασικότερο πρόβλημα που δημιουργείται.

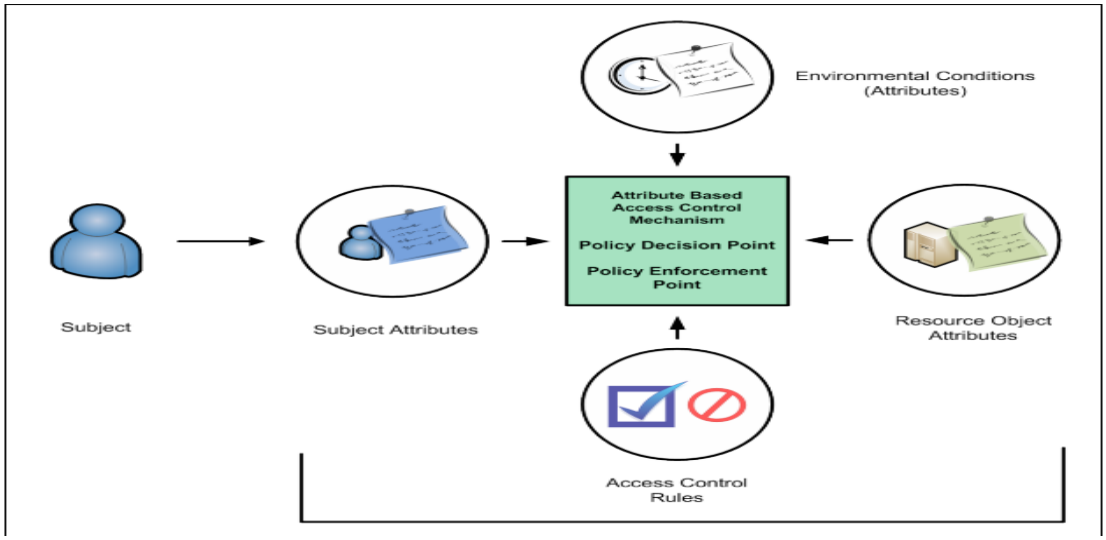
- Το κυριότερο πλεονέκτημα του ABAC σε σχέση με τα αλλά μοντέλα ελέγχου πρόσβασης και κυρίως με το RBAC είναι ότι στο συγκεκριμένο μοντέλο έχεις την ευελιξία να ελέγχεις σε πολύ μικρότερο χρονικό διάστημα λίστες ελέγχου από διάφορες ομάδες υποκειμένων. Αυτή η ιδιότητα ικανοποιεί σε μεγάλο βαθμό τις μεγάλες επιχειρήσεις καθώς τους γλυτώνει τεράστιο χρόνο[4].
- Ένα άλλο σημαντικό πλεονέκτημα είναι ότι είναι συμβατό με τα νέα υποκείμενα. Σε περίπτωση που μια επιχείρηση θέλει να εισάγει στο σύστημα τους ένα καινούριο υποκείμενο, δεν υποχρεώνεται να αλλάξει τους κανόνες για τον νέο υποκείμενο αρκεί απλά να εκχώρηση σε αυτό τα νέα του χαρακτηριστικά. Αυτό έχει ως αποτέλεσμα οι οργανισμοί να έχουν μια ευελιξία σχετικά με το προσωπικό τους αλλά και με εξωτερικούς συνεργάτες, καθώς δεν είναι ασυνήθιστο να βλέπουμε ένα υποκείμενο να αυθεντικοποιειται στον οργανισμό του τοπικά και στην συνέχεια να έχει εγκεκριμένη πρόσβαση σε εξωτερικούς οργανισμούς[6].
- Επιπλέον χάρη στην δυνατότητα των χαρακτηριστικών που διαθέτει, αυτομάτως γίνεται και πιο δυναμικό σε σχέση με αλλά μοντέλα όπως το RBAC που είναι πιο στατικό καθώς δεν υποστηρίζει αποφάσεις πολλών παραγόντων[4].

- Τέλος το ABAC παρέχει υψηλή ασφάλεια και απόρρητο επειδή παρέχει στον οργανισμό έξυπνες προσβάσεις. Για παράδειγμα ένας καρδιοχειρουργός θα έχει πρόσβαση σε ασθενείς με καρδιολογικά προβλήματα και μόνο[2][4][6].

Δυστυχώς όμως παρότι είναι αρκετά προσαρμόσιμο και ασφαλές εκεί που υστερεί είναι στον τρόπο εγκατάστασης του καθώς χρειάζεται να ορίσει ο οργανισμός εκατοντάδες έως και χιλιάδες χαρακτηριστικά και κανόνες με αποτέλεσμα να χρησιμοποιεί αρκετούς πόρους και χρόνο[4].

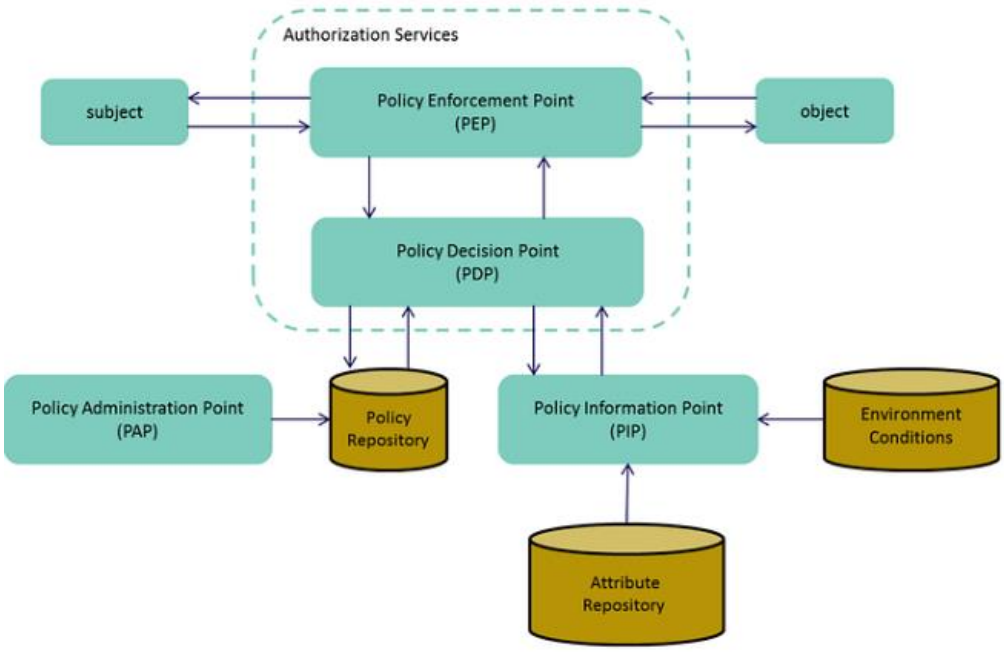
(2.2.3 Ο ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ ABAC)

Όπως είπαμε και παραπάνω το ABAC μοντέλο λειτουργεί με βάση τα χαρακτηριστικά ενός υποκείμενου, ενός αντικειμένου και ενός κανόνα που ορίζει την επιτρεπτή λειτουργία έτσι ώστε να συνδυαστούν μεταξύ τους υποκείμενο και αντικείμενο. Παρακάτω βλέπουμε την πιο βασική μορφή του ABAC και πως όλες οι οντότητες δουλεύουν αρμονικά για να παράξουν ένα ασφαλές σύστημα πληροφοριών.



Εικόνα 2.1 Βασική Αρχιτεκτονική ABAC[6]

Ο ρόλος του μηχανισμού ελέγχου πρόσβασης(ACM) του ABAC είναι να προστατεύει τα αντικείμενα οριοθετώντας την επιτρεπόμενη πρόσβαση μόνο από υποκείμενα που τα χαρακτηριστικά τους ταυτίζονται με μια πολιτική. Για να γίνει αυτό απαιτεί την ικανότητα να αναφερθούν με σωστή σειρά τα χαρακτηριστικά των αντικειμένων και των υποκείμενων, συμπεριλαμβανομένου και της ανάκτησης της πολιτικής[6]. Στην συνέχεια οφείλει να εκτελέσει τους υπολογισμούς από όλες τις πληροφορίες που έχει λάβει και να πάρει την απόφαση με βάση την λογική της πολιτικής που έλαβε πιο πριν. Όπως καταλαβαίνουμε λοιπόν η παρουσία του μηχανισμού ελέγχου πρόσβασης είναι αρκετά κρίσιμη για την επιτυχία ενός συστήματος ABAC[6]. Τα λειτουργικά τμήματα του μηχανισμού όπως είδαμε και στην Εικόνα 2.1 βρίσκονται μαζί. Αυτό όμως είναι για ένα πολύ βασικό σύστημα ABAC. Σε έναν οργανισμό οπού υπάρχουν χιλιάδες υποκείμενα και αντικείμενα τα λειτουργικά τμήματα είναι κατανεμημένα σε ολόκληρη την επιχείρηση. Παρακάτω βλέπουμε ένα πιο πολύπλοκο μηχανισμό ελέγχου που αντιπροσωπεύει έναν σύνθετο οργανισμό διαχείρισης πληροφοριών.



Εικόνα 2.2 Λειτουργικά μέρη ACM[9]

Στην Εικόνα 2.2 παρουσιάζονται τα κυριά λειτουργικά μέλη ενός μηχανισμού ελέγχου πρόσβασης. Πιο συγκεκριμένα το *σημείο πληροφοριών πολιτικής (PIP)* αποτελεί την προέλευση ανάκτησης των χαρακτηριστικών ή των δεδομένων που απαιτούνται για την εκτίμηση της πολιτικής ώστε να παρέχει τις πληροφορίες που χρειάζεται το PDP για την λήψη των αποφάσεων. Το *σημείο διαχείρισης πολίτικης(PAP)* είναι αυτό που διαθέτει στο υποκείμενο μια διεπαφή για την θέσπιση και διαχείριση των πολιτικών και την αποθήκευση αυτών στο αρμόδιο αρχείο. Κατόπιν έχουμε το *σημείο επιβολής πολιτικής (PEP)* οπού εξασφαλίζει τις αποφάσεις πολιτικής ως απάντηση σε ένα αίτημα ενός υποκείμενου που αιτείται πρόσβαση σε ένα προστατευόμενο αντικείμενο. Τέλος έχουμε το *σημείο λήψης αποφάσεων πολιτικής (PDP)* με ρολό την σύνταξη αποφάσεων πρόσβασης εκτιμώντας τις ισχύουσες πολιτικές του συστήματος. Μια από τις κυριότερες αρμοδιότητες του PDP είναι η διαμεσολάβηση ή η αποκατάσταση των πολιτικών.

(2.2.4 ΕΦΑΡΜΟΓΕΣ)

Το ABAC χρησιμοποιείται σε πολλές διαφορετικές εφαρμογές και οργανισμούς για τη διαχείριση και τη ρύθμιση της πρόσβασης σε πόρους. Ακολουθούν ορισμένες περιπτώσεις επιχειρήσεων και προγραμμάτων λογισμικού που κάνουν χρήση του ABAC:

1. Υγειονομική περίθαλψη: Το ABAC χρησιμοποιείται στον τομέα της υγειονομικής περίθαλψης για την επιβολή των νόμων περί προστασίας της ιδιωτικής ζωής, όπως ο Νόμος Φορητότητας και Λογοδοσίας Ασφάλισης Υγείας (Health Insurance and Accountability Act – HIPAA). Η πρόσβαση σε ιατρικούς φακέλους μπορεί να ελέγχεται με τη χρήση κανόνων ABAC, διασφαλίζοντας ότι μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση σε ευαίσθητα δεδομένα ασθενών.
2. Χρηματοοικονομικές υπηρεσίες: Για να περιορίσουν την πρόσβαση σε εμπιστευτικά οικονομικά δεδομένα και συναλλαγές, οι χρηματοπιστωτικοί οργανισμοί χρησιμοποιούν το ABAC. Οι κανόνες ABAC μπορούν να

χρησιμοποιηθούν για την τήρηση νόμων όπως το Πρότυπο ασφάλειας δεδομένων βιομηχανίας καρτών πληρωμής (Payment Card Industry Data Security Standard - PCI DSS) και για τη διακοπή της μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα οικονομικά δεδομένα[10][12].

3. Κυβέρνηση: Προκειμένου να εφαρμόσουν κανονισμούς ασφαλείας και να περιορίσουν την πρόσβαση σε ευαίσθητες πληροφορίες, οι κυβερνητικοί φορείς χρησιμοποιούν ABAC. Το ABAC μπορεί να χρησιμοποιηθεί για τη διασφάλιση της συμμόρφωσης με κανόνες όπως ο Ομοσπονδιακός νόμος εκσυγχρονισμού της ασφάλειας πληροφοριών (Federal Information Security Modernization Act – FISMA), καθώς και με πρότυπα ασφαλείας για την πρόσβαση σε ευαίσθητες πληροφορίες, όπως απόρρητα έγγραφα[6][12].
4. Cloud computing: Το ABAC χρησιμοποιείται σε περιβάλλον υπολογιστικού νέφους για τη ρύθμιση της πρόσβασης σε πόρους νέφους. Οι έλεγχοι πρόσβασης για εφαρμογές που βασίζονται στο υπολογιστικό νέφος και την αποθήκευση στο υπολογιστικό νέφος μπορούν να επιβληθούν με τη βοήθεια κανόνων ABAC[10][12].
5. Εφαρμογές για την επιχείρηση: Το ABAC χρησιμοποιείται σε εφαρμογές για την επιχείρηση για τη διαχείριση της πρόσβασης σε πόρους, συμπεριλαμβανομένων των βάσεων δεδομένων, των συστημάτων αρχείων και των υπηρεσιών ιστού. Οι κανόνες ABAC μπορούν να χρησιμοποιηθούν για τη ρύθμιση της πρόσβασης σε ευαίσθητες πληροφορίες, όπως δεδομένα πελατών, και για την επιβολή περιορισμών πρόσβασης βάσει ρόλων[2][6].

Αυτές είναι μερικές μόνο περιπτώσεις επιχειρήσεων και προγραμμάτων που χρησιμοποιούν το ABAC. Το ABAC μπορεί να χρησιμοποιηθεί σε διάφορα πλαίσια και κλάδους χάρη στην προσαρμοστικότητά του.

(2.2.5 ΣΥΜΠΕΡΑΣΜΑΤΑ)

Εν κατακλείδι, έπειτα από εξέταση όλων των συστημάτων ελέγχου πρόσβασης, απορρέει το συμπέρασμα ότι το μέλλον στα μοντέλα αυτά είναι το μοντέλο Βάση Χαρακτηριστικών (ABAC), καθώς και ο τρόπος με τον οποίο υλοποιείται και εγκαθίσταται. Παρόλα αυτά, αν και είναι αρκετά δυναμικό σε σχέση με τα άλλα μοντέλα, δεδομένου ότι χρησιμοποιεί αρκετούς πόρους, δεν είναι ιδιαίτερα αναγκαίο να εγκατασταθεί σε συστήματα των οποίων πρωταρχικός στόχος δεν είναι η προστασία κάποιων δεδομένων ή είναι αρκετά μικρά και απλά από άποψη λειτουργίας.

(2.3 XACML)

(2.3.1 ΤΙ ΕΙΝΑΙ Η XACML)

Ένα ευέλικτο και συμβατό framework για τη διαχείριση πολιτικών εξουσιοδότησης σε διάφορες καταστάσεις παρέχεται από την eXtensible Access Control Markup Language (XACML), ένα πρότυπο ελέγχου πρόσβασης βασισμένο σε XML. Ως ανοιχτό πρότυπο για τον έλεγχο πρόσβασης βάσει πολιτικών, η XACML δημιουργήθηκε και τυποποιήθηκε από την Organization for the Advancement of Structured Information Standards (OASIS). Με το XACML, οι πολιτικές εξουσιοδότησης μπορούν να εκφραστούν με συνέπεια και διαλειτουργικότητα και τα αιτήματα πρόσβασης μπορούν να αξιολογηθούν. Οι κανονισμοί XACML με βάση την XML καθορίζουν τις συνθήκες υπό τις οποίες πρέπει να επιτρέπεται ή να απαγορεύεται η πρόσβαση σε πόρους. Μια ολοκληρωμένη αρχιτεκτονική εξουσιοδότησης μπορεί να δημιουργηθεί συνδυάζοντας και τροποποιώντας τις πολιτικές, παρέχοντας στις επιχειρήσεις μια ευέλικτη προσέγγιση για το χειρισμό του ελέγχου πρόσβασης σε ολόκληρο τον οργανισμό τους. Ο συνδυασμός πολιτικών και η αξιολόγηση των πολιτικών είναι τα δύο βασικά στάδια της διαδικασίας αξιολόγησης των πολιτικών XACML. Οι πολιτικές συγχωνεύονται στη φάση του συνδυασμού πολιτικών για να παρέχουν μια ενιαία απόφαση πολιτικής που χρησιμοποιείται για την αξιολόγηση ενός αιτήματος πρόσβασης. Για τη λήψη της τελικής απόφασης πρόσβασης, η φάση αξιολόγησης πολιτικής λαμβάνει υπόψη τις ιδιότητες του αιτήματος πρόσβασης καθώς και την επιλογή που έγινε κατά τη φάση συνδυασμού πολιτικής.

(2.3.2 Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΑΙ ΣΧΕΔΙΑΣΜΟΣ ΤΗΣ XACML)

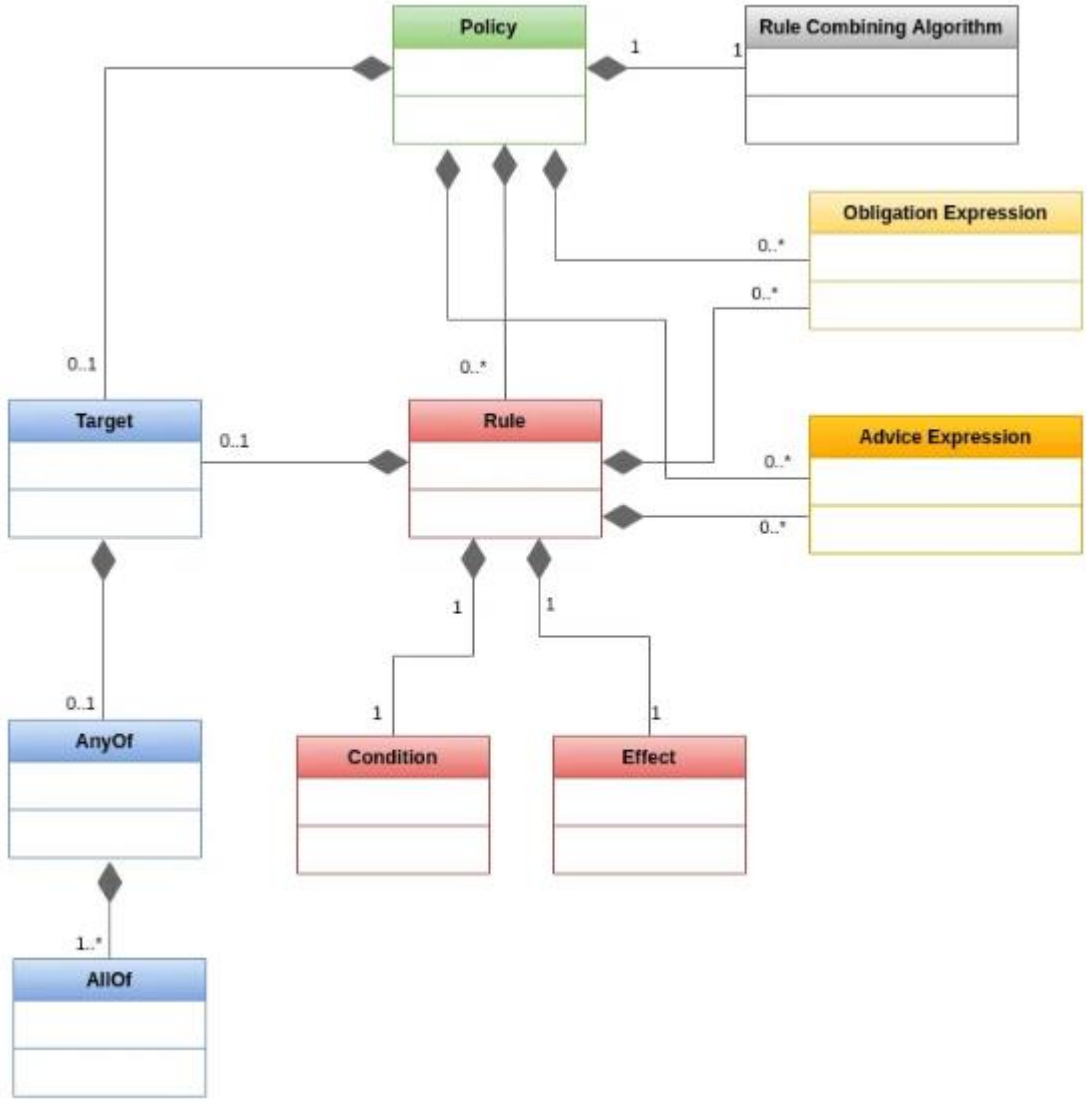
Ο αρθρωτός και ευέλικτος σχεδιασμός της αρχιτεκτονικής XACML καθιστά δυνατό τον απλό συνδυασμό της με διάφορες λύσεις ασφαλείας. Η αρχιτεκτονική αποτελείται από τρία κύρια μέρη: το σημείο λήψης αποφάσεων πολιτικής (PDP), το σημείο επιβολής πολιτικής και το σημείο διαχείρισης πολιτικής (PAP) (PEP) αντίστοιχα. Το PDP είναι υπεύθυνο για τη σύγκριση των αιτήσεων ελέγχου πρόσβασης με τις πολιτικές, το PAP είναι υπεύθυνο για τη διαχείριση και την αποθήκευση των πολιτικών ελέγχου πρόσβασης και το PEP είναι υπεύθυνο για την εφαρμογή των αποφάσεων ελέγχου πρόσβασης που εκδίδονται από το PDP[2][6][13].

Μια πολιτική XACML αποτελείται από έναν αριθμό κανόνων, καθένας από τους οποίους καθορίζει μια προϋπόθεση που πρέπει να πληρούνται για να είναι αποτελεσματικός ο κανόνας. Για να καταλήξουμε στην τελική απόφαση ελέγχου πρόσβασης, οι κανόνες συνδυάζονται με τη χρήση ενός αλγορίθμου συνδυασμού (όπως deny-overrides και permit-overrides).

Τα βασικά στοιχεία μιας πολιτικής XACML είναι[13]:

- Target: Ο πόρος και η δραστηριότητα στην οποία εφαρμόζεται η πολιτική ορίζονται από τον target.
- Rule:Ένας κανόνας προσδιορίζει μια προϋπόθεση που πρέπει να πληρείται για να τεθεί σε ισχύ ο κανόνας, επίσης περιέχει μέσα και ένα Boolean Expression.
- Condition: Το Condition είναι μια απαίτηση που πρέπει να πληρείται προκειμένου ο κανόνας να είναι αποτελεσματικός.
- Obligation: Μια υποχρέωση είναι μια απαίτηση που πρέπει να τηρηθεί εάν ο κανονισμός είναι κατάλληλος.
- Advice: Οι συμβουλές είναι πληροφορίες που δίνονται στο PDP αλλά δεν επηρεάζουν την επιλογή σχετικά με τους ελέγχους πρόσβασης.

- Policy: αποτελείται από έναν αριθμό στοιχείων "Rule" και μια μέθοδο συγχώνευσης των αποτελεσμάτων της εξέτασής τους. Σκοπός του είναι να χρησιμεύσει ως βάση για μια εγκεκριμένη απόφαση, επειδή αποτελεί τη θεμελιώδη μονάδα της πολιτικής του PDP.
- PolicySet: περιλαμβάνει ένα σύνολο στοιχείων "Policy" ή "PolicySet", μαζί με μια μέθοδο για τη συγχώνευση των αποτελεσμάτων αξιολόγησης.



Εικόνα 2.3 Αρχιτεκτονική XACML[13]

- AnyOf,AllOf,Matches: Τα συγκεκριμένα κλειδιά καθορίζουν σε λογικό νόημα πως έχει δημιουργηθεί η πολιτική. Το match είναι παιδί του AllOf το οποίο είναι παιδί του AnyOf.

1. Αν το Condition A ΚΑΙ το Condition B είναι matched.

```
<Target>
   <AnyOf>
      <AllOf>
         <Match>conditionA</Match>
         <Match>conditionB</Match>
      </AllOf>
   </AnyOf>
</Target>
```

Εικόνα 2.4 AND Συνθήκη[13]

2. Αν το Condition A Ή το Condition B είναι matched

```
<Target>
   <AnyOf>
      <AllOf>
         <Match>conditionA</Match>
      </AllOf>
      <AllOf>
         <Match>conditionB</Match>
      </AllOf>
   </AnyOf>
</Target>
```

Εικόνα 2.5 OR Συνθήκη[13]

Επειδή η XACML προορίζεται να είναι αρθρωτή, μπορεί να ενσωματωθεί γρήγορα σε διάφορα συστήματα ασφαλείας. Είναι δυνατή η προσθήκη πρόσθετων τμημάτων στην XACML ανάλογα με τις ανάγκες, επειδή προορίζεται να είναι επεκτάσιμη. Η ευελιξία της XACML καθιστά δυνατή τη γρήγορη ενημέρωση και τροποποίηση των πολιτικών ανάλογα με τις ανάγκες. Λόγω της επεκτασιμότητάς της, η XACML μπορεί να εφαρμοστεί σε ρυθμίσεις μεγάλης κλίμακας.

(2.3.3 ΥΛΟΠΟΙΗΣΗ ΚΑΙ ΕΦΑΡΜΟΓΕΣ)

Η XACML υποστηρίζει τόσο τον έλεγχο πρόσβασης βάσει ρόλων όσο και τον έλεγχο πρόσβασης βάσει χαρακτηριστικών. Σύμφωνα με το ρόλο του χρήστη που υποβάλλει την αίτηση, η πρόσβαση επιτρέπεται ή απορρίπτεται στο πλαίσιο του ελέγχου πρόσβασης βάσει ρόλων. Η πρόσβαση δίνεται ή απορρίπτεται στον έλεγχο πρόσβασης βάσει χαρακτηριστικών ανάλογα με τις τιμές των χαρακτηριστικών που συνδέονται με τον χρήστη, τον πόρο που αναζητείται και την ενέργεια που πραγματοποιείται. Προκειμένου να επιτύχουν με τον καλύτερο δυνατό τρόπο τους στόχους τους, οι επιχειρήσεις μπορούν να δημιουργήσουν κανόνες ελέγχου πρόσβασης χρησιμοποιώντας έναν συνδυασμό ελέγχου πρόσβασης βάσει ρόλων και ελέγχου πρόσβασης βάσει χαρακτηριστικών, ο οποίος υποστηρίζεται από το XACML.

Το XACML χρησιμοποιείται σε πολλά διαφορετικά προϊόντα, τόσο ανοικτού κώδικα όσο και κερδοσκοπικού χαρακτήρα. Πολυάριθμες επιχειρήσεις, όπως η υγειονομική περίθαλψη, οι τράπεζες και η κυβέρνηση, έχουν υιοθετήσει και χρησιμοποιούν την XACML. Συχνά λειτουργεί ως μέρος μιας ολοκληρωμένης υποδομής ασφάλειας μαζί με άλλα πρότυπα ασφάλειας όπως το SAML[6][13].

(2.3.4 ΠΑΡΑΔΕΙΓΜΑΤΑ)

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Policy PolicyId="2" Version="0" RuleCombiningAlgId="" MaxDelegationDepth="0" xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
    <Description></Description>
    <Target>
        <AnyOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="string">Πνευμονολογικό</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" AttributeId="sect" DataType="string" Issuer="" MustBePresent="true"/>
                </Match>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <AttributeValue DataType="string">ΓΝ Λαμίας</AttributeValue>
                    <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment" AttributeId="hosp" DataType="string" Issuer="" MustBePresent="true"/>
                </Match>
            </AllOf>
        </AnyOf>
    </Target>
    <Rule RuleId="2" Effect="Permit">
        <Description></Description>
        <Target>
            <AnyOf>
                <AllOf>
                    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <AttributeValue DataType="string">Πνευμονολογικό</AttributeValue>
                        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" AttributeId="sect" DataType="string" Issuer="" MustBePresent="true"/>
                    </Match>
                    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <AttributeValue DataType="string">ΓΝ Λαμίας</AttributeValue>
                        <AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment" AttributeId="hosp" DataType="string" Issuer="" MustBePresent="true"/>
                    </Match>
                </AllOf>
            </AnyOf>
        </Target>
    </Rule>
</Policy>
```

Εικόνα 2.6 XACML Πολιτική[21]

Παραπάνω βλέπουμε μια πολιτική XACML η οποία δίνει εξουσιοδότηση σε υποκείμενα τα οποία έχουν χαρακτηριστικά:

1. Να βρίσκονται στο ΓΝ Λαμίας
   ΚΑΙ
2. Να βρίσκονται στον τομέα του Πνευμονολογικού

ΚΕΦΑΛΑΙΟ 3 ΚΡΥΠΤΟΓΡΆΦΗΣΗ ΒΑΣΕΙ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ (ABE)

(3.1 Η ΙΣΤΟΡΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ)

Η κλασική κρυπτογραφία, η οποία δημιουργήθηκε και χρησιμοποιήθηκε πριν από την εφεύρεση της σύγχρονης τεχνολογίας των υπολογιστών, είναι η μελέτη και η χρήση της ασφαλούς επικοινωνίας με τη χρήση κωδίκων και κρυπτογραφήσεων. Η κλασική κρυπτογραφία είναι ένα αντικείμενο μελέτης που χρονολογείται χιλιάδες χρόνια πριν, με παραδείγματα που βρέθηκαν σε χειρόγραφα από πολιτισμούς όπως η Αίγυπτος, η Ελλάδα και η Ρώμη[20].

Η κρυπτογράφηση του Καίσαρα, μια απλή κρυπτογράφηση αντικατάστασης που περιλαμβάνει τη μετακίνηση κάθε γράμματος του απλού κειμένου κατά έναν προκαθορισμένο αριθμό θέσεων στο αλφάβητο, είναι μια από τις πρώτες εφαρμογές της κλασικής κρυπτογραφίας. Ο Ιούλιος Καίσαρας πιστώνεται ότι χρησιμοποίησε την κρυπτογράφηση Καίσαρα για να επικοινωνεί μυστικά με τους στρατηγούς του κατά τη διάρκεια στρατιωτικών μαχών, εξ ου και το όνομα της κρυπτογράφησης[17][27].

Η κρυπτογράφηση Vigenère, μια πολυαλφαβητική κρυπτογράφηση αντικατάστασης που δημιουργήθηκε τον 16ο αιώνα, είναι μια άλλη γνωστή κρυπτογράφηση. Κάθε γράμμα του απλού κειμένου μετατοπίζεται κατά διαφορετικό αριθμό θέσεων με βάση τη θέση του στο μήνυμα σε αυτή την κρυπτογράφηση, η οποία χρησιμοποιεί μια ακολουθία αλληλένδετων κρυπτογραφήσεων Καίσαρα[27][17].

Και οι δύο πλευρές χρησιμοποίησαν περίπλοκες κρυπτογραφήσεις και κώδικες για να προστατεύσουν τις επικοινωνίες τους κατά τη διάρκεια του Πρώτου και του Δεύτερου Παγκοσμίου Πολέμου, κατά τους οποίους έγινε ευρεία χρήση της κλασικής κρυπτογραφίας. Η γερμανική μηχανή Enigma, η οποία χρησιμοποιήθηκε για την κρυπτογράφηση των επικοινωνιών που έστελνε ο γερμανικός στρατός, ήταν μία από τις πιο γνωστές κρυπτογραφήσεις που χρησιμοποιούνταν εκείνη την εποχή. Το απλό κείμενο κρυπτογραφούνταν από τη μηχανή Enigma με τη χρήση ενός εξελιγμένου συστήματος ρήτορά και βύσματος, καθιστώντας πολύ δύσκολη την αποκρυπτογράφηση χωρίς τη βοήθεια μιας συσκευής αποκρυπτογράφησης[27][17].

Λόγω της βελτίωσης της επεξεργαστικής ισχύος και της έρευνας στην κρυπτογραφία, πολλοί ιστορικοί κρυπτογράφοι θεωρούνται ευρέως ότι είναι λιγότερο ασφαλείς από τους σύγχρονους κρυπτογραφικούς αλγορίθμους. Η ανάλυση συχνότητας και οι επιθέσεις brute-force είναι δύο σχετικά εύκολες μέθοδοι που μπορούν να χρησιμοποιηθούν για να σπάσουν πολλές παραδοσιακές κρυπτογραφήσεις. Η κλασική κρυπτογραφία, ωστόσο, συνεχίζει να αποτελεί ζωτικό πεδίο έρευνας για τους επιστήμονες πληροφορικής, τους κρυπτογράφους και τους ιστορικούς, καθώς ρίχνει φως στην ανάπτυξη και την ιστορία της κρυπτογραφίας στο σύνολό της[28].

Εν κατακλείδι, η παραδοσιακή κρυπτογραφία είναι ένα συναρπαστικό αντικείμενο έρευνας που έχει μακρά ιστορία. Οι κλασικές κρυπτογραφήσεις έχουν χρησιμοποιηθεί για την απόκρυψη σημαντικών πληροφοριών σε όλη τη διάρκεια της ιστορίας, από την απλή κρυπτογράφηση του Καίσαρα έως την περίπλοκη μηχανή Enigma. Αυτές οι κρυπτογραφήσεις μπορεί να μην είναι τόσο ασφαλείς όσο τα σύγχρονα κρυπτογραφικά συστήματα, αλλά παρόλα αυτά είναι σημαντικές για την εξέλιξη της ασφαλούς επικοινωνίας στο πέρασμα του χρόνου και προσφέρουν ζωτικό ιστορικό πλαίσιο[17][27].

(3.2 ΚΛΑΣΣΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ)

Η τεχνική της χρήσης κρυπτογραφίας χρησιμοποιείται για την προστασία των επικοινωνιών από μη εξουσιοδοτημένη πρόσβαση. Αυτό επιτυγχάνεται μέσω των διαδικασιών της κρυπτογράφησης και της αποκρυπτογράφησης, οι οποίες περιλαμβάνουν τη μετατροπή του απλού κειμένου σε κρυπτογραφημένο κείμενο και του κρυπτογραφημένου κειμένου πίσω σε απλό κείμενο, αντίστοιχα. Η συμμετρική και η ασύμμετρη κρυπτογραφία είναι οι δύο κύριες κατηγορίες[24].

Στη συμμετρική κρυπτογραφία χρησιμοποιείται ένα μόνο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Ο αποστολέας και ο παραλήπτης υποχρεούνται να διατηρούν αυτό το κλειδί ιδιωτικό. Ο AES (Advanced Encryption Standard), ο οποίος χρησιμοποιείται ευρέως σε διαδικτυακές συναλλαγές, υπηρεσίες ανταλλαγής μηνυμάτων και πλατφόρμες ανταλλαγής αρχείων, είναι ο πιο δημοφιλής αλγόριθμος συμμετρικής κρυπτογράφησης[24][25].

Από την άλλη πλευρά, η ασύμμετρη κρυπτογραφία χρησιμοποιεί ένα ζεύγος κλειδιών: ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Η επικοινωνία κρυπτογραφείται με τη χρήση του δημόσιου κλειδιού και αποκρυπτογραφείται με τη χρήση του ιδιωτικού κλειδιού. Ο προοριζόμενος παραλήπτης λαμβάνει το δημόσιο κλειδί του αποστολέα και το χρησιμοποιεί για την κρυπτογράφηση του μηνύματος. Η επικοινωνία μπορεί να αποκρυπτογραφηθεί μόνο από τον παραλήπτη, επειδή διαθέτει το ιδιωτικό κλειδί. Οι ψηφιακές υπογραφές, το ασφαλές ηλεκτρονικό ταχυδρομείο και οι ηλεκτρονικές συναλλαγές ασφαλίζονται συχνά με τη χρήση ασύμμετρης κρυπτογραφίας[25].

Η εγκυρότητα και η ακεραιότητα των ψηφιακών εγγράφων μπορούν να διασφαλιστούν με τη χρήση ψηφιακών υπογραφών. Η ασύμμετρη κρυπτογραφία χρησιμοποιείται στις ψηφιακές υπογραφές για τη δημιουργία διακριτών υπογραφών που μπορούν να παραχθούν μόνο από τον κάτοχο του ιδιωτικού κλειδιού. Οποιοσδήποτε έχει πρόσβαση στο δημόσιο κλειδί μπορεί στη συνέχεια να επικυρώσει την υπογραφή. Αυτό εγγυάται ότι η υπογραφή είναι γνήσια και ότι το έγγραφο δεν έχει παραποιηθεί. Στην κρυπτογραφία χρησιμοποιείται μια ποικιλία αλγορίθμων, καθένας από τους οποίους έχει μοναδικά πλεονεκτήματα και μειονεκτήματα. Οι πιο δημοφιλείς αλγόριθμοι είναι η κρυπτογραφία ελλειπτικής καμπύλης, ο RSA και ο DSA (ECC)[26].

Οι αλγόριθμοι ασύμμετρης κρυπτογράφησης όπως ο RSA (Rivest-Shamir-Adleman) χρησιμοποιούνται συχνά για την ασφάλεια του ηλεκτρονικού ταχυδρομείου, των ψηφιακών υπογραφών και των ηλεκτρονικών συναλλαγών. Δημιουργήθηκε το 1977 και βασίζεται στο πόσο δύσκολος μπορεί να είναι ο υπολογισμός μεγάλων αριθμών. Ένα άλλο σχήμα ασύμμετρης κρυπτογράφησης που χρησιμοποιείται στις ψηφιακές υπογραφές είναι ο DSA (Digital Signature Algorithm). Βασίζεται στη μαθηματική ιδέα της αρθρωτής αριθμητικής και δημιουργήθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST).Οι ελλειπτικές καμπύλες χρησιμοποιούνται για τη δημιουργία των δημόσιων και ιδιωτικών κλειδιών στη σχετικά νέα τεχνολογία κρυπτογράφησης που είναι γνωστή ως ECC (Elliptic Curve Cryptography). Χρησιμοποιείται συχνά για την ασφάλεια ασύρματων δικτύων και κινητών συσκευών, καθώς θεωρείται ασφαλέστερη από την RSA και την DSA[24][25].

Συμπερασματικά, η ασφαλής επικοινωνία στην ψηφιακή εποχή απαιτεί τη χρήση της κρυπτογραφίας. Η ασύμμετρη κρυπτογραφία χρησιμοποιεί ένα ζεύγος κλειδιών, ενώ η συμμετρική κρυπτογραφία χρησιμοποιεί ένα μόνο κλειδί για την κρυπτογράφηση και την αποκωδικοποίηση. Η αυθεντικότητα και η ακεραιότητα των ψηφιακών εγγράφων μπορούν να διασφαλιστούν με τη βοήθεια των ψηφιακών υπογραφών. Στην κρυπτογραφία χρησιμοποιείται μια ποικιλία αλγορίθμων, καθένας από τους οποίους έχει μοναδικά πλεονεκτήματα και μειονεκτήματα.

(3.3 ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΒΑΣΕΙ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ABE)

(3.3.1 ΕΙΣΑΓΩΓΗ)

Τα δεδομένα μπορούν να κρυπτογραφηθούν και να αποκρυπτογραφηθούν με τη χρήση χαρακτηριστικών χάρη σε έναν τύπο κρυπτογράφησης γνωστό ως κρυπτογράφηση βάσει χαρακτηριστικών (ABE). Αντίθετα, οι συμβατικές τεχνικές κρυπτογράφησης βασίζονται σε κρυπτογραφικά κλειδιά. Με την ABE, αντί η κρυπτογράφηση να βασίζεται σε ένα συγκεκριμένο κρυπτογραφικό κλειδί, η πρόσβαση στα κρυπτογραφημένα δεδομένα αποφασίζεται με βάση τα χαρακτηριστικά που διαθέτει ένα άτομο[5].

Η ABE έχει εφαρμοστεί σε πολλούς τομείς, όπως στα κυβερνητικά, τα οικονομικά την υγειονομική περίθαλψη, και αποτελεί ένα κρίσιμο εργαλείο για τη διασφάλιση ευαίσθητων δεδομένων. Παρακάτω θα εξετάσουμε τις βασικές αρχές του ABE, τα οφέλη και τα μειονεκτήματά του και ορισμένες από τις πιθανές εφαρμογές του.

(3.3.2 ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ABE)

Η ABE είναι ένας τύπος κρυπτογράφησης δημόσιου κλειδιού. Στην κλασική κρυπτογράφηση δημόσιου κλειδιού χρησιμοποιείται ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Ενώ το ιδιωτικό κλειδί πρέπει να διατηρείται μυστικό, το δημόσιο κλειδί μπορεί να διαμοιράζεται ελεύθερα. Το δημόσιο κλειδί μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση δεδομένων και το ιδιωτικό κλειδί απαιτείται για την αποκρυπτογράφηση. Καθώς μόνο ο προοριζόμενος παραλήπτης μπορεί να διαβάσει τα δεδομένα, αυτό επιτρέπει την ασφαλή επικοινωνία[19][5].

Τα δεδομένα κρυπτογραφούνται με ένα σύνολο ιδιοτήτων στο ABE σε αντίθεση με ένα συγκεκριμένο δημόσιο κλειδί. Ο τίτλος εργασίας του χρήστη, η τοποθεσία ή η εξουσιοδότηση ασφαλείας είναι μερικά παραδείγματα αυτών των ιδιοτήτων. Για παράδειγμα, μόνο οι χρήστες που διαθέτουν την ιδιότητα "διευθυντής" θα είναι σε θέση να αποκρυπτογραφήσουν δεδομένα που έχουν κρυπτογραφηθεί με τη χρήση αυτής της ιδιότητας[5].

Ένας χρήστης πρέπει να κατέχει ένα σύνολο ιδιοτήτων που αντιστοιχούν στις ιδιότητες που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων προκειμένου να χρησιμοποιήσει το ABE. Για παράδειγμα, ένας χρήστης που κατέχει το χαρακτηριστικό "manager" μπορεί να αποκρυπτογραφήσει υλικό που έχει κρυπτογραφηθεί με αυτό το χαρακτηριστικό. Τα δεδομένα δεν μπορούν να αποκρυπτογραφηθούν από έναν χρήστη που δεν διαθέτει το χαρακτηριστικό "διαχειριστής"[19][5].

Η κρυπτογράφηση βασισμένη σε χαρακτηριστικά με βάση την πολιτική κλειδιού (KP-ABE) και η κρυπτογράφηση βασισμένη σε χαρακτηριστικά με βάση την πολιτική κρυπτογράφησης είναι οι δύο κατηγορίες στις οποίες μπορεί να χωριστεί η ABE (CP-ABE).

Η KP-ABE είναι μια παραλλαγή της ABE στην οποία το κλειδί κρυπτογράφησης περιέχει την πολιτική ελέγχου πρόσβασης. Τα δεδομένα μπορούν να αποκρυπτογραφηθούν στην KP-ABE εάν τα χαρακτηριστικά του χρήστη ταιριάζουν με τα χαρακτηριστικά που σχετίζονται με το κλειδί κρυπτογράφησης. Ένα κλειδί κρυπτογράφησης συνδέεται με ένα σύνολο χαρακτηριστικών[19].

Αντίθετα, η CP-ABE είναι μια περίπτωση ABE στην οποία η πολιτική ελέγχου πρόσβασης περιλαμβάνεται στα κρυπτογραφημένα δεδομένα. Στην CP-ABE, η πρόσβαση παρέχεται εάν τα χαρακτηριστικά του χρήστη ταιριάζουν με τα χαρακτηριστικά που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων. Τα δεδομένα κρυπτογραφούνται με ένα σύνολο χαρακτηριστικών[19][14].

(3.3.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ABE)

Η ABE έχει μια σειρά πλεονεκτημάτων σε σχέση με τις συμβατικές τεχνικές κρυπτογράφησης. Η ABE, για αρχή, επιτρέπει ακριβέστερη διαχείριση της πρόσβασης. Η πρόσβαση περιορίζεται με τη χρήση συμβατικών τεχνικών κρυπτογράφησης σε όσους κατέχουν ένα κρυπτογραφικό κλειδί. Με άλλα λόγια, εάν ένας χρήστης έχει το κλειδί, έχει πρόσβαση σε όλα τα δεδομένα που έχουν κρυπτογραφηθεί με αυτό. Η πρόσβαση με το ABE βασίζεται σε κάποιες ιδιότητες, επιτρέποντας ακριβέστερο έλεγχο του ποιος έχει πρόσβαση σε ποια δεδομένα[7].

Δεύτερον, το ABE μπορεί να εφαρμοστεί σε περιπτώσεις όπου η διανομή και η διαχείριση των κλειδιών αποτελεί πρόκληση και είναι δύσκολη. Για παράδειγμα, μπορεί να υπάρχουν πολλοί χρήστες σε ένα πλαίσιο υγειονομικής περίθαλψης που πρέπει να έχουν πρόσβαση σε διάφορα σύνολα δεδομένων. Η διαχείριση και η διανομή κλειδιών σε όλα αυτά τα άτομα με τη χρήση συμβατικών τεχνικών κρυπτογράφησης μπορεί να αποτελέσει πρόκληση. Με την ABE, όμως, τα δεδομένα μπορούν να κρυπτογραφηθούν με βάσει τις ιδιότητες, καθιστώντας απλούστερο τον έλεγχο του ποιος έχει πρόσβαση στα δεδομένα[7].

Η ABE μπορεί επίσης να χρησιμοποιηθεί για την επιβολή κανόνων και πολιτικών. Για παράδειγμα, μπορεί να υπάρχουν αυστηροί κανόνες που να διέπουν το ποιος μπορεί να έχει πρόσβαση σε συγκεκριμένα είδη δεδομένων μέσα σε ένα κυβερνητικό περιβάλλον. Μόνο οι χρήστες με τη σωστή εξουσιοδότηση ασφαλείας θα πρέπει να μπορούν να έχουν πρόσβαση σε αυτά τα δεδομένα, σύμφωνα με το ABE. Αυτό μπορεί να βοηθήσει στη διασφάλιση της προστασίας των εμπιστευτικών πληροφοριών και της τήρησης των νόμων[5][7].

Η χρήση της ABE έχει πολλά πλεονεκτήματα, αλλά υπάρχουν και κάποια μειονεκτήματα. Πρώτον, σε σύγκριση με τις συμβατικές τεχνικές κρυπτογράφησης, η ABE μπορεί να είναι πιο δαπανηρή από υπολογιστική άποψη. Αυτό συμβαίνει για να μπορούν να ληφθούν υπόψη οι ιδιότητες που σχετίζονται με τα δεδομένα κατά τη διάρκεια των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης. Η ABE μπορεί να είναι πιο αργή και να χρησιμοποιεί περισσότερους πόρους ως αποτέλεσμα από τις συμβατικές τεχνικές κρυπτογράφησης[19].

Δεύτερον, σε σύγκριση με τις συμβατικές τεχνικές κρυπτογράφησης, η ABE μπορεί να είναι πιο δύσκολη στη συντήρηση και την ανάπτυξη. Αυτό οφείλεται στο γεγονός ότι η διαχείριση και η διανομή χαρακτηριστικών για την ABE απαιτεί μια πιο περίπλοκη υποδομή. Επίσης, σε σύγκριση με τις συμβατικές τεχνικές κρυπτογράφησης, η διαχείριση των κανονισμών ελέγχου πρόσβασης με τη χρήση ABE μπορεί να είναι πιο δύσκολη[5].

Τέλος, σε σύγκριση με τις συμβατικές τεχνικές κρυπτογράφησης, η ABE μπορεί να είναι πιο ευάλωτη σε επιθέσεις. Αυτό συμβαίνει έτσι ώστε να μπορεί η ABE να βασίζεται στην ασφάλεια των χαρακτηριστικών κατά την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Τα ευαίσθητα δεδομένα μπορεί να είναι προσβάσιμα εάν ένας επιτιθέμενος είναι σε θέση να θέσει σε κίνδυνο την ασφάλεια αυτών των ιδιοτήτων. Επιπλέον, εάν οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης δεν εκτελούνται αποτελεσματικά, ένας επιτιθέμενος μπορεί να είναι σε θέση να παρακάμψει τους κανονισμούς ελέγχου πρόσβασης[7].

.

(3.3.4 ΕΦΑΡΜΟΓΕΣ ABE)

Η ABE έχει πολλές πιθανές χρήσεις σε πολυάριθμες βιομηχανίες. Η υγειονομική περίθαλψη είναι ένας κλάδος όπου η ABE είναι πολύ χρήσιμη. Οι ευαίσθητες πληροφορίες των ασθενών πρέπει να προστατεύονται στον τομέα της υγειονομικής περίθαλψης, ενώ παράλληλα πρέπει να είναι προσβάσιμες από τους γιατρούς, τους νοσηλευτές και το λοιπό ιατρικό προσωπικό. Με βάσει χαρακτηριστικά όπως, η τοποθεσία και η εξειδίκευση του επαγγελματία υγείας, το ABE μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων των ασθενών. Αυτό μπορεί να βοηθήσει στη διασφάλιση ότι οι πληροφορίες των ασθενών είναι διαθέσιμες μόνο στο απαραίτητο ιατρικό προσωπικό[5][7].

Η χρηματοοικονομική βιομηχανία είναι ένας άλλος κλάδος όπου η ABE είναι χρήσιμη. Τα ευαίσθητα οικονομικά δεδομένα πρέπει να διασφαλίζονται στον οικονομικό τομέα, ενώ παράλληλα πρέπει να είναι προσβάσιμα από τους υπαλλήλους. Με βάσει παράγοντες όπως ο τίτλος εργασίας του υπαλλήλου, η τοποθεσία και το τμήμα, το ABE μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση των οικονομικών δεδομένων. Αυτό μπορεί να βοηθήσει στη διασφάλιση ότι οι οικονομικές πληροφορίες είναι διαθέσιμες μόνο στα μέλη του προσωπικού που έχουν βάσιμο λόγο πρόσβασης σε αυτές[5][19].

Τέλος, το ABE έχει εφαρμογές στον δημόσιο τομέα. Οι ευαίσθητες πληροφορίες, συμπεριλαμβανομένων των δεδομένων που σχετίζονται με την εθνική ασφάλεια και τις προσωπικές πληροφορίες, πρέπει να προστατεύονται εντός της κυβέρνησης. Με βάσει παράγοντες όπως το επίπεδο εξουσιοδότησης ασφαλείας, ο τίτλος εργασίας και η τοποθεσία, το ABE μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση αυτών των πληροφοριών. Αυτό μπορεί να βοηθήσει στη διασφάλιση ότι πρόσβαση σε ευαίσθητες πληροφορίες έχουν μόνο άτομα με πραγματική ανάγκη πρόσβασης σε αυτές[7][19].

(3.4 Ciphertext-Policy Attribute-Based Encryption CP-ABE)

Η Ciphertext-Policy Attribute-Based Encryption (CP-ABE) είναι μια κρυπτογραφική μέθοδος που επιτρέπει σε εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε κρυπτογραφημένα δεδομένα βάσει συγκεκριμένων χαρακτηριστικών, ενώ παράλληλα επιτρέπει την ασφαλή μετάδοση και την ευέλικτη αποθήκευση δεδομένων. Πολλές εφαρμογές, όπως το ασφαλές ηλεκτρονικό ταχυδρομείο, η υπολογιστική νέφους και οι συσκευές IoT, έχουν κάνει εκτεταμένη χρήση της CP-ABE. Σε αυτήν την ενότητα θα δοθεί μια γενική επισκόπηση της CP-ABE, συμπεριλαμβανομένης της αρχιτεκτονικής, της υλοποίησης, των πλεονεκτημάτων και των μειονεκτημάτων της[14].

(3.4.1 ΕΙΣΑΓΩΓΗ)

Ένα ευέλικτο σύστημα ελέγχου πρόσβασης για κρυπτογραφημένα δεδομένα καθίσταται δυνατό με την κρυπτογραφική μέθοδο που είναι γνωστή ως CP-ABE. Βασίζεται στην ιδέα της κρυπτογράφησης βάσει χαρακτηριστικών (attribute-based encryption, ABE), ενός τύπου κρυπτογράφησης που επιτρέπει τη χρήση χαρακτηριστικών ως κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων και έχει αναλυθεί στην προηγούμενη ενότητα. Οι ιδιότητες στην CP-ABE χρησιμοποιούνται για τον καθορισμό των πολιτικών πρόσβασης και η κρυπτογράφηση πραγματοποιείται σύμφωνα με μία πολιτική[14].

Οι παραδοσιακές μέθοδοι κρυπτογράφησης, όπως η συμμετρική και η ασύμμετρη κρυπτογράφηση, οι οποίες χρησιμοποιούν σταθερά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων, έχουν ορισμένα μειονεκτήματα. Η μεθοδολογία CP-ABE αναπτύχθηκε για να αμβλύνει αυτά τα μειονεκτήματα. Αυτές οι μέθοδοι επιτρέπουν στους

κατόχους κλειδιών να έχουν πρόσβαση στα κρυπτογραφημένα δεδομένα μόνο εάν έχουν το σωστό κλειδί, επομένως προσφέρουν μόνο ένα ελάχιστο επίπεδο ελέγχου πρόσβασης. Ωστόσο, αποτελεί πρόκληση ο σχεδιασμός μιας ασφαλούς και αποτελεσματικής μεθόδου ελέγχου πρόσβασης όταν υπάρχουν πολλοί χρήστες με διαφορετικά δικαιώματα πρόσβασης[8].

Επιτρέποντας στους χρήστες να έχουν πρόσβαση στα κρυπτογραφημένα δεδομένα με βάση τις ιδιότητές τους, η CP-ABE ξεπερνά αυτόν τον περιορισμό. Έτσι, οι χρήστες που έχουν τις ιδιότητες που ταιριάζουν στην πολιτική πρόσβασης μπορούν να έχουν πρόσβαση στα δεδομένα. Η πολιτική πρόσβασης δηλώνεται με βάσει τις ιδιότητες[14].

(3.4.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ)

Η αρχιτεκτονική CP-ABE αποτελείται από τέσσερα κύρια στοιχεία: τον κρυπτογράφο, τη γεννήτρια κλειδιών, την αρχή χαρακτηριστικών και τον αποκρυπτογράφο.

- **Κρυπτογράφος:** Σύμφωνα με την πολιτική πρόσβασης, ο κρυπτογράφος είναι υπεύθυνος για την κρυπτογράφηση των δεδομένων. Του δίνονται τα δεδομένα που πρέπει να κρυπτογραφηθούν, μαζί με μια πολιτική πρόσβασης που καθορίζεται σε όρους χαρακτηριστικών. Στη συνέχεια, το κρυπτογραφημένο κείμενο δημιουργείται από τον κρυπτογράφο και μόνο οι χρήστες με τις απαραίτητες ιδιότητες μπορούν να το αποκρυπτογραφήσουν[8][14].

- **Γεννήτρια κλειδιών:** Με βάση τις ιδιότητες του χρήστη, η γεννήτρια κλειδιών είναι υπεύθυνη για την παραγωγή των κλειδιών αποκρυπτογράφησης. Εάν οι ιδιότητες του χρήστη ικανοποιούν την πολιτική πρόσβασης, λαμβάνει τις ιδιότητες του χρήστη από την αρχή χαρακτηριστικών και παράγει ένα κλειδί αποκρυπτογράφησης που μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση του κρυπτογραφημένου κειμένου[8][14].

- **Αρχή χαρακτηριστικών:** Εναπόκειται στην αρχή χαρακτηριστικών να χορηγεί και να ανακαλεί χαρακτηριστικά. Παρακολουθεί τα χαρακτηριστικά και τα άτομα που ανήκουν σε αυτά και αναθέτει χαρακτηριστικά σε χρήστες σύμφωνα με την ταυτότητά τους ή άλλα κριτήρια. Όταν ένας χρήστης δεν χρειάζεται πλέον πρόσβαση στα κρυπτογραφημένα δεδομένα, για παράδειγμα, ανακαλεί επίσης τα χαρακτηριστικά, αν αυτό είναι απαραίτητο[8][14].

- **Αποκρυπτογράφος:** Χρησιμοποιώντας το κλειδί αποκρυπτογράφησης που παράγεται από τη γεννήτρια κλειδιών, ο αποκρυπτογράφος είναι υπεύθυνος για την αποκρυπτογράφηση του κρυπτογραφημένου κειμένου. Επιβεβαιώνει πρώτα ότι ο χρήστης έχει τα προσόντα που απαιτούνται για την πρόσβαση στα δεδομένα πριν αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο[8][14].

(3.4.3 ΥΛΟΠΟΙΗΣΗ)

Πολλές μαθηματικές μέθοδοι, όπως η κρυπτογράφηση με βάσει την ταυτότητα, η την κρυπτογραφία ελλειπτικών καμπυλών και τα διγραμμικά ζεύγη, μπορούν να χρησιμοποιηθούν για την υλοποίηση της CP-ABE. Η χρήση των υποκείμενων

κρυπτογραφικών πρωτευόντων και οι μοναδικές απαιτήσεις της εφαρμογής καθορίζουν την υλοποίηση.

- **Διγραμμικά ζεύγη:** Στην CP-ABE, η σχέση μεταξύ δύο συνόλων σημείων καθορίζεται μέσω διγραμμικών ζευγών. Χρησιμοποιούνται για τη δημιουργία μιας κλιμακωτής τιμής με τον υπολογισμό του γινομένου τελείας δύο σημείων που βρίσκονται σε διαφορετικές ομάδες. Μπορείτε να χρησιμοποιήσετε αυτή την κλιμακωτή τιμή ως κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Τα διγραμμικά ζεύγη χρησιμοποιούνται στην CP-ABE για να παρέχουν μια σύνδεση μεταξύ των χαρακτηριστικών και της πολιτικής πρόσβασης. Οι ιδιότητες που είναι απαραίτητες για την πρόσβαση στα δεδομένα καθορίζονται στην πολιτική πρόσβασης, η οποία αναπαρίσταται ως τύπος Boolean. Η πολιτική πρόσβασης αναπαρίσταται ως γινόμενο των σημείων στα οποία αντιστοιχίζονται τα χαρακτηριστικά σε μια ομάδα. Στη συνέχεια, μια κλιμακωτή τιμή που χρησιμεύει ως κρυπτογράφημα παράγεται με τον υπολογισμό του γινομένου σημείων του απλού κειμένου και της πολιτικής πρόσβασης. Τα χαρακτηριστικά του χρήστη αντιστοιχίζονται επίσης σε σημεία της ίδιας ομάδας για την αποκρυπτογράφηση του κρυπτοκειμένου. Στη συνέχεια, υπολογίζοντας το γινόμενο των ιδιοτήτων του χρήστη και των ιδιοτήτων που απαιτεί η πολιτική πρόσβασης, η γεννήτρια κλειδιών παράγει ένα κλειδί αποκρυπτογράφησης. Η κλιμακωτή τιμή που παράγεται από αυτό το γινόμενο μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση του κρυπτοκειμένου[8][19].

- **Κρυπτογραφία ελλειπτικής καμπύλης:** Στην CP-ABE, η κρυπτογραφία ελλειπτικών καμπυλών (ECC) είναι μια άλλη μαθηματική μέθοδος. Η ECC είναι μια μέθοδος για τη δημιουργία κλειδιών, την κρυπτογράφηση δεδομένων και την αποκρυπτογράφηση δεδομένων που βασίζεται στα μαθηματικά χαρακτηριστικά των ελλειπτικών καμπυλών. Η ECC χρησιμοποιείται στην CP-ABE για την παραγωγή των δημόσιων και ιδιωτικών κλειδιών που απαιτούνται από τον κρυπτογράφο και τον αποκρυπτογράφο. Η πολιτική πρόσβασης εκφράζεται ως εξίσωση στην ίδια ελλειπτική καμπύλη με τα χαρακτηριστικά, τα οποία αναπαρίστανται ως σημεία της καμπύλης. Το απλό κείμενο δημιουργείται στη συνέχεια από τον κρυπτογράφο και χρησιμοποιείται ως τυχαίο σημείο στην καμπύλη. Το απλό κείμενο προστίθεται στην εξίσωση της πολιτικής πρόσβασης για τη δημιουργία του κρυπτοκειμένου. Η γεννήτρια κλειδιών δημιουργεί ένα ιδιωτικό κλειδί χρησιμοποιώντας τα χαρακτηριστικά του χρήστη προκειμένου να αποκρυπτογραφήσει το κρυπτοκείμενο. Στη συνέχεια, το απλό κείμενο δημιουργείται χρησιμοποιώντας το ιδιωτικό κλειδί για τον υπολογισμό του αντίστροφου της εξίσωσης πολιτικής πρόσβασης[8][18].

- **Κρυπτογράφηση με βάση την ταυτότητα:** Μια άλλη κρυπτογραφική μέθοδος που μπορεί να χρησιμοποιηθεί για την υλοποίηση της CP-ABE είναι η κρυπτογράφηση με βάσει την ταυτότητα (IBE). Η IBE χρησιμοποιεί την ταυτότητα ενός χρήστη ως δημόσιο κλειδί, ενώ το ιδιωτικό κλειδί παράγεται από μια γεννήτρια ιδιωτικού κλειδιού, ένα αξιόπιστο τρίτο μέρος (PKG).Στην CP-ABE, η πολιτική πρόσβασης αναπαρίσταται ως ένας τύπος Boolean που απαριθμεί τα απαραίτητα χαρακτηριστικά και τα χαρακτηριστικά αναπαρίστανται ως ταυτότητα του χρήστη. Το κρυπτογραφημένο κείμενο δημιουργείται όταν ο κρυπτογράφος κρυπτογραφεί το απλό κείμενο χρησιμοποιώντας την πολιτική πρόσβασης και την ταυτότητα του χρήστη. Η γεννήτρια κλειδιών ζητά από την PKG ένα κλειδί αποκρυπτογράφησης προκειμένου να αποκρυπτογραφήσει το κρυπτοκείμενο. Το PKG παράγει το

κλειδί αποκρυπτογράφησης χρησιμοποιώντας την ταυτότητα του χρήστη και τις απαραίτητες ιδιότητες. Το κρυπτογραφημένο κείμενο αποκρυπτογραφείται στη συνέχεια από τον αποκρυπτογράφο χρησιμοποιώντας το κλειδί αποκρυπτογράφησης[8].

(3.4.4 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ)

Η CP-ABE προσφέρει αρκετά πλεονεκτήματα σε σχέση με τις παραδοσιακές τεχνικές κρυπτογράφησης.

1. **Ευέλικτος έλεγχος πρόσβασης:** Με βάσει τις ιδιότητες του χρήστη, η CP-ABE επιτρέπει μεταβλητό έλεγχο πρόσβασης. Αυτό επιτρέπει τον έλεγχο πρόσβασης σε λεπτό επίπεδο, καθώς η πολιτική πρόσβασης μπορεί να περιγραφεί με βάσει οποιονδήποτε συνδυασμό ιδιοτήτων. Εξαιτίας αυτού, η CP-ABE λειτουργεί αποτελεσματικά σε καταστάσεις όπου υπάρχουν πολλοί χρήστες και διαφορετικά επίπεδα πρόσβασης[8].

2. **Αποδοτική διαχείριση κλειδιών:** Επιτρέποντας τη χρήση ιδιοτήτων ως κλειδιά, η CP-ABE βελτιώνει τη διαδικασία διαχείρισης κλειδιών. Αυτό σημαίνει ότι αντί για τη δημιουργία ενός κλειδιού για κάθε χρήστη, η γεννήτρια κλειδιών χρειάζεται απλώς να δημιουργήσει ένα κλειδί για κάθε ιδιότητα. Αυτό μειώνει την ποσότητα των κλειδιών που πρέπει να διαχειριστεί και βελτιώνει την αποτελεσματικότητα της διαδικασίας διαχείρισης κλειδιών[18].

3. **Εμπιστευτικότητα δεδομένων:** Σύμφωνα με την πολιτική πρόσβασης, η CP-ABE κρυπτογραφεί τα δεδομένα για να παρέχει υψηλό επίπεδο εμπιστευτικότητας των δεδομένων. Αυτό εξασφαλίζει υψηλό επίπεδο μυστικότητας των δεδομένων, επειδή μόνο τα άτομα που διαθέτουν τις σχετικές ιδιότητες μπορούν να έχουν πρόσβαση στα δεδομένα[25].

Το CP-ABE έχει επίσης ορισμένους περιορισμούς, όπως:

1. **Πολυπλοκότητα:** Η εφαρμογή και η συντήρηση της εξελιγμένης κρυπτογραφικής τεχνολογίας που είναι γνωστή ως CP-ABE απαιτούν υψηλό επίπεδο γνώσεων. Αρκετά στοιχεία συνθέτουν την αρχιτεκτονική CP-ABE, η οποία απαιτεί επίσης την εφαρμογή μαθηματικών μεθόδων όπως η κρυπτογραφία ελλειπτικών καμπυλών και τα διγραμμικά ζεύγη. Μπορεί να είναι πρόκληση η κατασκευή και η συντήρηση λόγω αυτής της πολυπλοκότητας[26][14].

2. **Αποθήκευση κλειδιών:** Για τη χορήγηση και ανάκληση χαρακτηριστικών, η CP-ABE χρησιμοποιεί μια αξιόπιστη αρχή χαρακτηριστικών. Αυτό εγείρει την πιθανότητα παρακαταθήκης κλειδιών, οπότε η αρχή χαρακτηριστικών μπορεί να είναι σε θέση να αποκρυπτογραφήσει κρυφά τα κρυπτογραφήματα. Κατά συνέπεια, μπορεί να τεθεί σε κίνδυνο η ασφάλεια και η εμπιστευτικότητα των δεδομένων[14][26].
3. **Επεκτασιμότητα:** Καθώς αυξάνεται ο αριθμός των χαρακτηριστικών και των χρηστών, το CP-ABE δεν θα μπορούσε να είναι επεκτάσιμο για εφαρμογές που απαιτούν μεγάλη βάσει χρηστών. Η απόδοση του συστήματος μπορεί να επηρεαστεί από το υπολογιστικό κόστος που σχετίζεται με την παραγωγή και αποκρυπτογράφηση κλειδιών καθώς αυξάνεται ο αριθμός των χαρακτηριστικών και των χρηστών[14].

(3.4.5 ΠΕΡΙΠΤΩΣΕΙΣ ΧΡΗΣΗΣ)

Το CP-ABE έχει ένα ευρύ φάσμα περιπτώσεων χρήσης σε διάφορες βιομηχανίες και σενάρια, όπως:

1. **Υγειονομική περίθαλψη:** Η CP-ABE μπορεί να χρησιμοποιηθεί στον τομέα της υγειονομικής περίθαλψης για να προσφέρει ασφαλή πρόσβαση σε ιατρικούς φακέλους. Οι ευαίσθητες πληροφορίες που βρίσκονται στα ιατρικά αρχεία πρέπει να προστατεύονται, αλλά πρέπει επίσης να είναι διαθέσιμες σε εξουσιοδοτημένα άτομα. Μόνο τα άτομα με τα απαραίτητα διαπιστευτήρια και εξουσιοδότηση μπορούν να έχουν πρόσβαση στα ιατρικά αρχεία χάρη στο CP-ABE[15].

2. **Υπολογιστικό νέφος:** Το CP-ABE μπορεί να χρησιμοποιηθεί στο υπολογιστικό νέφος για να εγγυηθεί το απόρρητο των δεδομένων που φυλάσσονται εκεί. Οι παραβιάσεις δεδομένων μπορεί να προκύψουν ως αποτέλεσμα του υπολογιστικού νέφους, το οποίο περιλαμβάνει την αποθήκευση δεδομένων σε απομακρυσμένους υπολογιστές. Με βάση την πολιτική πρόσβασης, η CP-ABE μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων, εξασφαλίζοντας ότι μόνο οι επιτρεπόμενοι χρήστες μπορούν να έχουν πρόσβαση στις πληροφορίες[15].

3. **Διαδίκτυο των πραγμάτων (IoT):** Η CP-ABE μπορεί να χρησιμοποιηθεί για την ασφάλεια της επικοινωνίας των συσκευών στο Διαδίκτυο των πραγμάτων (IoT). Οι συσκευές IoT επικοινωνούν και συλλέγουν ευαίσθητα δεδομένα που μπορούν να υποκλαπούν από μη εξουσιοδοτημένους χρήστες και να αποκτήσουν πρόσβαση. Για να εξασφαλιστεί ότι μόνο εξουσιοδοτημένες συσκευές με τα απαραίτητα προσόντα μπορούν να έχουν πρόσβαση στα δεδομένα, μπορεί να χρησιμοποιηθεί η CP-ABE[11].

(3.4.6 ΣΥΜΠΕΡΑΣΜΑΤΑ)

Επομένως, η CP-ABE είναι μια πολύ ισχυρή κρυπτογραφική μέθοδος που παρέχει προσαρμόσιμο έλεγχο πρόσβασης και αποτελεσματική διαχείριση κλειδιών. Αυτό το επιτυγχάνει κρυπτογραφώντας τα δεδομένα σύμφωνα με τους κανόνες πρόσβασης, εξασφαλίζοντας υψηλό επίπεδο μυστικότητας των δεδομένων. Περιορίζεται, ωστόσο, από προβλήματα πολυπλοκότητας και επεκτασιμότητας. Παρά τα μειονεκτήματα αυτά, η CP-ABE προσφέρει μια μεγάλη ποικιλία περιπτώσεων εφαρμογής σε διάφορους τομείς και περιστάσεις, όπως η υγειονομική περίθαλψη, η υπολογιστική νέφους και το IoT. Η σημασία της CP-ABE στον τομέα της κρυπτογραφίας προβλέπεται να αυξηθεί καθώς αυξάνεται η ζήτηση για ασφαλή έλεγχο πρόσβασης και μυστικότητα δεδομένων.

ΚΕΦΑΛΑΙΟ 4 ΚΩΔΙΚΟΠΟΙΗΣΗ XACML ΣΕ ABE

(4.1 ΕΙΣΑΓΩΓΗ)

Σε περίπλοκα περιβάλλοντα όπου οι χρήστες μπορεί να έχουν διαφορετικά επίπεδα πρόσβασης ανάλογα με τη λειτουργία τους ή άλλα κριτήρια, η μέθοδος έλεγχος πρόσβασης βάσει Χαρακτηριστικών (ABAC) επιτρέπει λεπτομερή έλεγχο του ποιος μπορεί να έχει πρόσβαση σε ποια δεδομένα.

Ο έλεγχος πρόσβασης με βάση τα χαρακτηριστικά (Attribute-Based Access Control - ABAC), είναι μια ευέλικτη και κλιμακούμενη μέθοδος ελέγχου πρόσβασης που κερδίζει ολοένα και μεγαλύτερη δημοτικότητα στις σύγχρονες επιχειρήσεις, και είναι μια από τις χρήσεις του ABE. Οι επιλογές πρόσβασης μπορούν να καθοριστούν με τη χρήση του ABAC ανάλογα με τα χαρακτηριστικά του υποκείμενου, τον πόρο στον οποίο έχει πρόσβαση και το πλαίσιο του αιτήματος. Αυτή η στρατηγική μπορεί να καταστήσει δυνατή τη δημιουργία πιο σύνθετων κανόνων ελέγχου πρόσβασης που μπορούν να προσαρμόζονται στις μεταβαλλόμενες συνθήκες και στις απαιτήσεις των χρηστών.

Οι ABE και ABAC είναι ισχυρές τεχνολογίες που μπορούν να βοηθήσουν τις επιχειρήσεις να επιτύχουν υψηλότερη ασφάλεια και διαχείριση δεδομένων. Αυτές οι τεχνολογίες επιτρέπουν στις επιχειρήσεις να δημιουργούν πιο λεπτομερείς, προσαρμόσιμες και κλιμακούμενες πολιτικές ελέγχου πρόσβασης, ενώ παράλληλα ενισχύουν την προστασία των κρίσιμων δεδομένων. Οι τεχνολογίες ABE και ABAC αναμένεται να γίνουν ακόμη πιο κρίσιμες τα επόμενα χρόνια, καθώς ο όγκος των δεδομένων και η πολυπλοκότητα των πολιτικών ελέγχου πρόσβασης συνεχίζουν να αυξάνονται.

Σε σύγκριση με τις συμβατικές στρατηγικές ελέγχου πρόσβασης, η ABE σε συνεργασία με την ABAC προσφέρει μια σειρά από πλεονεκτήματα. Ακολουθούν ορισμένα από τα κύρια πλεονεκτήματα:

1. Ο λεπτομερής έλεγχος πρόσβασης είναι δυνατός με το ABE/ABAC, το οποίο επιτρέπει τη χορήγηση ή την άρνηση πρόσβασης σε πόρους ανάλογα με ορισμένες ιδιότητες του υποκείμενου. Αυτό είναι ιδιαίτερα χρήσιμο σε περιπτώσεις όπου η πρόσβαση σε ευαίσθητα δεδομένα πρέπει να περιοριστεί σε μια συγκεκριμένη ομάδα ατόμων[7][19].

2. Η πρόσβαση μπορεί να επιτραπεί ή να απορριφθεί ανάλογα με τις αλλαγές στα χαρακτηριστικά του υποκείμενου χάρη στη δυνατότητα δυναμικού ελέγχου πρόσβασης του ABE/ABAC. Σε σύγκριση με τις συμβατικές στρατηγικές ελέγχου πρόσβασης, οι οποίες μπορεί να απαιτούν χειροκίνητες αλλαγές στις λίστες ελέγχου πρόσβασης, αυτό προσφέρει μεγαλύτερη ευελιξία και ασφάλεια[14][16].

3. Το ABE/ABAC μπορεί να αυξήσει την ιδιωτικότητα, επιτρέποντας στα υποκείμενα να επικοινωνούν με δεδομένα χωρίς να αποκαλύπτουν την ταυτότητά τους. Για να γίνει αυτό, τα δεδομένα κρυπτογραφούνται χρησιμοποιώντας χαρακτηριστικά και όχι τις ταυτότητες των χρηστών(ciphertext)[15].

(4.2 ΥΛΟΠΟΙΗΣΗ)

Μια αρχή χαρακτηριστικών(Trusted Authority - TA) που ελέγχει τα χαρακτηριστικά του υποκείμενου και των άλλων δεδομένων (περιβάλλον, ενέργεια)χρησιμοποιείται για

την υλοποίηση του ABE/ABAC. Με βάσει τα χαρακτηριστικά του χρήστη και των δεδομένων, η TA παράγει και διανέμει κρυπτογραφικά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων.

Η ABE με πολιτική κλειδιού (KP-ABE) και η ABE με πολιτική κρυπτοκειμένου (CP-ABE) είναι οι δύο διαφορετικοί τύποι συστημάτων ABE. Ενώ οι πολιτικές πρόσβασης στην CP-ABE καθορίζονται με βάση τα χαρακτηριστικά των δεδομένων, στην KP-ABE βασίζονται στα χαρακτηριστικά του υποκείμενου[14].

Τα ακόλουθα βήματα αποτελούν μέρος της στρατηγικής υλοποίησης της ABE σε συνεργασία με την ABAC[23][14]:

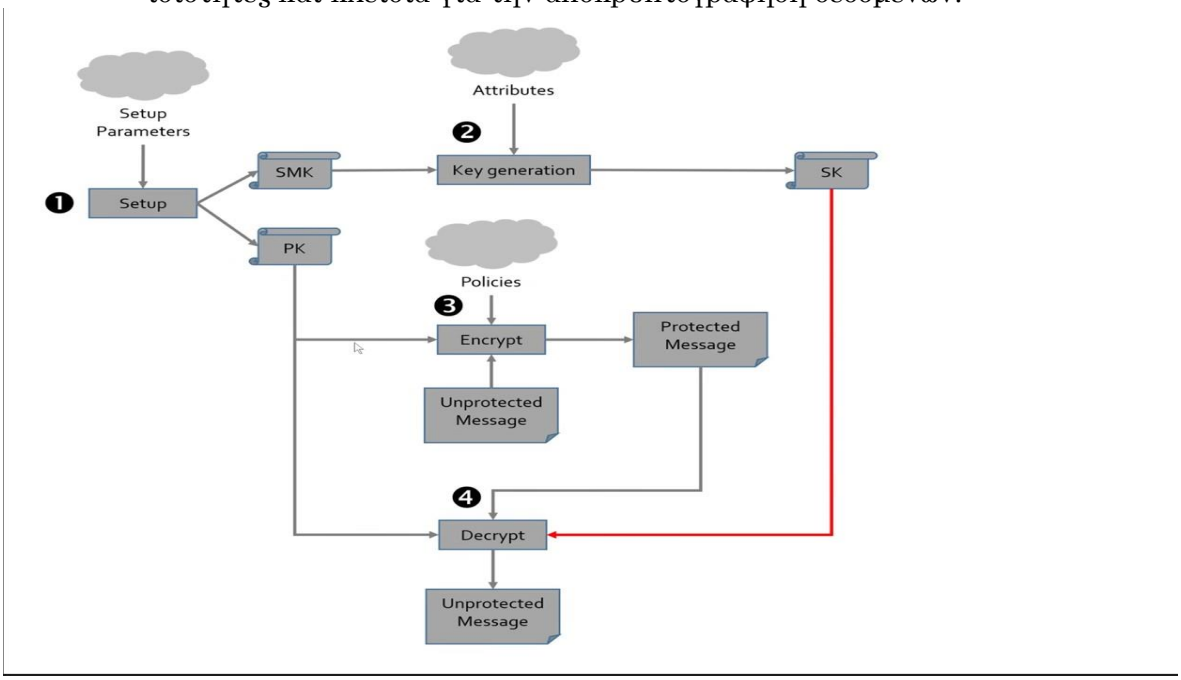
1. **Καταχώρηση χαρακτηριστικών**: Η αρχή χαρακτηριστικών (Trusted Authority) αποθηκεύει τα χαρακτηριστικά του χρήστη και των δεδομένων σε μια βάση δεδομένων.

2. **Δημιουργία κλειδιών**: Ο αρχή χαρακτηριστικών (Trusted Authority) παράγει κρυπτογραφικά κλειδιά ανάλογα με τις ιδιότητες του υποκείμενου και τα δεδομένων(περιβάλλον, ενέργεια), με βάση ένα mastery key που εκδόθηκε πιο πριν. Παράλληλα εκδίδεται και ένα δημόσιο κλειδί.

3. **Κρυπτογράφηση δεδομένων**: Χρησιμοποιούνται κρυπτογραφικές ιδιότητες και κλειδιά για την κρυπτογράφηση δεδομένων.

4. **Έλεγχος πρόσβασης**: Ανάλογα με τις ιδιότητες του χρήστη, η πρόσβαση στα κρυπτογραφημένα δεδομένα είτε επιτρέπεται είτε απορρίπτεται.

5. **Αποκρυπτογράφηση δεδομένων**: Χρησιμοποιούνται κρυπτογραφικές ιδιότητες και κλειδιά για την αποκρυπτογράφηση δεδομένων.



Εικόνα 4.1 Βασικό Σύστημα ABAC με ABE

Η παραπάνω εικόνα αναλύει λεπτομερώς πως λειτουργεί ένα τέτοιο σύστημα. Πιο συγκεκριμένα το setup γίνεται από την αρχή χαρακτηριστικών (Trusted Authority) το οποίο εξάγει τα κλειδιά (secret, public και mastery). Τα Policies εκδίδονται από αρχεία XACML που αναφέρθηκαν στο κεφάλαιο 2 τα οποία με κατάλληλους αλγορίθμους που θα

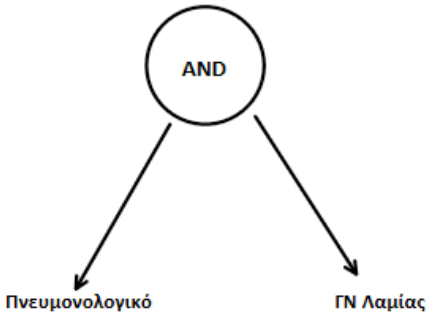
παρουσιαστούν παρακάτω επιστρέφουν μια λογική έκφραση η οποία στην συνέχεια κρυπτογραφείται μαζί με τα δεδομένα που χρειάζονται να κρυπτογραφηθούν αλλά και το public key και παράγεται το κρυπτογραφημένο μήνυμα ή αλλιώς ciphertext.

(4.2.1 ΑΛΓΟΡΙΘΜΟΣ ΜΕΤΑΤΡΟΠΗΣ)

```
 1: Function AbacToABE(String pathfile)
 2:     Logical_expr <- NULL
 3:     Document parse(pathfile)
 4:     Node rule<-getElementsByTagName("Rule")
 5:     Node target<-rule.getChildNodes
 6:     Node AnyOf<-target.getChildNodes
 7:     if rule.getAttribute("Effect")==Permit
 8:         return Logical_expr <- handleAnyOf(AnyOf)
 9:     else
10:         return Logical_expr <- !(handleAnyOf(AnyOf))
11: Endfunction
12: Function handleAnyOf(Node AnyOf)
13:     Logical_expr <- NULL
14:     get.AnyOfChild
15:     if num_AnyOfChild >= 2
16:         for each AnyOfChild in AnyOf do
17:             get.AllOfChild
18:             for each AllofChild in AllOf do
19:                 if AllofChild != AnyOf
20:                     k <- getAttributeValue
21:                     if num(AttributeValue) >=2
22:                         temp_table[] <- k
23:                     else
24:                         table[] <- k
25:                     endif
26:                 else
27:                       Logical_expr <- Logical_expr + handleAnyOf(AnyOf)
28:                 endif
29:             endfor
30:             temp_string= add "and" between each table_item in temp_table
31:             table[] <- temp_string
32:         endfor
33:         Logical_expr= Logical_expr + (add "or" between each table_item in table)
34:     else
35:         for each AnyOfChild in AnyOf do
36:             get.AllOfChild
37:             for each AllofChild in AllOf do
38:                 if AllofChild != AnyOf
39:                   k <- getAttributeValue
40:                   table[]<- k
41:                 else
42:                   Logical_expr <- Logical_expr + handleAnyOf(AnyOf)
43:                 endif
44:             endfor
45:         endfor
46:         Logical_expr <- Logical_expr + (add "and" between each table_item in table)
47:     endif
48:     return Logical_expr
49: Endfunction
```

Εικόνα 4.2 Αλγόριθμος Μετατροπής XACML σε ABE

Στο συγκεκριμένο αλγόριθμο πρέπει να δοθεί σημαντική προσοχή καθώς ο συγκεκριμένος είναι που δίνει την δυνατότητα να συνυπάρχουν ABE και ABAC μεταξύ τους. Αποτελείται από 2 συναρτήσεις με την κάθε μια να έχει και μια συγκεκριμένη λειτουργία. Ο σκοπός αυτού του αλγορίθμου είναι να δέχεται μια πολιτική ελέγχου πρόσβασης βάσει χαρακτηριστικών(ABAC) η οποία θα παρέχεται από ένα πρότυπο XACML σε αρχείο XML και θα το μετατρέπει σε λογική έκφραση έτσι ώστε στην συνέχεια να χρησιμοποιηθεί για την κρυπτογράφηση των αρχείων μέσω της ABE. Στην πράξη πρέπει να μετατρέψει μια πολιτική εξουσιοδότησης σε ένα ABE Tree που εκφράζει μια λογική έκφραση όπως στο παρακάτω παράδειγμα.



Εικόνα 4.3 ABE Tree

- **AbacToAbe(String Pathfile):** Η συγκεκριμένη συνάρτηση είναι και η πιο βασική του αλγορίθμου. Αρχικά παίρνει σαν όρισμα ένα αλφαριθμητικό το οποίο θα δηλώνει την τοποθεσία του αρχείου πολιτικής εξουσιοδότησης(XACML) στο σύστημα και θα επιστρέφει μια λογική έκφραση. Στην γραμμή 2 Αρχικοποιει το αλφαριθμητικό Logical_expr που θα επιστρέψει η συνάρτηση. Στην γραμμή 3 εγκαταστατεί τον αναλυτή στο αρχείο. Η γραμμές 4-6 δηλώνουν τους κόμβους-ετικέτες από τις ετικέτες Rule,Target και AnyOf. Στην γραμμή 7 γίνεται ο πρώτος έλεγχος ο οποίος ελέγχει το χαρακτηριστικό Effect από τον κόμβο Rule αν είναι ίσο με Permit. Στην περίπτωση που είναι ίσο με Permit ο αλγόριθμος συνεχίζει στην γραμμή 8 όπου επιστρέφει το αλφαριθμητικό Logical_expr το οποίο είναι ίσο με την υποσυναρτηση handleAnyOf. Στην περίπτωση όμως που δεν είναι ίσο με Permit πηγαίνει στην γραμμή 10, τότε ο αλγόριθμος επιστρέφει το αλφαριθμητικό Logical_expr το οποίο είναι ίσο με την υποσυναρτηση handleAnyOf με ένα θαυμαστικό από μπροστά «!» το οποίο δηλώνει την λογική λέξη κλειδί NOT.

- **handleAnyOf(Node AnyOf):** Η συνάρτηση αυτή είναι εξίσου σημαντική καθώς μέσω αυτής καθορίζονται οι λογικές λέξεις κλειδιά (AND,OR) μαζί με τα χαρακτηριστικά που βρίσκονται μέσα στην πολιτική. Ο σκοπός της είναι ότι εκμεταλλεύεται την δομή του πρότυπου της XACML έτσι ώστε να εξάγει την λογική έκφραση με τα χαρακτηριστικά που χρειάζεται η ABE για να κρυπτογραφήσει τα δεδομένα και να δημιουργήσει το *ciphertext*. Πιο συγκεκριμένα στην γραμμή 12 δηλώνεται η συνάρτηση αυτή και παίρνει σαν όρισμα ένα κόμβο-ετικέτα AnyOf. Στην γραμμή 13 δηλώνεται το αλφαριθμητικό Logical_expr το οποίο θα επιστραφεί στο τέλος. Η γραμμή 14 λαμβάνει τα παιδιά (AllOf) του κόμβου-ετικέτα AnyOf. Στην γραμμή 15 γίνεται ένας έλεγχος για το αν τα παιδιά του κόμβου-ετικέτα AnyOf είναι παραπάνω ή ίσα από 2. Στην γραμμή 16 έχει μπει στην περίπτωση να ισχύει ο παραπάνω έλεγχος, και να δημιουργείται μια επανάληψη ίσα με το νούμερο των παιδιών του AnyOf. Η γραμμή 17 λαμβάνει τα παιδιά του AllOf. Η γραμμή 18 με την σειρά της δημιουργεί μια επανάληψη ίσα με το νούμερο των παιδιών του κόμβου-ετικέτα AllOf. Η γραμμή 19 ελέγχει αν δεν υπάρχει εμφολευμένος κόμβος-ετικέτα AnyOf (δηλαδή να είναι παιδί του κόμβου-ετικέτα AllOf). Αν μεταφερθεί ο αλγόριθμος στην γραμμή 20 τότε ισχύει ο παραπάνω έλεγχος και αποθηκεύει την τιμή των χαρακτηριστικών στο k. Στην γραμμή 21 γίνεται ακόμα ένας έλεγχος οποίος βλέπει αν τα χαρακτηριστικά είναι παραπάνω ή ίσα από 2 έτσι ώστε αν ισχύει, το k να αποθηκευτεί σε έναν προσωρινό πίνακα. Αν δεν ισχύει τότε μεταφέρεται στην γραμμή 24 όπου το k θα αποθηκευτεί στον βασικό πίνακα της συνάρτησης. Στην γραμμή 27 ο αλγόριθμος θα μεταφερθεί

αν βρει ο έλεγχος τις γραμμής 19 ένα εμφολευμένο κόμβο-ετικέτα AnyOf έτσι ώστε μετα το αλφαριθμητικό Logical_expr θα γίνει ίσο με τον εαυτό του συν την ίδια την συνάρτηση η οποία θα κάνει αναδρομή. Στην γραμμή 30 δημιουργείται ένα προσωρινό αλφαριθμητικό το οποίο θα είναι ίσο με το Join του προσωρινού πίνακα με την λέξη κλειδί AND, και στην συνέχεια αυτό θα μπει σαν ένα στοιχείο στον βασικό πίνακα της συνάρτησης. Αφού τελειώσει η επανάληψη, μετα το Logical_expr θα πάρει την τιμή του εαυτού του συν το Join του βασικού πίνακα με την λέξη κλειδί OR στην γραμμή 33.
Στην περίπτωση που δεν ισχύει ο έλεγχος στην γραμμή 15 τότε τα πράγματα είναι πιο εύκολα για τον αλγόριθμο. Στην γραμμή 35 δημιουργείται μια επανάληψη ίσα με το νούμερο των παιδιών του κόμβου-ετικέτα AnyOf. Στην γραμμή 36 παίρνει ο αλγόριθμος όλα τα παιδιά του κόμβου-ετικέτα AllOf. Στην γραμμή 38 ελέγχει αν δεν υπάρχει εμφολευμενη AnyOf έτσι ώστε αν ισχύει αυτή συνθήκη να αποθηκεύσει σε ένα k τις τιμές των χαρακτηριστικών και στην συνέχεια αυτό να αποθηκευτεί στον βασικό πίνακα. Αν τώρα δεν ισχύει η συνθήκη μεταφέρεται ο αλγόριθμος στην γραμμή 42 όπου το Logical_expr θα γίνει ίσο με τον εαυτό του συν την ίδια την συνάρτηση που θα κάνει αναδρομή. Αφού τελειώσει η επανάληψη, στην γραμμή 46 το Logical_expr θα γίνει ίσο με τον εαυτό του συν το Join που θα γίνει στο βασικό πίνακα με την λέξη κλειδί AND. Τέλος στην γραμμή 48 θα επιστραφεί το Logical_expr.

ΚΕΦΑΛΑΙΟ 5 ΣΥΣΤΗΜΑ ΜΕΤΑΤΡΟΠΗΣ XACML ΣΕ ABE

(5.1 ΕΙΣΑΓΩΓΗ)

Όπως αναφέρθηκε και παραπάνω, η συνεργασία αναμεσά στο ABAC με το ABE προσφέρουν σημαντικά προνομία πάνω στην ασφάλεια και στην προσαρμοστικότητα σε μεγάλα συστήματα και οργανισμούς όπως για παράδειγμα τα συστήματα υγείας. Παρακάτω σε αυτό το κεφάλαιο θα παρουσιαστεί ένα σύστημα υγειάς γραμμένο στην γλώσσα προγραμματισμού Java, το οποίο αξιοποιεί αυτό το μοντέλο ασφάλειας δεδομένων και έχει σαν στόχο την κρυπτογράφηση δεδομένων από ασθενείς και τον έλεγχο πρόσβασης από συγκεκριμένους ιατρούς. Η παρακάτω υλοποίηση βρίσκεται στο διαδίκτυο. (https://github.com/krotskas/Converter-XACML-to-ABE)

(5.2 ΣΕΝΑΡΙΑ ΚΑΙ ΑΠΑΙΤΗΣΕΙΣ)

Στην συγκεκριμένη υλοποίηση η απαιτήσεις είναι οι πολύ βασικές για ένα μοντέλο ABAC/ABE και παρουσιάζονται παρακάτω:

- Η εφαρμογή θα πρέπει να χρησιμοποιεί αλγόριθμους και πρωτόκολλα κρυπτογράφησης κατά τα πρότυπα του κλάδου για την προστασία των δεδομένων των ασθενών.
- Να μπορεί να αποκρυπτογραφεί το ιστορικό του ασθενή από κάποιον ιατρό με παρόμοια χαρακτηριστικά, χαρακτηριστικά περιβάλλοντος και δράσης.
- Να υπάρχουν πολιτικές εξουσιοδότησης με βάσει κάποια χαρακτηριστικά του ασθενή, του περιβάλλοντος, του χρήστη και της δράσης.
- Να υπάρχει ο αλγόριθμος μετατροπής από ABAC σε ABE.
- Να υπάρχει ένας τρόπος αποθήκευσης για τα δεδομένα των υποκειμένων και των ασθενών.
- Να υπάρχει ένα βασικό μενού για επικοινωνία του συστήματος με το υποκείμενο.
- Σε περίπτωση μη αυθεντικοποίησης του αρχείου να παρουσιάζει ένα μήνυμα ότι δεν δίνεται έγκριση για πρόσβαση στο αρχείο.
- Να μπορεί το υποκείμενο να ανεβάσει ένα καινούριο αρχείο ασθενή.
- Να μπορεί το υποκείμενο να ψάχνει μέσω του μοναδικού patient_id τον ασθενή και να κάνει request για πρόσβαση στο αρχείο.
- Σε περίπτωση λανθασμένου patient_id να εμφανίσει μήνυμα το σύστημα να ξανα προσπαθήσει με ένα έγκυρο patient_id αυτή την φορά.

Σε ένα πιο επαγγελματικό σύστημα, θα μπορούσαν να ισχύουν ακόμα και οι παρακάτω απαιτήσεις:

- Η εφαρμογή θα πρέπει να δημιουργηθεί χρησιμοποιώντας μια ασφαλή γλώσσα προγραμματισμού και αρχιτεκτονική.

- Για τη διασφάλιση των δεδομένων των ασθενών και τη χορήγηση πρόσβασης σε εξουσιοδοτημένο προσωπικό υγείας, η εφαρμογή θα πρέπει να χρησιμοποιεί κρυπτογράφηση βάσει χαρακτηριστικών (ABE).

- Για να διασφαλιστεί ότι μόνο εξουσιοδοτημένοι εργαζόμενοι μπορούν να έχουν πρόσβαση στα δεδομένα των ασθενών, η εφαρμογή πρέπει να διαθέτει σύστημα διαχείρισης χρηστών που να ορίζει σαφώς τους ρόλους και τα δικαιώματα των χρηστών.

- Η εφαρμογή θα πρέπει να περιλαμβάνει ένα σύστημα ελέγχου και καταγραφής που παρακολουθεί τη συμπεριφορά των χρηστών και τηρεί αρχείο όλων των λειτουργιών που πραγματοποιούνται στα δεδομένα των ασθενών.

- Σε περίπτωση βλάβης του συστήματος ή άλλης έκτακτης ανάγκης, η εφαρμογή θα πρέπει να διαθέτει σχέδιο δημιουργίας αντιγράφων ασφαλείας και αποκατάστασης μετά από καταστροφή, ώστε να διασφαλίζεται ότι τα δεδομένα των ασθενών δεν θα καταστραφούν.

- Η εφαρμογή πρέπει να συμμορφώνεται με όλους τους ισχύοντες νόμους περί προστασίας δεδομένων και ιδιωτικότητας, όπως ο HIPAA στις ΗΠΑ ή ο Γενικός Κανονισμός για την Προστασία των Δεδομένων(General Data Protection Regulation – GDPR) στην ΕΕ.

- Η εφαρμογή θα πρέπει να διαθέτει ασφαλές σύστημα διαχείρισης κλειδιών για να διασφαλίζει ότι τα κλειδιά κρυπτογράφησης προστατεύονται και δεν είναι προσβάσιμα σε μη εξουσιοδοτημένο προσωπικό.

- Η εφαρμογή θα πρέπει να διαθέτει φιλικό προς το χρήστη περιβάλλον εργασίας που είναι εύκολο στη χρήση και την πλοήγηση για τους επαγγελματίες υγείας και τους ασθενείς.

- Η εφαρμογή θα πρέπει να διαθέτει ασφαλές σύστημα σύνδεσης που χρησιμοποιεί ισχυρές μεθόδους ελέγχου ταυτότητας, όπως έλεγχο ταυτότητας δύο παραγόντων ή βιομετρικό έλεγχο ταυτότητας.

- Η εφαρμογή θα πρέπει να ελέγχεται τακτικά για ευπάθειες και να ενημερώνεται με επιδιορθώσεις ασφαλείας και διορθώσεις σφαλμάτων ανάλογα με τις ανάγκες.

- Η εφαρμογή θα πρέπει να είναι επεκτάσιμη και ικανή να διαχειρίζεται μεγάλο όγκο δεδομένων ασθενών, διατηρώντας παράλληλα τις επιδόσεις και την ασφάλεια.

Τα σενάρια στην συγκεκριμένη υλοποίηση του συστήματος είναι 2 βασικά μέρη, τα οποία περιγράφονται παρακάτω. Αρχικά το υποκείμενο συνδέεται με τα εξής χαρακτηριστικά:

- *Id=12345*
- *Username=John Davies*
- *Email=JDavies@gmail.com*
- *Sector=Πνευμονολογικό*
- Hospital=*ΓΝ Λαμίας*

Και του δίνεται η δυνατότητα να παρακολουθήσει κάποια εκ των αρχεία ασθενών ή να καταχωρήσει ο ίδιος ένα ιατρικό αρχείο ασθενή.

Το πρώτο σενάριο είναι ότι το υποκείμενο θέλει να ανεβάσει ένα καινούριο αρχείο ασθενή, επομένως πληκτρολογεί την επιλογή που του δίνει το menu για την καταχώρηση καινούριου αρχείου. Στην αρχή το σύστημα τον ρωτάει το ονοματεπώνυμο του ασθενή αλλά και την τοποθεσία του νοσοκομείου μαζί και σε ποιο τμήμα του κρατείται ο ασθενής. Στην συνέχεια το σύστημα τον επιβάλει να καταχωρήσει μια πολιτική εξουσιοδότησης ελέγχου πρόσβασης βάσει χαρακτηριστικών, την οποία την έχει αποθηκεύσει σε μια δικιά του τοποθεσία το υποκείμενο. Τέλος το αρχείο αποθηκεύεται ασφαλές και κρυπτογραφημένο στο σύστημα.

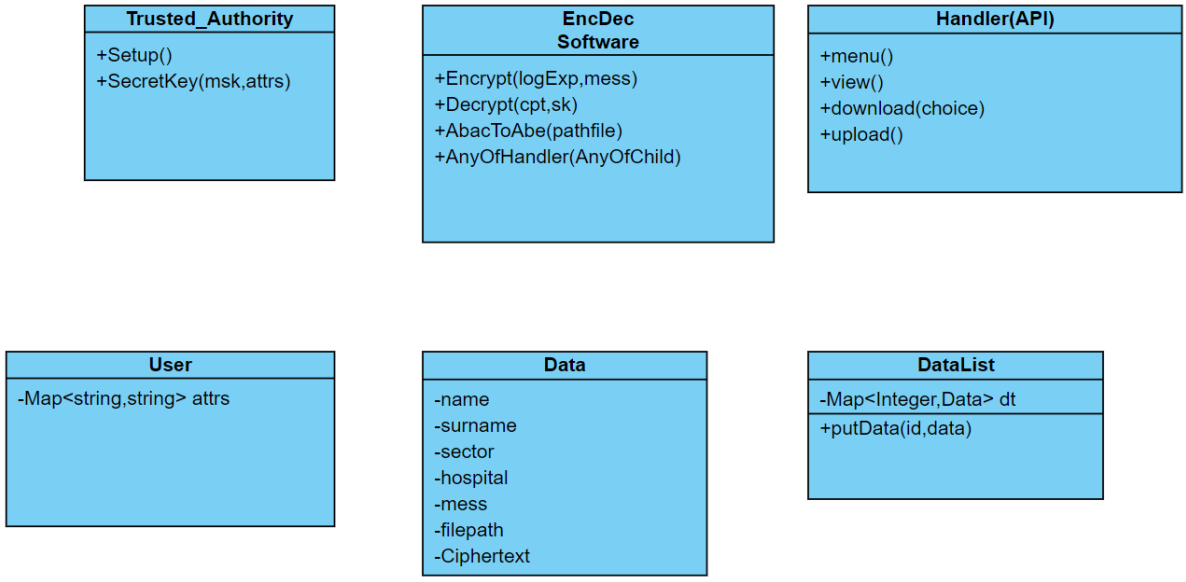
Το δεύτερο σενάριο είναι όταν το υποκείμενο θα χρειαστεί να δει ένα ιατρικό αρχείο ασθενή. Αρχικά θα χρειαστεί να επιλέξει την επιλογή για την παρουσίαση όλων των ασθενών στον οργανισμό από το menu επίλογων. Έπειτα θα πληκτρολογήσει το μοναδικό patient_id του ασθενή που θέλει να παρακολουθήσει. Αν τα χαρακτηριστικά του ασθενή είναι ιδιά με αυτού του υποκειμένου, δηλαδή ($SECTOR_{patient}$= *Πνευμονολογικό AND* $HOSPITAL_{patient}$=*ΓΝ Λαμίας)* τότε γίνεται αποδεκτή η πρόσβαση και κρυπτογραφείται το ιστορικό υγείας του ασθενή. Αν τώρα τα χαρακτηριστικά είναι διαφορετικά θα εμφανιστεί στην οθόνη το μήνυμα *You Don't have the Authority!!!*.

Κάλλιστα όμως θα μπορούσε σε ένα επαγγελματικό περιβάλλον, τα σενάρια να ήταν περισσότερα με πιο πολλές και ευέλικτες δυνατότητες για το υποκείμενο. Αρχικά αν και δεν επιτρέπεται να εξετάζει τις προσωπικές πληροφορίες του ασθενούς, ένας νοσηλευτής πρέπει να έχει πρόσβαση στο ιστορικό του ασθενούς. Το σύστημα ΑΒΕ θα διατηρεί τις προσωπικές πληροφορίες κρυπτογραφημένες και θα επιτρέπει μόνο στον νοσηλευτή να δει το ιστορικό του. Επίσης ένα μέλος της ιατρικής ομάδας που εργάζεται από απόσταση πρέπει να έχει πρόσβαση στα δεδομένα του ασθενούς. Το μέλος του προσωπικού θα έχει ασφαλή απομακρυσμένη πρόσβαση στα απαιτούμενα δεδομένα χρησιμοποιώντας το σύστημα ΑΒΕ, προστατεύοντας το απόρρητο των ασθενών και την ασφάλεια των δεδομένων. Σε περίπτωση τώρα που απαιτείται απομακρυσμένη πρόσβαση των ασθενών στους δικούς τους ιατρικούς φακέλους, ο ασθενής θα έχει ασφαλή πρόσβαση στα δεδομένα του μέσω του συστήματος ΑΒΕ και η προστασία της ιδιωτικής ζωής του θα είναι εγγυημένη. Τέλος το ιστορικό και οι προσωπικές πληροφορίες κάθε ασθενούς θα είναι σε θέση να κοινοποιούνται με ασφάλεια τις πληροφορίες ασθενούς στον ειδικό χρησιμοποιώντας το σύστημα ΑΒΕ, διατηρώντας τις κρυπτογραφημένες και περιορίζοντας την πρόσβαση μόνο σε εξουσιοδοτημένους υπαλλήλους.

(5.3 ΣΧΕΔΙΑΣΗ)

(5.3.1 ΔΙΑΓΡΑΜΜΑ ΚΛΑΣΕΩΝ UML)

Το σύστημα διαθέτει έξι βασικές κλάσεις οι οποίες αποτελούνται από τα παρακάτω χαρακτηριστικά (variables,methods):



Εικόνα 5.1 Διάγραμμα Κλάσεων

- **Trusted_Authority Class:** Η συγκεκριμένη κλάση είναι η οντότητα που αναφέρθηκε στο Κεφάλαιο 4.2(Αρχή Χαρακτηριστικών) η οποία κάνει εγκατάσταση το σύστημα και εξάγει στους χρήστες του οργανισμού τα προσωπικά τους κλειδιά. Πιο συγκεκριμένα:
  - Η μέθοδος *Setup()* επιστρέφει ένα mastery_key.
  - Η μέθοδος *SecretKey(msk,attrs)* δίνει σε κάθε υποκείμενο ένα προσωπικό κλειδί ανάλογα με τα χαρακτηριστικά που έχει αυτό αλλά και τα δεδομένα του περιβάλλοντος και της ενέργειας προς το αντικείμενο, και χρησιμοποιεί σαν βάση το mastery_key που εκδόθηκε από την μέθοδο *Setup()*.

- **EncDecSoftware Class:** Αυτή η κλάση κατέχει τις τέσσερις πιο σημαντικές μεθόδους που ασφαλίζουν το σύστημα. Αρχικά:
  - Η μέθοδος *Encrypt(logExp,mess)* επιστρέφει στο σύστημα ένα κρυπτογραφημένο μήνυμα(*ciphertext*) το οποίο έχει κρυπτογραφηθεί με μια λογική έκφραση.
  - Κατόπιν η μέθοδος *Decrypt(cpt,sk)* αποκρυπτογραφεί το κρυπτογραφημένο μήνυμα(*ciphertext*) μόνο αν κατέχει το υποκείμενο που θέλει να κάνει αυτή την ενέργεια το ανάλογο *secret_key* με τα ορθά κρυπτογραφημένα χαρακτηριστικά.
  - Στην συνέχεια παρουσιάζεται ο αλγόριθμος AbacToAbe(pathfile) με την υποσυναρτηση AnyOfHandler(AnyOfChild), τον οποίο τον αναλύσαμε στο υποκεφάλαιο 4.2.1.
- **Handler(API) Class:** Η Κλάση αυτή δημιουργήθηκε για να διευκολύνει το υποκείμενο να επικοινωνεί με το σύστημα και με τα δεδομένα του ασθενή. Πιο συγκεκριμένα:
  - Υπάρχει η μέθοδος *menu()* η οποία δημιουργεί ένα menu επίλογων για το υποκείμενο και ανάλογα με το τι θα επιλέξει αυτό θα ενεργήσει το σύστημα.

- Επίσης η παραπάνω κλάση κατέχει την μέθοδο *upload()* στην οποία το υποκείμενο έχει την δυνατότητα να ανεβάσει ένα ιατρικό αρχείο ασθενή και να κρυπτογραφηθεί από το σύστημα.
- Η μέθοδος *Download(choice)* δέχεται σαν όρισμα ένα id που αντιπροσωπεύει έναν μοναδικό ασθενή, το οποίο id θα εισέρχεται από το υποκείμενο που θέλει να δει τα δεδομένα του ασθενή. Σε περίπτωση που έχει την έγκριση από το σύστημα ABAC/ABE τότε η μέθοδος *view()* θα εμφανίσει τα δεδομένα στην οθόνη του υποκειμένου αποκρυπτογραφημένα.

- **User Class:** Η κλάση αυτή περιέχει ένα Map<string,string> στο οποίο αποθηκεύεται το υποκείμενο με τα διαφορά χαρακτηριστικά που μπορεί να έχει και τις τιμές τους.

- **Data Class:** Η συγκεκριμένη κλάση λειτουργεί σαν καλούπι για τα δεδομένα που μπορεί να έχει ένα ιατρικό αρχείο ασθενή. Περιέχει:
  - *Όνομα Ασθενή*
  - *Επίθετο Ασθενή*
  - *Τμήμα Νοσοκομείου*
  - *Τοποθεσία Νοσοκομείου*
  - *Περιεχόμενο*
  - Τοποθεσία Αρχείου XACML πολιτικής
  - *Ciphertext*

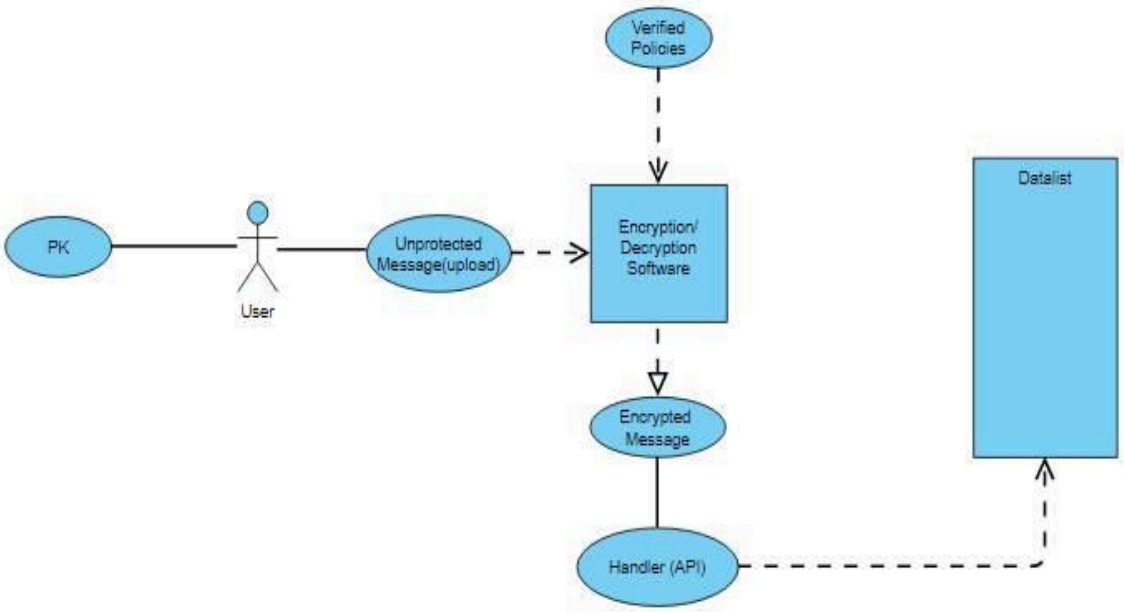
- **DataList Class:** Η κλάση αυτή λειτουργεί σαν τρόπο αποθήκευσης των δεδομένων ιατρικών αρχείων ασθενών. Περιέχει ένα Map <Integer,Data> με το Integer να δηλώνει το Id ενός ασθενή και τα Data τις πληροφορίες το ιατρικού αρχείου. Σε ένα επαγγελματικό σύστημα καλό θα ήταν να υπήρχε μια βάση δεδομένων για αποθήκευση όλων των στοιχείων στο σύστημα.

(5.3.2 ΔΙΑΓΡΑΜΜΑΤΑ ΠΕΡΙΠΤΩΣΕΩΝ ΧΡΗΣΗΣ UML)

Ο σκοπός των διαγραμμάτων αυτών είναι να δώσουν μια σαφή και συνεπή περιγραφή για το τι θα πρέπει να κάνει ακριβώς το σύστημα αλλά και με ποιο τρόπο θα επαληθεύονται τα στοιχεία του συστήματος για να νιώθει η κοινότητα του οργανισμού ασφαλής.

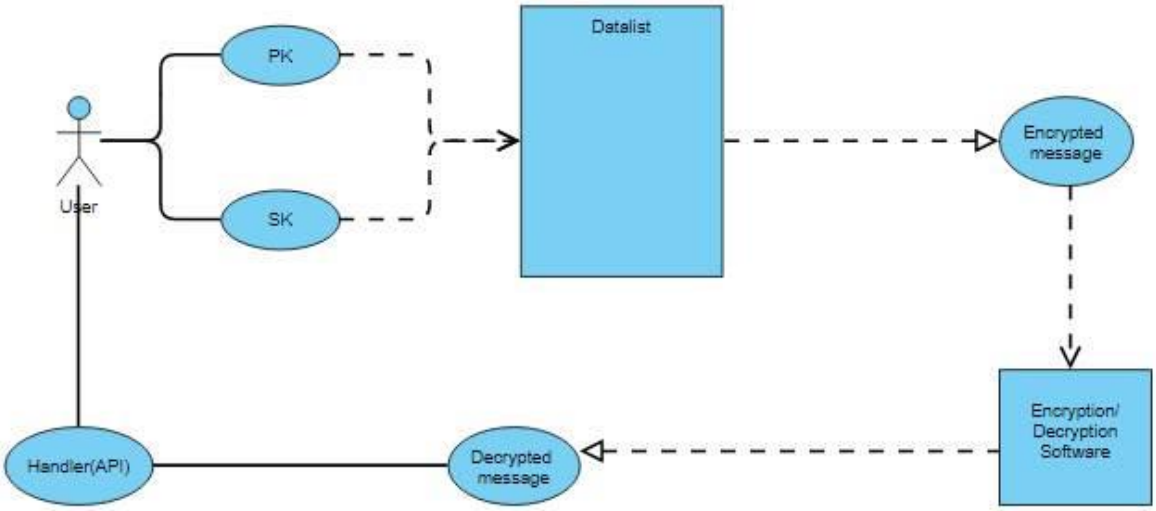
1. **Διάγραμμα Χρήσης για την Κρυπτογράφηση:**
   a. Το πρώτο βήμα είναι το υποκείμενο να λάβει από το Trusted Authority το δημόσιο κλειδί (Public Key - PK).
   b. Στην συνέχεια το υποκείμενο προσθέτει ότι δεδομένα θέλει στο ιατρικό αρχείο του ασθενή.

c. Κατόπιν η κλάση Encryption/Decryption Software λαμβάνει τα απροστάτευτα δεδομένα και τις πολίτικες εξουσιοδότησης (XACML) μέσω του αλγορίθμου AbacToAbe και γίνεται η κρυπτογράφηση με την βοήθεια της συνάρτησης Encrypt.
d. Τέλος το κρυπτογραφημένο μήνυμα αποθηκεύεται μέσω του Handler(API) στο Map Datalist.



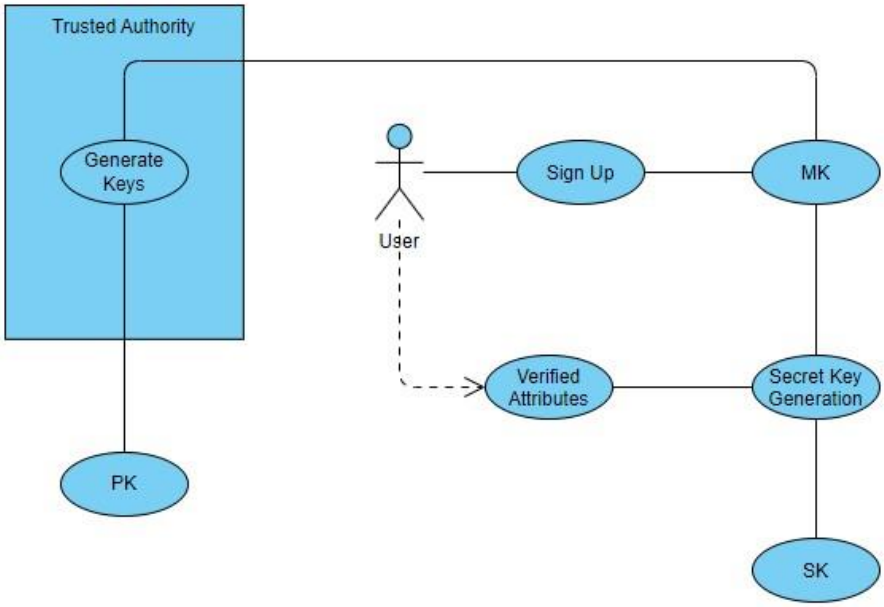
Εικόνα 5.2 Διάγραμμα Χρήσης Encryption

2. **Διάγραμμα Χρήσης για την Αποκρυπτογράφηση:**
   a. Αρχικά το υποκείμενο χρησιμοποιεί το προσωπικό του κλειδί(Secret Key - SK) με το δημόσιο κλειδί(PK).
   b. Στην συνέχεια επιλεγεί ποιο ιατρικό αρχείο ασθενή θέλει να παρακολουθήσει.
   c. Στο backend κομμάτι τώρα το SK θα προσπαθήσει να ξεκλειδώσει το κρυπτογραφημένο μήνυμα μέσω της συνάρτησης Decrypt.
   d. Στην περίπτωση που η πολιτική εξουσιοδότησης εγκρίνει την πρόσβαση τότε αναλαμβάνει το Handler(API) και παραδίδει στον χρήστη το αποκρυπτογραφημένο μήνυμα.



Εικόνα 5.3 Διάγραμμα Χρήσης Decryption

3. **Διάγραμμα Χρήσης για την Εγκατάσταση:**
    a. Αρχικά το Trusted Authority εκδίδει ένα Public Key(PK) και ένα Mastery Key(MK). Το συγκεκριμένο βήμα γίνεται μόνο μια φορά στο ξεκίνημα του συστήματος.
    b. Σε κάθε εγγραφή υποκείμενου στο σύστημα εκδίδεται από το Trusted Authority μέσω του Mastery Key ένα προσωπικό Secret Key(SK) με βάση τα χαρακτηριστικά που εξαρτιούνται από τον ίδιο το χρήστη.

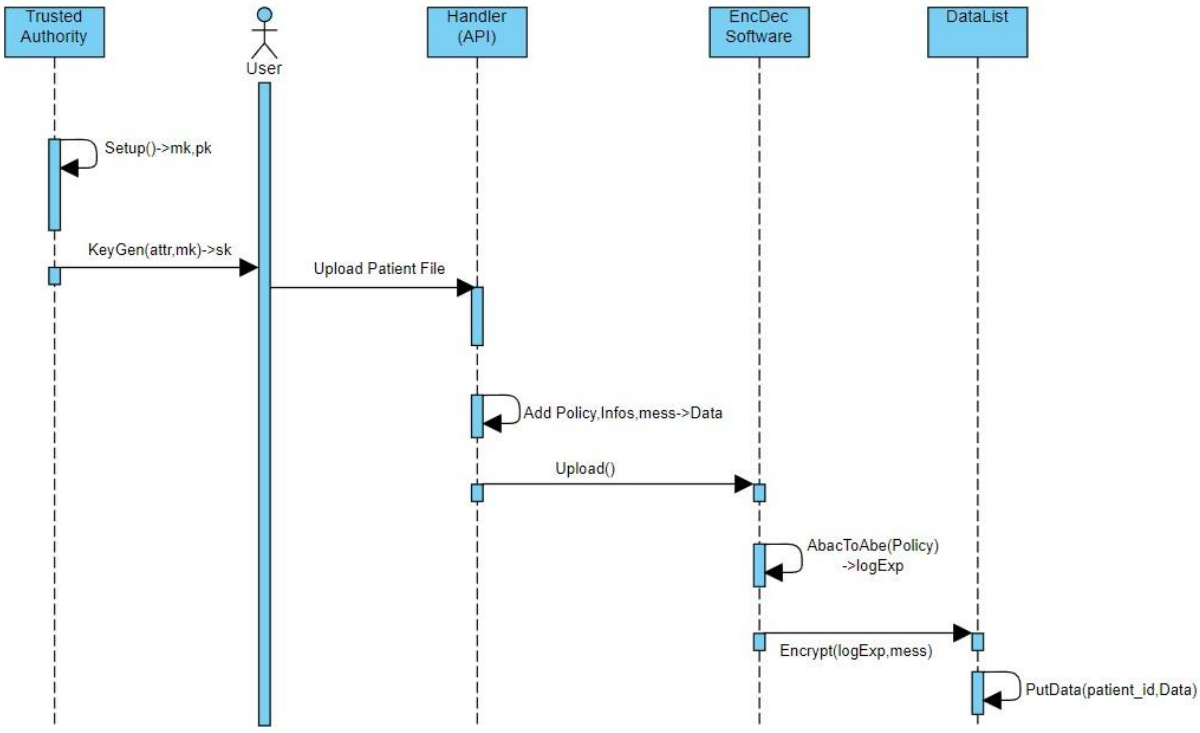


Εικόνα 5.4 Διάγραμμα Χρήσης Εγκατάστασης

(5.3.3 ΔΙΑΓΡΑΜΜΑΤΑ ΑΚΟΛΟΥΘΙΑΣ UML)

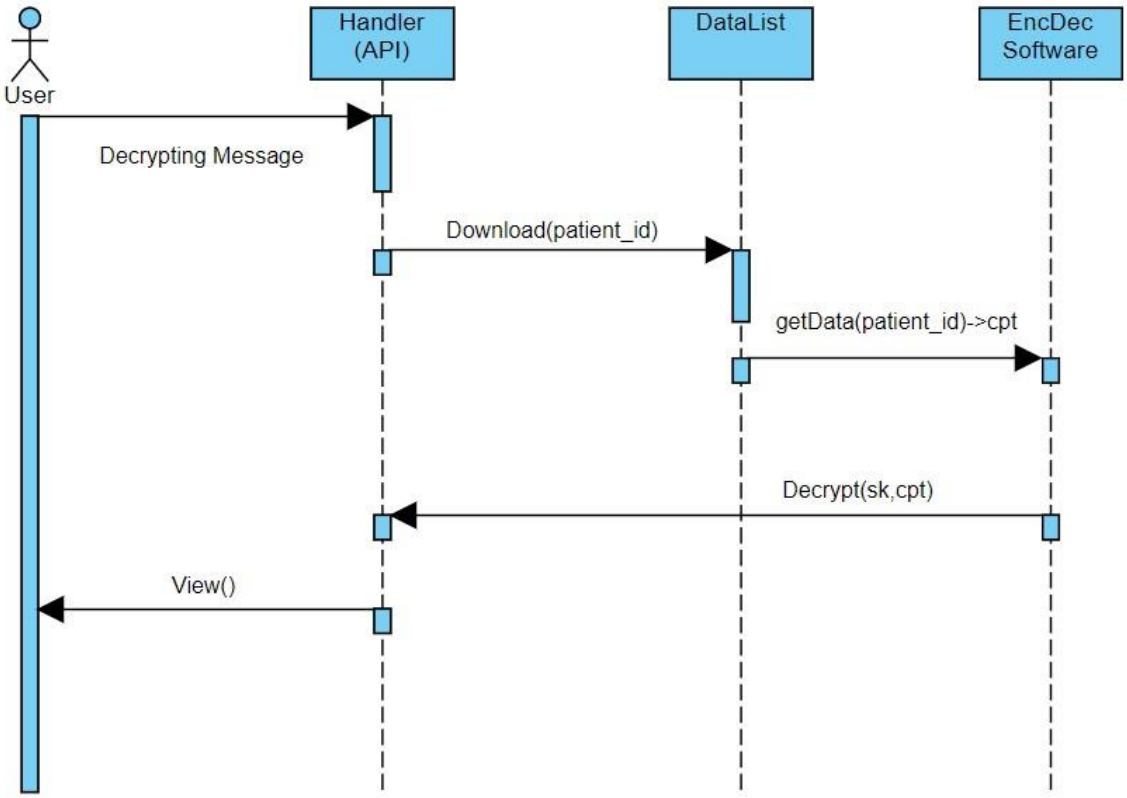
Τα παρακάτω διαγράμματα περιγράφουν την επικοινωνία των αντικειμένων και την όλη εξέλιξη που μπορεί να έχει το σύστημα με σκοπό την διασφάλιση του ιατρικού απορρήτου στον οργανισμό.

1. **Διάγραμμα Ακολουθίας Κρυπτογράφησης:**
   a. Το πρώτο πράγμα που γίνεται στο σύστημα είναι να εγκαταστήσει το Trusted Authority το όλο μοντέλο και να εκδώσει τα κλειδιά σε όσα υποκείμενα είναι στο σύστημα μέσω της μεθόδου KeyGen(attr,msk).
   b. Στην συνέχεια το υποκείμενο επιλέγει την ενέργεια να ανεβάσει ένα ιατρικό αρχείο ασθενή.
   c. Το σύστημα και πιο συγκεκριμένα η οντότητα Handler(API) του ζητάει να εκχωρήσει κάποιες πληροφορίες όπως την πολιτική εξουσιοδότησης, τον τομέα του νοσοκομείου αλλά και την τοποθεσία του αλλά και το ονοματεπώνυμο και το μήνυμα που θέλει να κρυπτογραφήσει το σύστημα.
   d. Στην συνέχεια η μέθοδος Upload() στέλνει όλες τις πληροφορίες που εκχώρησε το υποκείμενο και ο αλγόριθμος AbacToAbe μετατρέπει την πολιτική εξουσιοδότησης σε λογική έκφραση.
   e. Ακολουθεί η συνάρτηση Encrypt(logExp,mess) όπου θα δεχτεί σαν ορίσματα την λογική έκφραση από το βήμα d και το μήνυμα που πρέπει να γίνει κρυπτογραφημένο.
   f. Τέλος αφού γίνει επιτυχώς η κρυπτογράφηση το σύστημα μέσω της συνάρτησης PutData αποθηκεύει το αρχείο ασθενή στο Map DataList.



Εικόνα 5.5 Διάγραμμα Ακολουθίας Encryption

2. **Διάγραμμα Ακολουθίας Αποκρυπτογράφησης:**
   a. Σε περίπτωση που το υποκείμενο αποφασίσει να δει ένα ιατρικό αρχείο ασθενή τότε, θα πρέπει ο ίδιος να γράψει στο σύστημα το μοναδικό Id ασθενή που θα θέλει να παρακολουθήσει, στην συνέχεια ο Handler(API) θα ενεργοποιήσει την μέθοδο download του αρχείου ασθενή.
   b. Κατόπιν θα στείλει το σύστημα τα δεδομένα του αρχείου στην κλάση Encodes Software.
   c. Η μέθοδος Decrypt θα αναλάβει δράση και θα προσπαθήσει να αποκρυπτογραφήσει το μνήμα(*ciphertext*) μέσα στο αρχείο με βάση το secret key του υποκείμενου και την πολιτική εξουσιοδότησης.
   d. Αν εγκριθεί η πρόσβαση τότε το μήνυμα θα αποκρυπτογραφηθεί και θα εμφανιστεί στο υποκείμενο μέσω της view συνάρτησης. Στην περίπτωση όμως που δεν έχει αυθεντικοποιηθει σωστά η ταυτότητα του υποκειμένου με το ιατρικό αρχείο ασθενή τότε η μέθοδος view θα στείλει ένα μήνυμα σε αυτό ότι δεν έχει Authority.



Εικόνα 5.6 Διάγραμμα Ακολουθίας Decryption

(5.4 ΕΡΓΑΛΕΙΑ)

Για την πραγμάτωση αυτού του συστήματος χρειάστηκαν κάποια εργαλεία για την σχεδίαση και κάποιες βιβλιοθήκες της γλώσσας προγραμματισμού Java για την υλοποίηση των μεθόδων που είδαμε παραπάνω. Πιο συγκεκριμένα χρησιμοποιήθηκαν:

- **Java (Java JDK 13 Azul Zulu 13.0.13)**: Η Java είναι μια δημοφιλής αντικειμενοστραφής γλώσσα προγραμματισμού που κυκλοφόρησε για πρώτη φορά το 1995 από τη Sun Microsystems. Χρησιμοποιείται ευρέως για την ανάπτυξη ποικίλων εφαρμογών, συμπεριλαμβανομένων εφαρμογών για υπολογιστές γραφείου, διαδικτύου και κινητών τηλεφώνων, καθώς και συστημάτων επιχειρήσεων μεγάλης κλίμακας. Η Java είναι γνωστή για τη φορητότητά της, πράγμα που σημαίνει ότι μπορεί να εκτελεστεί σε οποιαδήποτε πλατφόρμα διαθέτει Java Virtual Machine (JVM), καθιστώντας την ιδανική γλώσσα για την κατασκευή εφαρμογών πολλαπλών πλατφορμών. Η γλώσσα έχει σχεδιαστεί για να είναι απλή, εύκολη στην εκμάθηση και εξαιρετικά ασφαλής, με ενσωματωμένα χαρακτηριστικά για τη διαχείριση μνήμης και το χειρισμό εξαιρέσεων. Η Java υποστηρίζει επίσης πολυνηματικότητα, επιτρέποντας στα προγράμματα να εκτελούν ταυτόχρονα πολλαπλές εργασίες, γεγονός που την καθιστά δημοφιλή επιλογή για την ανάπτυξη εφαρμογών υψηλής απόδοσης. Συνολικά, η Java διαθέτει μια μεγάλη και ενεργή κοινότητα προγραμματιστών, με πολυάριθμες βιβλιοθήκες και πλαίσια διαθέσιμα για τη γρήγορη και αποτελεσματική δημιουργία εφαρμογών.

- **DOMParser(Για την ανάλυση του XACML αρχείου):** Η γλώσσα προγραμματισμού Java παρέχει την κλάση DOMParser, η οποία επιτρέπει στους προγραμματιστές να αναλύουν έγγραφα XML και να τα μετατρέπουν στο Μοντέλο Αντικειμένου Εγγράφου (DOM). Η αναπαράσταση ενός εγγράφου XML στη μνήμη, γνωστή ως DOM, μπορεί να τροποποιηθεί με τη βοήθεια μιας γλώσσας υπολογιστών όπως η Java. Ο DOMParser είναι ένας αναλυτής που δημιουργεί ένα δέντρο DOM στη μνήμη μετά την ανάγνωση ενός ολόκληρου εγγράφου XML. Η δομή και το περιεχόμενο του εγγράφου XML αναπαρίστανται από μια ιεραρχία κόμβων που ονομάζονται κόμβοι κειμένου, στοιχεία και χαρακτηριστικά που αποτελούν το δέντρο DOM. Οι προγραμματιστές μπορούν στη συνέχεια να πλοηγηθούν και να εργαστούν με τους κόμβους του δέντρου DOM για να έχουν πρόσβαση και να τροποποιήσουν τα δεδομένα του εγγράφου XML χρησιμοποιώντας το API DOM. Για παράδειγμα, μπορούν να αλλάξουν κόμβους κειμένου, ιδιότητες και στοιχεία. Το πακέτο javax.xml.parsers περιέχει το συστατικό Java API γνωστό ως DOMParser. Χρησιμοποιείται συχνά σε εφαρμογές Java, όπως εφαρμογές ιστού, επιχειρηματικά συστήματα και προγράμματα γραφείου, που απαιτούν ανάγνωση, ανάλυση και τροποποίηση δεδομένων XML.Η απλότητα της χρήσης του DOMParser είναι ένα από τα βασικά πλεονεκτήματά του. Οι προγραμματιστές μπορούν να αναλύουν γρήγορα και να χειρίζονται έγγραφα XML χάρη στο απλό και φιλικό προς το χρήστη API που προσφέρει. Ωστόσο, η χρήση του DOMParser μπορεί να έχει διάφορα μειονεκτήματα, όπως η πιθανότητα χρήσης μνήμης, ιδίως κατά την ανάλυση μεγάλων σελίδων XML. Άλλες τεχνικές ανάλυσης, όπως η SAX (Simple API for XML), μπορεί να είναι πιο κατάλληλες σε τέτοιες περιπτώσεις.

- **FAME(Για τις μεθόδους κρυπτογράφησης και αποκρυπτογράφησης):** Το FAME είναι ένα από τα πιο γνωστά πλαίσια ABE. Το FAME είναι ένα ευέλικτο και αποτελεσματικό σύστημα ABE που επιτρέπει την ταυτόχρονη κρυπτογράφηση και αποκρυπτογράφηση δεδομένων ανάλογα με διάφορα χαρακτηριστικά, καθιστώντας το κατάλληλο για χρήση σε περίπλοκες ρυθμίσεις ελέγχου πρόσβασης. Κάθε χρήστης λαμβάνει ένα συγκεκριμένο σύνολο χαρακτηριστικών από το πλαίσιο FAME, το οποίο χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Για παράδειγμα, σε ένα περιβάλλον υγειονομικής περίθαλψης, η ηλικία, το φύλο και η ιατρική κατάσταση του ασθενούς μπορούν να χρησιμοποιηθούν ως χαρακτηριστικά για την κρυπτογράφηση των ιατρικών πληροφοριών του ασθενούς. Τα δεδομένα μπορούν στη συνέχεια να αποκρυπτογραφηθούν από εξουσιοδοτημένους χρήστες με τα σωστά

χαρακτηριστικά, ενώ οι μη εξουσιοδοτημένοι χρήστες με τα λάθος ή μερικά χαρακτηριστικά εμποδίζονται να το πράξουν. Η προσαρμοστικότητα του FAME είναι ένα από τα κύρια πλεονεκτήματά του. Ως αποτέλεσμα, μπορεί να διαχειριστεί καταστάσεις στις οποίες τα χαρακτηριστικά δεν είναι πάντα ακριβή. Επιτρέπει τόσο την ασαφή όσο και την ακριβή αντιστοίχιση των χαρακτηριστικών. Για παράδειγμα, στην κατάσταση υγειονομικής περίθαλψης που περιγράφηκε προηγουμένως, το χαρακτηριστικό της ιατρικής κατάστασης του ασθενούς μπορεί να είναι θολό ή ασαφές, αλλά το FAME μπορεί να καταστήσει τα δεδομένα προσβάσιμα σε εγκεκριμένους χρήστες που έχουν συγκρίσιμες ιατρικές καταστάσεις. Η αποτελεσματικότητα του FAME είναι ένα άλλο πλεονέκτημα. Για την ελαχιστοποίηση του κόστους επεξεργασίας και τον περιορισμό του όγκου των κρυπτογραφημένων δεδομένων, συνδυάζει συμμετρικούς και ασύμμετρους αλγορίθμους κρυπτογράφησης. Εξαιτίας αυτού, μπορεί να χρησιμοποιηθεί σε καταστάσεις με περιορισμένους πόρους, όπως αυτές που συναντώνται σε κινητές συσκευές και στο Διαδίκτυο των πραγμάτων (IoT). Παρατήρηση ότι η βιβλιοθήκη FAME της κρυπτογράφησης με βάσει χαρακτηριστικών (ABE) που χρησιμοποιήθηκε δεν έχει την δυνατότητα να κρυπτογραφήσει τα χαρακτηριστικά με την λογική λέξη κλειδί OR.

- **Policy-tool-service(Για την παραγωγή XACML πολιτική εξουσιοδότησης):** Το συγκεκριμένο εργαλείο κατασκευάστηκε από τον Γεώργιο Σούλτο φοιτητή του Πανεπιστήμιου Θεσσαλίας στο τμήμα Πληροφορικής και Τηλεπικοινωνίων. Στόχος αυτού του εργαλείου είναι χάρη στο φιλικό του περιβάλλον με τον χρήστη, να δίνει σε αυτόν μια πολύ πιο εύκολη κατασκευή πολιτικής ελέγχου πρόσβασης με βάση χαρακτηριστικών [21]. https://github.com/gsoultos/policy-tool-service.

- **Visual paradigm online(Για την σχεδίαση του συστήματος):** Η διαδικτυακή εφαρμογή μοντελοποίησης και σχεδιασμού που ονομάζεται Visual Paradigm Online επιτρέπει στους χρήστες να δημιουργούν μια ποικιλία διαγραμμάτων και μοντέλων για χρήση στην ανάπτυξη λογισμικού, την επιχειρηματική ανάλυση, την αρχιτεκτονική συστημάτων και άλλους τομείς. Πρόκειται για μια πλατφόρμα που βασίζεται στο cloud και μπορεί να χρησιμοποιηθεί για την ανάπτυξη, την επεξεργασία και τη συνεργασία σε διαγράμματα και μοντέλα με μέλη της ομάδας. Μπορεί να είναι προσβάσιμο από οποιοδήποτε τρέχον πρόγραμμα περιήγησης στο διαδίκτυο. Οι σημειώσεις UML, BPMN, ERD, DFD και άλλες σημειώσεις μοντελοποίησης και διαγραμμάτων υποστηρίζονται από το Visual Paradigm Online. Οι χρήστες μπορούν να κατασκευάσουν μια ποικιλία διαγραμμάτων, όπως διαγράμματα μηχανών κατάστασης, διαγράμματα περιπτώσεων χρήσης, διαγράμματα κλάσεων, διαγράμματα ακολουθίας και διαγράμματα δραστηριοτήτων. Η πλατφόρμα διαθέτει επίσης εργαλεία για έλεγχο εκδόσεων, ομαδική συνεργασία και διαχείριση έργων. Η προσβασιμότητα και η φιλικότητα προς το χρήστη του Visual Paradigm Online είναι δύο από τα κύρια πλεονεκτήματά του. Χωρίς να χρειάζεται να έχουν εκτεταμένες τεχνικές γνώσεις, οι χρήστες μπορούν απλώς να κατασκευάζουν και να αλλάζουν διαγράμματα και μοντέλα χρησιμοποιώντας το απλό και ξεκάθαρο περιβάλλον εργασίας χρήστη της πλατφόρμας. Επιπλέον, καθώς είναι βασισμένη στο cloud, οι χρήστες μπορούν να εργάζονται με τα μέλη της ομάδας σε πραγματικό χρόνο από οποιαδήποτε τοποθεσία. Συνολικά, το Visual Paradigm Online είναι μια δημοφιλής επιλογή για πολλές επιχειρήσεις, δεδομένου ότι αποτελεί ένα ισχυρό και προσαρμόσιμο εργαλείο μοντελοποίησης και σχεδιασμού που μπορεί να βοηθήσει τις ομάδες στον εξορθολογισμό των διαδικασιών τους και στην ενίσχυση της επικοινωνίας.

ΚΕΦΑΛΑΙΟ 6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Το συμπέρασμα είναι ότι το ABE/ABAC είναι μια ισχυρή μέθοδος ελέγχου πρόσβασης και κρυπτογράφησης που προσφέρει δυναμικό έλεγχο πρόσβασης, λεπτομερή έλεγχο πρόσβασης και αυξημένη ιδιωτικότητα. Η καταχώριση χαρακτηριστικών, η δημιουργία κλειδιών, η κρυπτογράφηση δεδομένων, ο έλεγχος πρόσβασης και η αποκρυπτογράφηση δεδομένων αποτελούν όλα τα στοιχεία της στρατηγικής υλοποίησης. Σε περιπτώσεις όπου απαιτείται λεπτομερής έλεγχος πρόσβασης, όπως σε εφαρμογές υγειονομικής περίθαλψης και χρηματοοικονομικές εφαρμογές, χρησιμοποιείται συχνά το ABE/ABAC. Σε σύγκριση με τις συμβατικές στρατηγικές ελέγχου πρόσβασης, η ABE/ABAC μπορεί να προσφέρει καλύτερη ασφάλεια και ιδιωτικότητα. Το ABE/ABAC θα συνεχίσει να είναι ζωτικής σημασίας για τη διασφάλιση της ασφάλειας των ευαίσθητων δεδομένων, καθώς όλο και περισσότερες επιχειρήσεις μεταφέρουν τα δεδομένα τους στο cloud και χρησιμοποιούν τεχνολογίες IoT. Επιπλέον έχει την δυνατότητα να βελτιωθεί παραπάνω με δυνατότητες και απαιτήσεις που αναφέρθηκαν στα προηγούμενα κεφάλαια αλλά και με την αναβάθμιση της βιβλιοθήκης FAME για την περίπτωση του λογικού κλειδιού OR.

Ακολουθούν ορισμένα παραδείγματα εφαρμογών και οργανισμών που έχουν χρησιμοποιήσει το ABE/ABAC:

- **Συστήματα Υγείας:** Ο τομέας της υγειονομικής περίθαλψης χρησιμοποιεί το ABE/ABAC για τη διασφάλιση της εμπιστευτικότητας των ευαίσθητων δεδομένων των ασθενών. Υπάρχουν πολλοί διαφορετικοί χρήστες που χρειάζονται πρόσβαση σε δεδομένα ασθενών στο πλαίσιο της υγειονομικής περίθαλψης, συμπεριλαμβανομένων των ιατρών, των νοσηλευτών και του προσωπικού υποστήριξης. Με βάση τη μοναδική λειτουργία και τα χαρακτηριστικά του υποκείμενου, το ABE/ABAC προσφέρει έναν μηχανισμό για τον περιορισμό της πρόσβασης σε δεδομένα ασθενών. Οι γιατροί, για παράδειγμα, θα μπορούσαν να έχουν πρόσβαση σε κάθε πληροφορία ασθενούς, ενώ οι διοικητικοί υπάλληλοι θα είχαν πρόσβαση μόνο στις πληροφορίες που αφορούν την ασφάλιση και την τιμολόγηση.

- **Χρηματοοικονομικά Συστήματα:** Για τη διαφύλαξη ευαίσθητων οικονομικών δεδομένων, συμπεριλαμβανομένων των οικονομικών αρχείων και συναλλαγών πελατών, ο χρηματοπιστωτικός τομέας χρησιμοποιεί το ABE/ABAC. Με βάση το μοναδικό ρόλο και τα χαρακτηριστικά του υποκείμενου, το ABE/ABAC μπορεί να χρησιμοποιηθεί για τον περιορισμό της πρόσβασης στα δεδομένα αυτά. Ένας διευθυντής θα μπορούσε να έχει πρόσβαση σε όλα τα δεδομένα πελατών, ενώ ένας ταμίας τράπεζας θα είχε πρόσβαση μόνο στις πληροφορίες για τους λογαριασμούς που είναι υπεύθυνος[5].

- **Κυβερνήσεις:** Σε κυβερνητικές εφαρμογές, το ABE/ABAC χρησιμοποιείται για τη διασφάλιση ευαίσθητων δεδομένων, όπως προσωπικές και διαβαθμισμένες πληροφορίες. Υπάρχουν πολλοί διαφορετικοί βαθμοί εξουσιοδότησης ασφαλείας σε ένα κυβερνητικό πλαίσιο και το ABE/ABAC προσφέρει έναν μηχανισμό για τον περιορισμό της πρόσβασης σε αυτά τα δεδομένα ανάλογα με το επίπεδο εξουσιοδότησης και άλλα χαρακτηριστικά του χρήστη.

- **Cloud Storage:** Οι εφαρμογές για αποθήκευση στο νέφος χρησιμοποιούν ABE/ABAC για να προσφέρουν ασφαλή πρόσβαση σε ευαίσθητα δεδομένα που φυλάσσονται εκεί. Οι ιδιοκτήτες δεδομένων μπορούν να ορίσουν λεπτομερείς

ελέγχους πρόσβασης με τη χρήση ABE/ABAC που λαμβάνουν υπόψη την τοποθεσία, το ρόλο και άλλα χαρακτηριστικά του χρήστη[11].

- **IoT Διαδίκτυο Των Πραγμάτων:** Οι εφαρμογές για το Διαδίκτυο των Πραγμάτων (IoT) χρησιμοποιούν το ABE/ABAC για να προσφέρουν ασφαλή πρόσβαση σε συνδεδεμένες συσκευές και δεδομένα. Χρησιμοποιώντας χαρακτηριστικά του υποκείμενου, όπως η τοποθεσία, ο ρόλος και άλλες εκτιμήσεις, το ABE/ABAC μπορεί να χρησιμοποιηθεί για τον περιορισμό της πρόσβασης σε συσκευές IoT[11].

Ακολουθούν μερικές περιπτώσεις επιχειρήσεων που έχουν χρησιμοποιήσει την ABE/ABAC:

- Microsoft: Για να προσφέρει ασφαλή πρόσβαση σε κλειδιά και μυστικά στο Cloud, η Microsoft δημιούργησε ένα σύστημα που ονομάζεται Azure Key Vault και χρησιμοποιεί το ABE/ABAC[12][15].

- IBM: Η IBM δημιούργησε ένα σύστημα που ονομάζεται Attribute-Based Access Control for the Cloud (ABAC4C), το οποίο χρησιμοποιεί ABE/ABAC[10].

- Ιδρύματα υγειονομικής περίθαλψης: Cleveland Clinic και το University of Utah Health, έχουν χρησιμοποιήσει το ABE/ABAC[11][16].

- Κυβερνητικοί οργανισμοί: Το Υπουργείο Εσωτερικής Ασφάλειας και το Υπουργείο Άμυνας της Αμερικής είναι δύο κυβερνητικοί οργανισμοί που έχουν υιοθετήσει το ABE/ABAC για τη διασφάλιση ευαίσθητων δεδομένων[16][15][6]

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Computer Security Division, I.T.L. (2016). *Role Based Access Control | CSRC | CSRC*. [online] CSRC | NIST. Available at: https://csrc.nist.gov/projects/role-based-access-control/faqs.

[2] De Capitani, S. and Sandhu, R. (2014). Access Control. *Computing Handbook, Third Edition*, pp.1–26. doi:https://doi.org/10.1201/b16812-54.

[3] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R. and Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3), pp.224–274. doi:https://doi.org/10.1145/501978.501980.

[4] Frontegg. (n.d.). *ABAC (Attribute-Based Access Control): A Complete Guide*. [online] Available at: https://frontegg.com/guides/abac.

[5] Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM conference on Computer and communications security - CCS '06*. doi:https://doi.org/10.1145/1180405.1180418.

[6] Hu, V., Ferraiolo, D., Kuhn, R., Friedman, A., Lang, A., Cogdell, M., Schnitzer, A., Sandlin, K., Miller, R. and Scarfone, K. (2013). *NIST Special Publication 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)*. [online] Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cab698a5b0949aa7acd0858b55352c5df0a2c2fb&fbclid=IwAR1liwYYHOj1wHJSo0AuibZ_51LYQVq9rAu7eFM-0lTzOX9_Wf89pXKZSkQ [Accessed 16 Feb. 2023].

[7] Huang, D., Dong, Q. and Zhu, Y. (2020). *Attribute-Based Encryption and Access Control*. CRC Press.

[8] Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P. and Jonker, W. (2009). Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application. *Information Security Applications*, pp.309–323. doi:https://doi.org/10.1007/978-3-642-10838-9_23.

[9] Matt (2022). *Building Access Control for OpenMetadata*. [online] Medium. Available at: https://blog.open-metadata.org/building-access-control-for-openmetadata-5b842a2abd90 [Accessed 16 Feb. 2023].

[10] Kuo, F., Li, P., & Huang, S. (2016). A Secure and Fine-Grained Access Control Scheme for Cloud Computing. IEEE Transactions on Services Computing, 9(3), 467-479. doi:10.1109/TSC.2015.2393613.

[11] McBurney, P. and Wilson, D. (2016). Attribute-based access control for the Internet of Things. *Journal of Information Security and Applications*.

[12] Ruj, S., Stojmenovic, M. and Nayak, A. (2014). Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds. *IEEE Transactions on Parallel and Distributed Systems*, 25(2), pp.384–394. doi:https://doi.org/10.1109/tpds.2013.38.

[13] Wimalasiri, P. (2021). *A beginner's guide to XACML*. [online] Identity Beyond Borders. Available at: https://medium.com/identity-beyond-borders/a-beginners-guide-to-acme-6dc75b547d55 [Accessed 16 Feb. 2023].

[14] Bethencourt, J., Sahai, A. and Waters, B. (2007). *Ciphertext-Policy Attribute-Based Encryption*. [online] IEEE Xplore. doi:https://doi.org/10.1109/SP.2007.11.

[15] Chinnasamy, P., Deepalakshmi, P., Dutta, A.K., You, J. and Joshi, G.P. (2021). Ciphertext-Policy Attribute-Based Encryption for Cloud Storage: Toward Data Privacy and Authentication in AI-Enabled IoT System. *Mathematics*, 10(1), p.68. doi:https://doi.org/10.3390/math10010068.

[16] Gama, N. and Nguyen, P.Q. (2007). New Chosen-Ciphertext Attacks on NTRU. *Public Key Cryptography – PKC 2007*, pp.89–106. doi:https://doi.org/10.1007/978-3-540-71677-8_7.

[17] Kahn, D. (1976). *The Codebreakers*.

[18] Moffat, S., Hammoudeh, M. and Hegarty, R. (2017). A Survey on Ciphertext-Policy Attribute-based Encryption (CP-ABE) Approaches to Data Security on Mobile Devices and its Application to IoT. *Proceedings of the International Conference on Future Networks and Distributed Systems*. doi:https://doi.org/10.1145/3102304.3102338.

[19] Sahai, A. and Waters, B. (2005). Fuzzy Identity-Based Encryption. *Lecture Notes in Computer Science*, pp.457–473. doi:https://doi.org/10.1007/11426639_27.

[20] Singh, S. (2009). *The code book : the science of secrecy from ancient Egypt to quantum cryptography*. Bridgewater, Nj: Distributed By Paw Prints / Baker & Taylor.

[21] Γεώργιος Σούλτος, Ανάπτυξη συστήματος διαχείρισης πολιτικών ελέγχου πρόσβασης βάσει χαρακτηριστικών, Πτυχιακή Εργασία, Πανεπιστήμιο Θεσσαλίας, 2022.

[22] Langaliya, C. and Aluvalu, R. (2015). Enhancing Cloud Security through Access Control Models: A Survey. International Journal of Computer Applications. Doi: 10.5120/19677-1400

[23] Sebastian Zickau, Dirk Thatmann, Artjom Butyrtschik , Iwailo Denisow , and Axel Kupper. (2016). Applied Attribute-based Encryption Schemes. 19th International ICIN Conference - Innovations in Clouds, Internet and Networks. https://dl.ifip.org/db/conf/icin/icin2016/1570228068.pdf

[24] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

[25] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice.

[26] NIST. (2021). Digital Signature Standard (DSS). https://csrc.nist.gov/projects/digital-signatures/digital-signature-standard

[27] Kahn, D. (1996). The codebreakers: the comprehensive history of secret communication from ancient times to the Internet. Scribner.

[28] Koblitz, N. (1994). A course in number theory and cryptography. Springer-Verlag.