ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΕΠΙΒΟΛΗ ΚΑΝΟΝΩΝ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ ΜΕ ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΑΣ ΔΙΑΧΕΙΡΙΣΗΣ ΨΗΦΙΑΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

ΔΟΥΝΑΒΗΣ ΒΑΣΙΛΕΙΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Εντεταλμένος διδάσκων

Λαμία, Ιούλιος 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΕΠΙΒΟΛΗ ΚΑΝΟΝΩΝ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ ΜΕ ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΑΣ ΔΙΑΧΕΙΡΙΣΗΣ ΨΗΦΙΑΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

ΔΟΥΝΑΒΗΣ ΒΑΣΙΛΕΙΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Λιουδάκης
Εντεταλμένος διδάσκων

Λαμία, Ιούλιος 2023

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

ENFORCING ACCESS CONTROL RULES USING DIGITAL RIGHTS MANAGEMENT TECHNOLOGY

DOUNAVIS VASILEIOS

FINAL THESIS

ADVISOR

Georgios Lioudakis
Adjunct Professor

Lamia, July 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: 13/7/2023

Ο – Η Δηλ.
Βασίλειος Δούναβης

(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

Ο έλεγχος πρόσβασης είναι πρωταρχικής σημασίας για τη διασφάλιση της ασφάλειας και του απορρήτου των ψηφιακών πόρων, ιδιαίτερα στο πλαίσιο της προστασίας των πνευματικών δικαιωμάτων. Αυτή η πτυχιακή εργασία στοχεύει να αντιμετωπίσει την πρόκληση της διατήρησης του ελέγχου της πρόσβασης στο περιεχόμενο λήψης για την αποτροπή μη εξουσιοδοτημένης διανομής και χρήσης. Ερευνώντας τις δυνατότητες της τεχνολογίας Digital Rights Management (DRM), αυτή η έρευνα επιδιώκει να επαναπροσδιορίσει και να επιβάλει κανόνες ελέγχου πρόσβασης ακόμη και μετά τη λήψη του περιεχομένου. Η DRM εξουσιοδοτεί τους κατόχους και τους παρόχους περιεχομένου να ασκούν έλεγχο και να επιβάλλουν περιορισμούς χρήσης, προστατεύοντας από μη εξουσιοδοτημένη κοινή χρήση και παραβίαση.

ABSTRACT

Access Control is of the utmost importance if the resources' security and privacy are in question, especially in the context of copyright trademarks. This thesis aims at delving into the challenge of preserving control over access to downloaded content to prohibit unauthorized distribution and usage. Exploring the potential of Digital Rights Management (DRM) technology, this research hopes to redefine and enforce access control rules even after downloading the content. The DRM technology enables content creators and providers to exercise and impose usage restrictions, protecting them from unauthorized sharing and infringement.

Table of Contents

Εισαγωγή

Ο έλεγχος πρόσβασης διαδραματίζει κρίσιμο ρόλο στη διασφάλιση της ασφάλειας και του απορρήτου των ψηφιακών πόρων. Στο σημερινό ταχέως διευρυνόμενο τοπίο ψηφιακού περιεχομένου, η προστασία της πνευματικής ιδιοκτησίας γίνεται όλο και πιο σημαντική. Είναι επιτακτική η επιβολή κανόνων ελέγχου πρόσβασης για τον μετριασμό των κινδύνων και τη διασφάλιση της εξουσιοδοτημένης χρήσης. Ωστόσο, μια σημαντική πρόκληση προκύπτει όταν το περιεχόμενο χάνει τους κανόνες πρόσβασής του μετά τη λήψη του από έναν χρήστη, με αποτέλεσμα τη πιθανή μη εξουσιοδοτημένη διανομή και χρήση.

Για την αντιμετώπιση αυτού του πιεστικού ζητήματος, αυτή η πτυχιακή στοχεύει να εμβαθύνει στις δυνατότητες της τεχνολογίας διαχείρισης ψηφιακών δικαιωμάτων (DRM) ως μια ισχυρή λύση. Με την αποτελεσματική εφαρμογή ενος DRM, μπορούμε να επαναπροσδιορίσουμε και να διατηρήσουμε κανόνες ελέγχου πρόσβασης ακόμα και μετά τη λήψη του πόρου από έναν χρήστη. Αυτό δίνει τη δυνατότητα στους κατόχους και τους παρόχους περιεχομένου να ασκούν έλεγχο και να επιβάλλουν περιορισμούς στη χρήση περιεχομένου, αποτρέποντας τη μη εξουσιοδοτημένη κοινή χρήση και παραβίαση.

Στο Κεφάλαιο 2, γίνεται μια ολοκληρωμένη εισαγωγή στην XACML και την ODRL, εξοικειώνοντας τους αναγνώστες με τις έννοιες, τις οντότητες και άλλες σχετικές πληροφορίες. Εξερευνούμε το μοντέλο ελέγχου πρόσβασης βάσει χαρακτηριστικών (ABAC) που ακολουθείται από την XACML.

Στο Κεφάλαιο 2.3 εμβαθύνει στον κρίσιμο ρόλο της τεχνολογίας Διαχείρισης Ψηφιακών Δικαιωμάτων (DRM) στην προστασία του ψηφιακού περιεχομένου και στη διατήρηση των δικαιωμάτων των δημιουργών, των εκδοτών και των διανομέων περιεχομένου. Εξετάζουμε πώς το DRM παρέχει ένα ισχυρό πλαίσιο για τη διαχείριση και την επιβολή του ελέγχου πρόσβασης, των περιορισμών χρήσης και των πολιτικών πνευματικών δικαιωμάτων. Με τη χρήση του DRM, οι οργανισμοί μπορούν να διατηρήσουν τον έλεγχο των ψηφιακών τους στοιχείων, να αποτρέψουν τη μη εξουσιοδοτημένη αντιγραφή και διανομή και να διασφαλίσουν τη συμμόρφωση με τις συμφωνίες αδειοδότησης και τους κανονισμούς περί πνευματικών δικαιωμάτων.

Στο Κεφάλαιο 2.4 εστιάζει στην Ανοιχτή Γλώσσα Ψηφιακών Δικαιωμάτων (ODRL) και τη συνάφειά της στον τομέα της διαχείρισης ψηφιακών δικαιωμάτων. Εξερευνούμε τις οντότητες και τα αντικείμενα που ορίζονται από την ODRL, τα οποία αποτελούν τη βάση για τον καθορισμό πολιτικών ελέγχου πρόσβασης και τη διαχείριση ψηφιακού περιεχομένου. Επιπλέον, εξετάζουμε τα διάφορα αντικείμενα

που παρέχονται από την ODRL, επιτρέποντας τη δομημένη έκφραση των πολιτικών ελέγχου πρόσβασης και ενεργοποίησης.

Το Κεφάλαιο 3 εμβαθύνει στο σχεδιασμό ενός συστήματος για τη μετατροπή πολιτικών XACML σε πολιτικές ODRL. Παρουσιάζουμε έναν αλγόριθμο ειδικά προσαρμοσμένο για να διευκολύνει αυτήν την διαδικασία μετατροπής. Ο αλγόριθμος εξάγει χαρακτηριστικά και κανόνες πολιτικής από την XACML, τα αντιστοιχίζει στα αντίστοιχα στοιχεία ODRL και δημιουργεί ένα αρχείο εξόδου που περιέχει την πολιτική ODRL που έχει μετατραπεί.

Διερευνώντας την επιβολή κανόνων ελέγχου πρόσβασης μέσω της τεχνολογίας DRM και τη μετατροπή από XACML σε ODRL, αυτή η πτυχιακή εργασία στοχεύει να συμβάλει στον τομέα της ασφάλειας πληροφοριών και της διαχείρισης ψηφιακών δικαιωμάτων. Τα επόμενα κεφάλαια εμβαθύνουν στις λεπτομέρειες της XACML και της ODRL, την προστασία του ψηφιακού περιεχομένου και τον αλγόριθμο μετατροπής, παρέχοντας πληροφορίες, αναλύσεις και μία πρακτική επιδείξη του συστήματος μετατροπής.

Τεχνολογίες ελέγχου πρόσβασης

Έλεγχος πρόσβασης

Ο έλεγχος πρόσβασης είναι μια κρίσιμη πτυχή των συστημάτων ασφαλείας που διέπει τα δικαιώματα και τους περιορισμούς στις αλληλεπιδράσεις των χρηστών με πόρους ή ευαίσθητες πληροφορίες. Λειτουργεί ως προστατευτικό φράγμα, διασφαλίζοντας ότι μόνο εξουσιοδοτημένα άτομα ή οντότητες μπορούν να έχουν πρόσβαση σε συγκεκριμένα περιουσιακά στοιχεία ή να εκτελούν ορισμένες ενέργειες εντός ενός συστήματος. Οι μηχανισμοί ελέγχου πρόσβασης έχουν σχεδιαστεί για τον μετριασμό των κινδύνων ασφαλείας, την πρόληψη της μη εξουσιοδοτημένης αποκάλυψης, τη διατήρηση της ακεραιότητας των δεδομένων και την επιβολή της συμμόρφωσης με κανονισμούς και πολιτικές.

ABAC

Ο έλεγχος πρόσβασης βάσει χαρακτηριστικών (ABAC) είναι μια προηγμένη προσέγγιση για τον έλεγχο πρόσβασης που βασίζεται σε παραδοσιακά μοντέλα. Το ABAC εξετάζει διάφορα χαρακτηριστικά που σχετίζονται με τους χρήστες, τους πόρους και τους περιβαλλοντικούς παράγοντες για τη λήψη αποφάσεων πρόσβασης. Αυτά τα χαρακτηριστικά μπορεί να περιλαμβάνουν ρόλους χρήστη, συμμετοχές σε ομάδες, επίπεδα άδειας, χρόνο πρόσβασης, τοποθεσία ή οποιοδήποτε άλλο σχετικό χαρακτηριστικό. Οι πολιτικές ABAC ορίζουν κανόνες και συνθήκες με βάση αυτά τα χαρακτηριστικά, επιτρέποντας λεπτομερή έλεγχο πρόσβασης.

Στο ABAC, οι αποφάσεις πρόσβασης λαμβάνονται δυναμικά με την αξιολόγηση των χαρακτηριστικών της αιτούσας οντότητας και του πόρου στον οποίο έχει πρόσβαση. Αυτή η δυναμική αξιολόγηση επιτρέπει πιο ευέλικτο και ενήμερο έλεγχο πρόσβασης. Οι πολιτικές ABAC μπορούν να οριστούν χρησιμοποιώντας μια γλώσσα πολιτικής όπως η XACML, η οποία παρέχει ένα τυποποιημένο πλαίσιο για τον καθορισμό πολιτικών ελέγχου πρόσβασης.

Κατανόηση της XACML

Η eXtensible Access Control Markup Language (XACML) είναι ένα ευρέως διαδεδομένο πρότυπο που αναπτύχθηκε από τον οργανισμό OASIS[1], βασισμένο σε XML, το οποίο χρησιμεύει ως γλώσσα περιγραφής για τις προδιαγραφές ελέγχου

[1] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

πρόσβασης. Προσφέρει ισχυρούς μηχανισμούς πολιτικής ασφαλείας και χρησιμοποιείται από πολλούς οργανισμούς και εταιρείες.

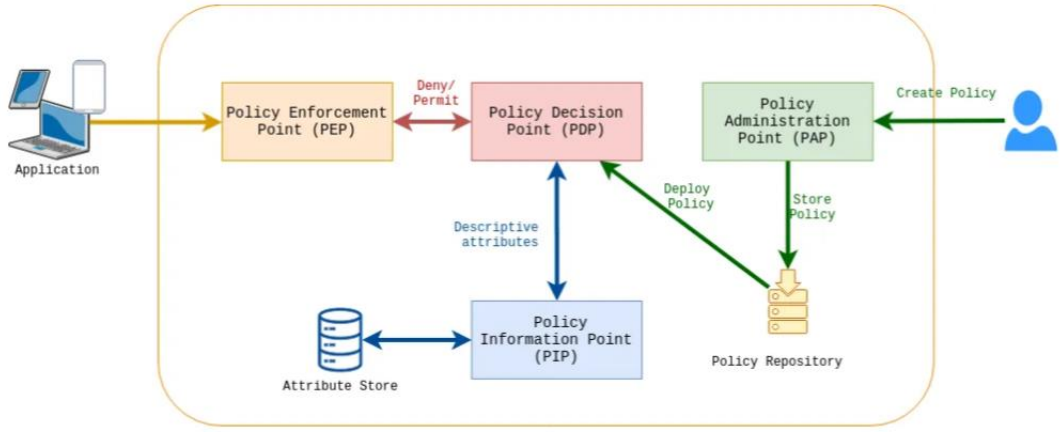
Στην αρχιτεκτονική XACML, το Σημείο Επιβολής Πολιτικής (Policy Enforcement Point, PEP) παρεμποδίζει και επιβάλλει πολιτικές ελέγχου πρόσβασης στο σύστημα. Λειτουργεί ως θυρωρός, λαμβάνοντας αιτήματα πρόσβασης από χρήστες ή οντότητες και τα προωθεί στο Σημείο Απόφασης Πολιτικής (Policy Decision Point, PDP) για αξιολόγηση. Το PEP λαμβάνει επίσης την απόφαση από το PDP και την επιβάλλει επιτρέποντας ή απορρίπτοντας την πρόσβαση στον ζητούμενο πόρο.

Το σημείο αυτό είναι υπεύθυνο για την αξιολόγηση των πολιτικών που βασίζονται σε αιτήματα πρόσβασης που λαμβάνονται από το PEP. Χρησιμοποιεί τις πληροφορίες που παρέχονται στα αιτήματα, μαζί με τις πολιτικές και τους κανόνες που ορίζονται στην XACML, για τη λήψη αποφάσεων ελέγχου πρόσβασης. Εάν το PDP απαιτεί πρόσθετες πληροφορίες χαρακτηριστικών για να λάβει μια απόφαση, μπορεί να ζητήσει αυτά τα χαρακτηριστικά από το σημείο πληροφοριών πολιτικής (Policy Information Point, PIP).

Στην αρχιτεκτονική XACML, το PIP είναι ένα στοιχείο που συλλέγει και ανακτά πληροφορίες χαρακτηριστικών από διάφορες πηγές, όπως βάσεις δεδομένων ή καταλόγους χρηστών. Λειτουργεί ως διεπαφή μεταξύ του PDP και των εξωτερικών συστημάτων που διατηρούν τις πληροφορίες χαρακτηριστικών. Το PIP παρέχει τις απαραίτητες τιμές χαρακτηριστικών στο PDP κατά τη διαδικασία αξιολόγησης πολιτικής.

Συνολικά, η συνεργατική διαδικασία στην αρχιτεκτονική XACML περιλαμβάνει το PEP να παρακολουθεί αιτήματα πρόσβασης και να επιβάλλει αποφάσεις, το PDP να αξιολογεί τις πολιτικές και να λαμβάνει αποφάσεις ελέγχου πρόσβασης με βάση τις πληροφορίες που παρέχονται από το PIP και τα αιτήματα που λαμβάνονται από το PEP. Αυτό εξασφαλίζει αποτελεσματική διαχείριση ελέγχου πρόσβασης σε

συστήματα που χρησιμοποιούν XACML.



Σχήμα 1 Αρχιτεκτονική XACML(πηγή: https://medium.com/identity-beyond-borders/a-beginners-guide-to-xacml-6dc75b547d55)

Κάθε στοιχείο της γλώσσας αποτελείται από τρία βασικά στοιχεία:

- <Rule>: Περιέχει μια λογική έκφραση που αξιολογείται ανεξάρτητα χωρίς να καθορίζεται η τελική απόφαση. Καθορίζει μια προϋπόθεση για τη λήψη αποφάσεων ελέγχου πρόσβασης.
- <PolicySet>: Περιέχει ένα σύνολο στοιχείων <Policy> και έναν αλγόριθμο για το συνδυασμό των αποτελεσμάτων αξιολόγησης. Παίζει ζωτικό ρόλο στην αξιολόγηση των πολιτικών και στη λήψη της τελικής απόφασης. Επιτρέπει την ομαδοποίηση και την οργάνωση πολιτικών και συνόλων πολιτικών σε μια ιεραρχική δομή.
- <Policy>: Καθορίζει πολιτικές ελέγχου πρόσβασης που αξιολογούνται και συνδυάζονται από το PDP.

Κάθε στοιχείο XACML περιλαμβάνει ένα στοιχείο <Target>, προσδιορίζοντας τις συνθήκες υπό τις οποίες ισχύει το συσχετισμένο <Rule>, <Policy> ή <PolicySet>:

- <AnyOf>: Καθορίζει ότι όλα τα στοιχεία <AllOf> που εσωκλείονται πρέπει να ικανοποιούνται.
- <AllOf>: Καθορίζει ότι όλα τα στοιχεία <Match> που εσωκλείονται πρέπει να ικανοποιούνται.
- <Match>: Καθορίζει μια συνθήκη που θα αντιστοιχιστεί με τα χαρακτηριστικά στο αίτημα πρόσβασης.

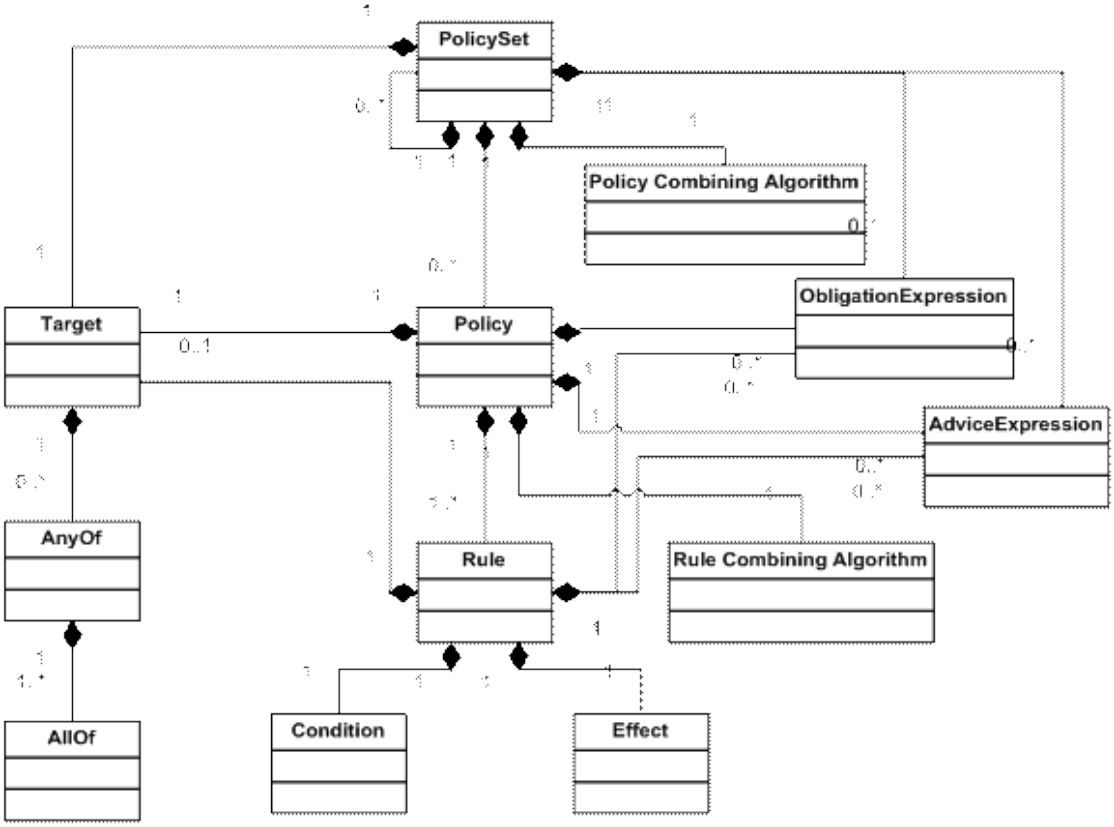
Η XACML υποστηρίζει αλγόριθμους συνδυασμού κανόνων:

- Οι συνηθισμένοι αλγόριθμοι περιλαμβάνουν Deny-overrides, Permit-overrides, and First-applicable.

- Αυτοί οι αλγόριθμοι καθορίζουν την τελική απόφαση με βάση μεμονωμένα αποτελέσματα από την αξιολόγηση των σχετικών κανόνων ή πολιτικών.

Η XACML ακολουθεί το μοντέλο ελέγχου πρόσβασης βάσει χαρακτηριστικών (ABAC) με βασικές κλάσεις ABAC:

- Θέμα(Subject): Αντιπροσωπεύει την οντότητα (π.χ. χρήστη) που ζητά πρόσβαση σε έναν πόρο.
- Πόρος(Resource): Αντιπροσωπεύει την οντότητα-στόχο(target) (π.χ. αρχείο, βάση δεδομένων) στην οποία έχετε πρόσβαση.
- Ενέργεια(Action): Αντιπροσωπεύει τη λειτουργία (π.χ. ανάγνωση, εγγραφή) που εκτελείται στον πόρο.
- Περιβάλλον(Environment): Αντιπροσωπεύει πληροφορίες συμφραζομένων (π.χ. ώρα, τοποθεσία) που σχετίζονται με το αίτημα πρόσβασης.



Σχήμα 2: Το μοντέλο της XACML (Πηγή: https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en_files/image004.gif)

Είναι σημαντικό να σημειωθεί ότι ξεκινώντας από την έκδοση XACML 3.0, η γλώσσα υποστηρίζει επίσης προσαρμοσμένες κατηγορίες ABAC, παρέχοντας περαιτέρω ευελιξία στον καθορισμό πολιτικών ελέγχου πρόσβασης.

Διαχείριση Ψηφιακών Δικαιωμάτων

Η Διαχείριση Ψηφιακών Δικαιωμάτων (Digital Rights Management, DRM) είναι μια κρίσιμη τεχνολογία που διαδραματίζει σημαντικό ρόλο στην προστασία του ψηφιακού περιεχομένου και στην προστασία των δικαιωμάτων των δημιουργών, των εκδοτών και των διανομέων περιεχομένου. Καθώς το ψηφιακό τοπίο συνεχίζει να εξελίσσεται και η κατανάλωση περιεχομένου γίνεται όλο και πιο ψηφιακή, το DRM παρέχει ένα πλαίσιο για τη διαχείριση και την επιβολή πολιτικών ελέγχου πρόσβασης, περιορισμών χρήσης και δικαιωμάτων πνευματικής ιδιοκτησίας. Χρησιμοποιώντας DRM, οι οργανισμοί μπορούν να διατηρήσουν τον έλεγχο των ψηφιακών τους στοιχείων, να αποτρέψουν τη μη εξουσιοδοτημένη αντιγραφή και διανομή και να διασφαλίσουν τη συμμόρφωση με τις συμφωνίες αδειοδότησης και τους κανονισμούς περί πνευματικών δικαιωμάτων. Αυτή η εισαγωγή θέτει το έδαφος για την κατανόηση της σημασίας του DRM στο πλαίσιο της διαχείρισης ψηφιακών δικαιωμάτων και ανοίγει το δρόμο για τη διερεύνηση του ρόλου πλαισίων όπως η ODRL στην αποτελεσματική εφαρμογή πολιτικών ελέγχου πρόσβασης και στη διαχείριση ψηφιακού περιεχομένου.

ODRL στη διαχείριση ψηφιακού δικαιωμάτων

Η Open Digital Rights Language (ODRL) παρέχει ένα πλούσιο πλαίσιο για την έκφραση και τη διαχείριση ψηφιακών δικαιωμάτων. Στον πυρήνα του, η ODRL ορίζει διάφορες οντότητες και αντικείμενα που επιτρέπουν την εξειδίκευση των πολιτικών ελέγχου πρόσβασης και τη διαχείριση ψηφιακού περιεχομένου. Αυτές οι οντότητες και τα αντικείμενα αποτελούν τα δομικά στοιχεία της ODRL και διαδραματίζουν κρίσιμο ρόλο στην περιγραφή των δικαιωμάτων, των υποχρεώσεων και των συνθηκών που σχετίζονται με τη χρήση και τη διανομή των ψηφιακών στοιχείων.

Οι οντότητες στην ODRL αντιπροσωπεύουν τα διάφορα ενδιαφερόμενα μέρη που εμπλέκονται στη διαδικασία διαχείρισης δικαιωμάτων. Οι βασικές οντότητες στην ODRL περιλαμβάνουν:

Asset: Ένα asset αντιπροσωπεύει το ψηφιακό περιεχόμενο ή τον πόρο στον οποίο εφαρμόζονται οι πολιτικές ελέγχου πρόσβασης. Μπορεί να αναφέρεται σε διάφορους τύπους ψηφιακών στοιχείων, όπως εικόνες, βίντεο, αρχεία ήχου, έγγραφα ή ακόμα και υπηρεσίες. Κάθε Στοιχείο προσδιορίζεται μοναδικά στο πλαίσιο μιας πολιτικής ODRL και χρησιμεύει ως αντικείμενο δικαιωμάτων και αδειών.

Party: Ένα party αντιπροσωπεύει ένα άτομο ή έναν οργανισμό που εμπλέκεται στη διαδικασία διαχείρισης δικαιωμάτων. Θα μπορούσε να είναι ένα άτομο, ένας όμιλος, μια εταιρεία ή οποιαδήποτε άλλη οντότητα που παίζει ρόλο στη χορήγηση ή

την άσκηση δικαιωμάτων. Τα μέρη μπορεί να είναι δημιουργοί, ιδιοκτήτες, διανομείς ή καταναλωτές ψηφιακών στοιχείων. Η ODRL παρέχει την ευελιξία για τον καθορισμό διαφόρων χαρακτηριστικών και ιδιοτήτων ενός party, όπως το όνομα, το αναγνωριστικό, ο ρόλος και η δικαιοδοσία του.

Agreement: Ένα agreement αντιπροσωπεύει μια νομική ή συμβατική σχέση μεταξύ των parties σχετικά με τη χρήση και τη διανομή ψηφιακών στοιχείων. Περιγράφει τους όρους και τις προϋποθέσεις που διέπουν τα δικαιώματα και τις υποχρεώσεις που σχετίζονται με τα περιουσιακά στοιχεία. Οι συμφωνίες μπορούν να ορίζουν κανόνες για τη χορήγηση αδειών, την επιβολή περιορισμών και τον καθορισμό υποχρεώσεων για τα εμπλεκόμενα μέρη. Η ODRL επιτρέπει την έκφραση διαφορετικών τύπων συμφωνιών, όπως άδειες, συμβάσεις ή άλλες μορφές νομικών ρυθμίσεων.

PartyCollection: Ένα PartyCollection αντιπροσωπεύει μια ομάδα ή μια συλλογή από μέρη στην ODRL. Επιτρέπει την ομαδοποίηση πολλών Μερών σε ένα κοινό αναγνωριστικό ή κατηγορία. Τα PartyCollections μπορούν να χρησιμοποιηθούν για την απλοποίηση της έκφρασης δικαιωμάτων και αδειών για πολλά μέρη ταυτόχρονα. Για παράδειγμα, ένα PartyCollection μπορεί να αντιπροσωπεύει τους υπαλλήλους μιας εταιρείας ή μια ομάδα χρηστών με παρόμοια δικαιώματα πρόσβασης.

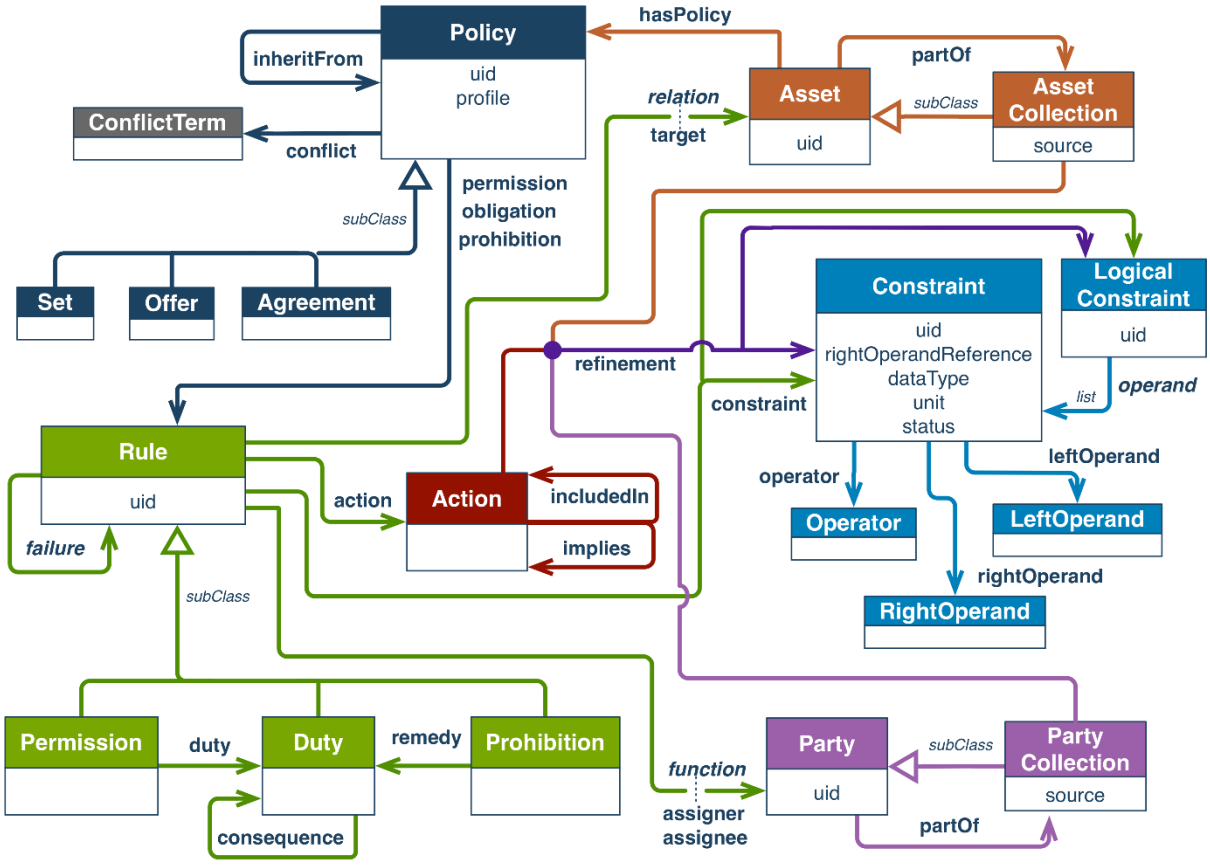
Εκτός από τις οντότητες, η ODRL εισάγει πολλά αντικείμενα που καθορίζουν τα δικαιώματα, τις υποχρεώσεις και τις προϋποθέσεις που σχετίζονται με τα ψηφιακά στοιχεία. Αυτά τα αντικείμενα παρέχουν έναν δομημένο τρόπο έκφρασης πολιτικών ελέγχου πρόσβασης και ενεργοποιούν την προδιαγραφή λεπτομερών αδειών. Τα βασικά αντικείμενα στην ODRL περιλαμβάνουν:

Permission: Ένα permission αντικείμενο αντιπροσωπεύει τα δικαιώματα που παραχωρούνται στα parties για πρόσβαση και χρήση ψηφιακών στοιχείων. Καθορίζει τι επιτρέπεται να κάνει ένα μέρος με ένα asset, όπως προβολή, αντιγραφή, τροποποίηση, εκτύπωση ή κοινή χρήση. Τα δικαιώματα μπορούν να εκφραστούν σε διάφορα επίπεδα ευαισθησίας, επιτρέποντας τον καθορισμό συγκεκριμένων δικαιωμάτων για διαφορετικά περιβάλλοντα ή ενέργειες.

Prohibition: Ένα Prohibition entity αντιπροσωπεύει τους περιορισμούς ή τις απαγορεύσεις που επιβάλλονται στα parties σχετικά με τη χρήση ψηφιακών στοιχείων. Καθορίζει τι δεν επιτρέπεται να κάνει ένα μέρος με ένα περιουσιακό στοιχείο. Οι απαγορεύσεις μπορούν να περιορίσουν ενέργειες όπως η αντιγραφή, η διανομή ή η τροποποίηση ενός Περιουσιακού στοιχείου. Παρόμοια με τα δικαιώματα, οι απαγορεύσεις μπορούν να καθοριστούν σε διαφορετικά επίπεδα ευαισθησίας.

Duty: Ένα αντικείμενο duty αντιπροσωπεύει μια υποχρέωση ή απαίτηση που πρέπει να εκπληρώσουν τα μέρη κατά την πρόσβαση ή τη χρήση ψηφιακών στοιχείων. Ορίζει ενέργειες που ένα party υποχρεούται να εκτελέσει, όπως η παροχή απόδοσης, η αναφορά χρήσης ή η πληρωμή δικαιωμάτων εκμετάλλευσης. Οι υποχρεώσεις συνήθως συνδέονται με Permissions ή Prohibitions και χρησιμεύουν ως προϋποθέσεις για την άσκηση των δικαιωμάτων.

Constraint: Ένα αντικείμενο Constraint αντιπροσωπεύει πρόσθετες προϋποθέσεις ή απαιτήσεις που πρέπει να πληρούνται για την άσκηση δικαιωμάτων ή την εκπλήρωση υποχρεώσεων. Οι περιορισμοί μπορούν να χρησιμοποιηθούν για τον καθορισμό προϋποθέσεων όπως χρονικά όρια, γεωγραφικοί περιορισμοί, συμβατότητα συσκευών ή οποιαδήποτε άλλα κριτήρια πρέπει να πληρούνται για την πρόσβαση ή τη χρήση ψηφιακών στοιχείων. Παρέχουν έναν ευέλικτο τρόπο έκφρασης συγκεκριμένων συνθηκών για την εφαρμογή των δικαιωμάτων.



Σχήμα 3: Το μοντέλο της ODRL (Πηγή: https://www.w3.org/TR/odrl-model/00Model.png)

Συνδυάζοντας αυτές τις οντότητες και τα αντικείμενα, η ODRL επιτρέπει τη δημιουργία ολοκληρωμένων πολιτικών ελέγχου πρόσβασης που καθορίζουν τα δικαιώματα, τις υποχρεώσεις και τις προϋποθέσεις που σχετίζονται με τα ψηφιακά στοιχεία. Η ευελιξία και η επεκτασιμότητα της ODRL τη καθιστούν κατάλληλη για

διάφορους τομείς, συμπεριλαμβανομένων των μέσων ενημέρωσης, των εκδόσεων, του ηλεκτρονικού εμπορίου και άλλων, όπου η ακριβής και τυποποιημένη διαχείριση δικαιωμάτων είναι ζωτικής σημασίας. Η χρήση οντοτήτων και αντικειμένων στην ODRL παρέχει μια δομημένη και εκφραστική προσέγγιση στα ψηφιακά δικαιώματα διαχείριση, παρέχοντας τη δυνατότητα στους δημιουργούς περιεχομένου, τους διανομείς και τους καταναλωτές να συνεργάζονται, να προστατεύουν τα συμφέροντά τους και να διασφαλίζουν την κατάλληλη χρήση και διανομή των ψηφιακών στοιχείων.

Σχεδιασμός συστήματος για μετατροπή πολιτικών XACML σε ODRL

Αλγόριθμος Μετατροπής

Σε αυτήν την ανάλυση, παρουσιάζουμε έναν αλγόριθμο που έχει σχεδιαστεί για να διευκολύνει τη μετατροπή των πολιτικών XACML σε πολιτικές ODRL. Ο αλγόριθμος περιλαμβάνει μια σειρά βημάτων που στοχεύουν στην εξαγωγή χαρακτηριστικών και κανόνων πολιτικής από την XACML, την αντιστοίχιση τους με τα αντίστοιχα ODRL στοιχεία και τη δημιουργία ενός αρχείου εξόδου που περιέχει τη πολιτικη ODRL που έχει μετατραπεί.Ο αλγόριθμος έχει τα εξής βήματα:

1. Λαμβάνει σαν είσοδο ένα αρχείο που περιέχει την XACML
2. Αναλύει το αρχείο που δόθηκε και εξάγει τα χαρακτηριστικά και τους κανόνες πολιτικής.
3. Μετατρέπει τα εξαγμένα XACML χαρακτηριστικά στα αντίστοιχα ODRL χαρακτηριστικά. Αυτή η μετατροπή απαιτεί την αντιστοίχηση των πολιτικών και των χαρακτηριστικών.
4. Γράφει στο αρχείο εξόδου, την ODRL με τα μετατρεπόμενα χαρακτηριστικά και τις μετατρεπόμενες πολιτικές
5. Δίνει ως έξοδο το αρχείο που περιέχει την ODRL

XACML Attributes	ODRL Properties
Subject	Assignee
Resource	Asset/Target
Action	Action
Obligation	Duty/Obligation
Rules	Constraints

Πίνακας Μετατροπών

Η λογική πίσω από τη μετατροπή από χαρακτηριστικά XACML σε ιδιότητες ODRL βασίζεται στις ομοιότητες στους ρόλους και τις λειτουργίες τους στα αντίστοιχα συστήματα:

1. Subject (XACML) σε Assignee (ODRL):

   Στην XACML, το θέμα αντιπροσωπεύει την οντότητα ή τις οντότητες (χρήστες, ομάδες, ρόλους) που ζητούν πρόσβαση σε έναν πόρο. Η ιδιότητα Assignee στην ODRL εξυπηρετεί παρόμοιο σκοπό, προσδιορίζοντας την οντότητα στην οποία έχουν εκχωρηθεί τα δικαιώματα ή οι υποχρεώσεις.
2. Resource (XACML) σε Asset/Target (ODRL):

   Στην XACML, ο πόρος αναφέρεται στο αντικείμενο ή το ψηφιακό στοιχείο στο οποίο έχει πρόσβαση ή προστατεύεται. Η ιδιότητα Asset/Target στην ODRL εκπληρώνει παρόμοιο ρόλο αντιπροσωπεύοντας το ψηφιακό στοιχείο στο οποίο εφαρμόζονται τα δικαιώματα και τα δικαιώματα. Ως εκ τούτου, ο πόρος στην XACML αντιστοιχίζεται στην ιδιότητα Asset/Target στην ODRL.
3. Action (XACML) σε Action (ODRL):

   Τόσο η XACML όσο και η ODRL χρησιμοποιούν τον όρο "Action" για να αναπαραστήσουν τη συγκεκριμένη λειτουργία ή δραστηριότητα που εκτελείται στον πόρο.
4. Obligation (XACML) σε Duty/Obligation (ODRL):

   Η XACML επιτρέπει τη συμπερίληψη υποχρεώσεων, οι οποίες είναι προϋποθέσεις ή ενέργειες που πρέπει να εκπληρωθούν ή να εκτελεστούν όταν παρέχεται πρόσβαση σε έναν πόρο. Στην ODRL, παρόμοιες έννοιες αντιπροσωπεύονται από καθήκοντα ή υποχρεώσεις.
5. Rules (XACML) σε Constraints (ODRL):

   Οι κανόνες XACML ορίζουν τις προϋποθέσεις που πρέπει να πληρούνται για να αξιολογηθεί μια πολιτική ως αληθής ή ψευδής. Οι περιορισμοί στην ODRL εξυπηρετούν παρόμοιο σκοπό ορίζοντας προϋποθέσεις ή περιορισμούς στη χρήση ή τα δικαιώματα που σχετίζονται με ένα ψηφιακό στοιχείο.

Ανάλυση των βημάτων:

1. Αναλύει το αρχείο που δόθηκε και εξάγει τα χαρακτηριστικά και τους κανόνες πολιτικής:
   a. Ανάγνωση του αρχείου: Για να εξάγουμε τα χαρακτηριστικά και τις πολιτικές, θα πρέπει να διαβάσουμε τα περιεχόμενα του αρχείου. Κάποια βιβλιοθήκη της γλώσσας προγραμματισμού ή κάποιο εξωτερικό εργαλείο μπορούν να χρησιμοποιηθούν.
   b. Εξαγωγή χαρακτηριστικών XACML:
      i. Ψάχνουμε τα Subjects, Resource και Action.
      ii. Εξαγωγή των τιμών των χαρακτηριστικών απο τα αντίστοιχα στοιχεία της XACML.
      iii. Εάν δεν βρέθηκαν τιμές χαρακτηριστικών, ορίζουμε την αντίστοιχη μεταβλητή σε null ή κενή τιμή.

c. Εξαγωγή πολιτικών XACML:
    i. Για κάθε κανόνα μέσα στην πολιτική:
        1. Εξάγουμε το Rule ID και το Effect που δίνει σε κάθε κανόνα, με χρήση API.
        2. Εξάγουμε το Condition του κάθε κανόνα.
        3. Εάν δεν βρέθηκαν τιμές χαρακτηριστικών, ορίζουμε την αντίστοιχη μεταβλητή σε null ή κενή τιμή.

2. Μετατρέπει τα εξαγμένα XACML χαρακτηριστικά στα αντίστοιχα ODRL χαρακτηριστικά. Αυτή η μετατροπή απαιτεί την αντιστοίχηση των πολιτικών και των χαρακτηριστικών, οι οποίες είναι οι ακόλουθες:
    a. Συσχέτιση των XACML χαρακτηριστικών με τις ODRL ιδιότητες:
        i. Συνάρτηση ConvertAttribute(XACML Attribute) η οποία γυρνάει το αντίστοιχο ODRL element.
        ii. Χρησιμοποιεί ένα mapping table για να βρει τις αντιστοιχίες(Βλέπε πιο κάτω).
        iii. Επιστρέφει το αναγνωρισμένο(identified) στοιχείο.
    b. Συσχέτιση των XACML πολιτικών με τις ODRL πολιτικές:
        i. Συνάρτηση ConvertPolicy(Struct XACML_Policy), παίρνει σαν παράμετρο κάποια δομή S_Rules.
        ii. (Αν αυτή υπάρχει, αλλίως θα πρέπει να δημιουργηθεί. Θα έχει μέσα τα απαραίτητα στοιχεία όπως Rule ID, Effect, Rule Specific Subjects, Resources και Actions).
        iii. Επιστρέφει μία δομή με τα αντίστοιχα πεδία της ODRL. Η δομή της ODRL έχει τα στοιχεία:
            1. Target
            2. Action
            3. Constraints
            4. Assigner
            5. Assignee
            6. Policy ID (uid)
            7. Obligation

3. Γράφει στο αρχείο εξόδου, την ODRL με τα μετατρεπόμενα χαρακτηριστικά και τις μετατρεπόμενες πολιτικές:
    a. Δημιουργούμε ένα αντικείμενο(class) της ODRL πολιτικής(απαιτείται η χρήση - και η ύπαρξη - βιβλιοθήκης για να γίνει αυτό).
    b. Βάζουμε το uid χρησιμοποιώντας την τιμή που επιστρέφεται από τη συνάρτηση ConvertPolicy.
    c. Δημιουργούμε ένα αντικείμενο κανόνα ODRL για κάθε κανόνα XACML που επιστρέφεται από τη συνάρτηση ConvertPolicy.

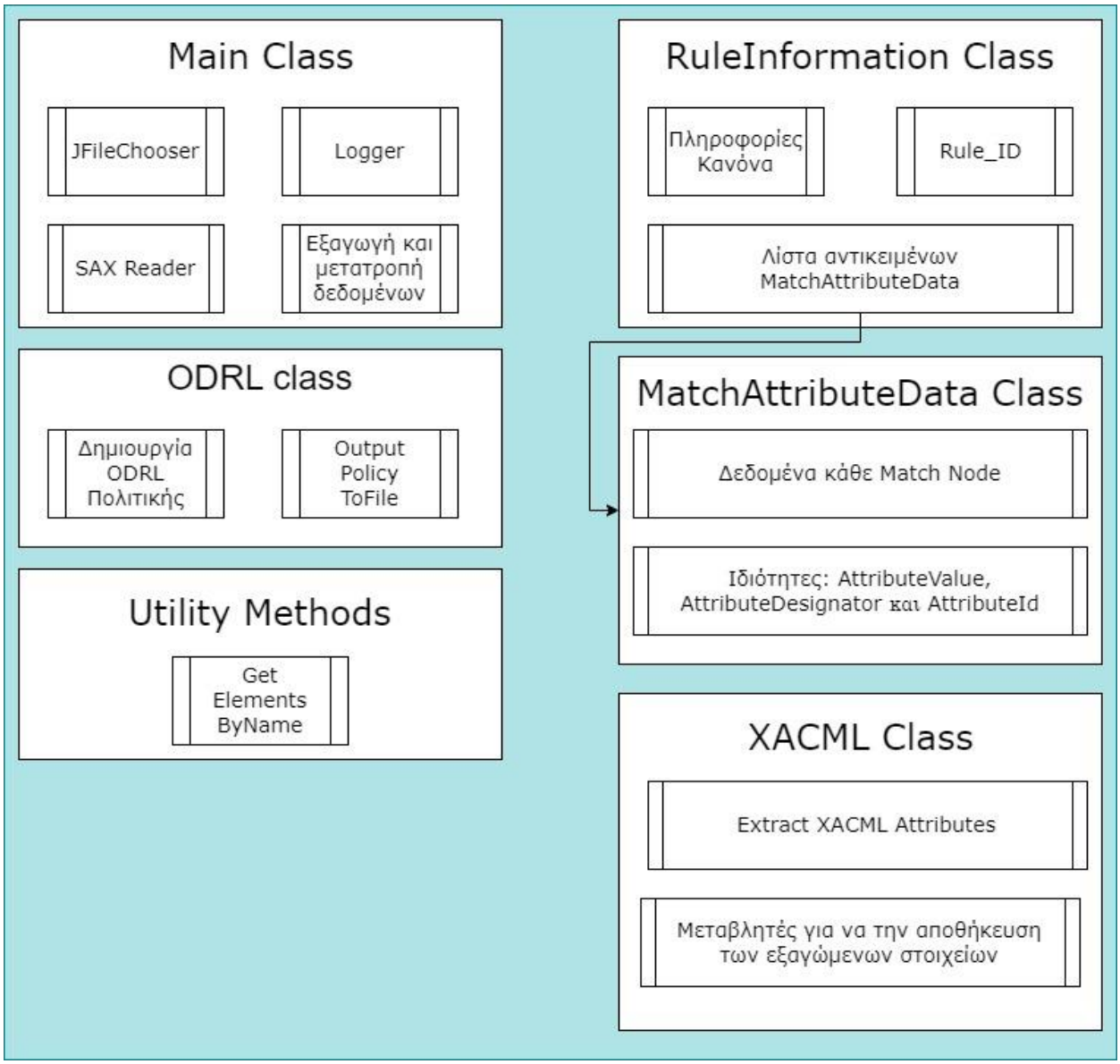
d. Για κάθε αντικείμενο κανόνα ODRL, ορίζουμε το Effect (Permit ή Deny), Subjects, Resources, Actions και Constraints (εάν υπάρχουν).
e. Προσθέτουμε το αντικείμενο κανόνα ODRL(όσα υπάρχουν) στην πολιτική του βήματος 1.
f. Προσθέτουμε τυχόν πρόσθετα στοιχεία ODRL στο αντικείμενο Πολιτικής ODRL όπως Assigner, Assignee ή Obligation.

Σειριοποιούμε, αν δεν είναι ήδη σε αυτήν την μορφή, ώστε να μετατρέψουμε την πολιτική σε μία μορφή που μπορεί να αποθηκευτεί. Εξάγουμε την μετατρεπόμενη πολιτική σε ένα αρχείο τύπου ttl, ο τύπος αρχείου της ODRL.

Αρχιτεκτονική Συστήματος

Το σύστημα είναι δομημένο σε πολλές κλάσεις:

- Η Main Class χρησιμεύει ως σημείο εισόδου και συντονίζει τη ροή του συστήματος.
- Η κλάση RuleInformation ενσωματώνει πληροφορίες που σχετίζονται με κανόνες.
- Η κλάση ODRL χειρίζεται τη δημιουργία της πολιτικής και την εκτύπωση της στο αρχείο.
- Η κλάση MatchAttributeData χειρίζεται την αντιστοίχιση χαρακτηριστικών.
- Η κλάση XACML χειρίζεται λειτουργίες που αφορούν την XACML πολιτική.



Σχήμα 4: Αρχιτεκτονική Συστήματος

Αυτή η δομή επιτρέπει τη οργανωμένη σχεδίαση, διαχωρίζοντας το σύστημα για την καλύτερη οργάνωση κώδικα, επαναχρησιμοποίηση και δυνατότητα συντήρησης. Κάθε τάξη εστιάζει σε μια συγκεκριμένη πτυχή, επιτρέποντας την εύκολη τροποποίηση ή επέκταση των λειτουργιών χωρίς να επηρεάζεται η συνολική δομή του συστήματος.

Main Class:

- Αυτή η κλάση περιέχει την κύρια μέθοδο, η οποία χρησιμεύει ως σημείο εισόδου για την εφαρμογή.
- Αλληλεπιδρά με τον χρήστη για να επιλέξει αρχεία εισόδου και εξόδου χρησιμοποιώντας το JFileChooser.
- Ρυθμίζει τον logger και διαβάζει το αρχείο εισόδου XML χρησιμοποιώντας το SAXReader.
- Εξάγει πληροφορίες κανόνων από το έγγραφο XML χρησιμοποιώντας τη μέθοδο ExtractXACMLAttributes.
- Δημιουργεί μια πολιτική ODRL, δικαιώματα και περιορισμούς με βάση τις εξαγόμενες πληροφορίες κανόνων.
- Τέλος, γράφει την πολιτική που δημιουργείται στο αρχείο εξόδου χρησιμοποιώντας τη μέθοδο OutputPolicyToFile.

RuleInformation Class:

- Αυτή η κλάση αντιπροσωπεύει τις πληροφορίες για κάθε κανόνα που εξάγεται από το έγγραφο XML.
- Έχει μια ιδιότητα Rule_ID και μια λίστα αντικειμένων MatchAttributeData.

MatchAttributeData Class:

- Αυτή η κλάση αντιπροσωπεύει τα δεδομένα χαρακτηριστικών για κάθε κόμβο αντιστοίχισης σε έναν κανόνα.
- Περιέχει ιδιότητες όπως AttributeValue, AttributeDesignator και AttributeId.

Μέθοδοι χρησιμότητας(Utility Methods):

- ExtractXACMLAttributes: Παίρνει μια λίστα με στοιχεία XML που αντιπροσωπεύουν κανόνες και εξάγει τα απαραίτητα χαρακτηριστικά, συμπληρώνοντας τα αντικείμενα RuleInformation.
- OutputPolicyToFile: Παίρνει ένα αντικείμενο Πολιτικής και μια διαδρομή αρχείου εξόδου, σειριοποιεί την πολιτική στη σύνταξη Turtle RDF χρησιμοποιώντας ODRLRDF και την γράφει στο αρχείο εξόδου.

- GetElementsByName: Είναι μια αναδρομική βοηθητική μέθοδος που βρίσκει όλα τα στοιχεία XML με ένα δεδομένο όνομα μέσα σε ένα γονικό στοιχείο.

Το σύστημα είναι γραμμένο σε Java. Οι τεχνολογίες και οι βιβλιοθήκες που χρησιμοποιούνται σε αυτό το σύστημα περιλαμβάνουν:

- Java I/O: Το σύστημα χρησιμοποιεί διάφορες κλάσεις από το πακέτο java.io, όπως File, FileWriter και FileReader, για χειρισμό αρχείων και λειτουργίες εισόδου/εξόδου.
- Swing: Το σύστημα εισάγει το javax.swing.JFileChooser για να δημιουργήσει ένα παράθυρο διαλόγου επιλογής αρχείων για την επιλογή των αρχείων εισόδου και εξόδου.
- Μοντέλο ODRL: Το σύστημα εισάγει κλάσεις από το πακέτο odrlmodel, το οποίο είναι μια προσαρμοσμένη βιβλιοθήκη για εργασία με το μοντέλο ODRL (Open Digital Rights Language).
- Apache Log4j: Το σύστημα εισάγει κλάσεις από το πακέτο org.apache.log4j για να διαμορφώσει την καταγραφή και να ορίσει το επίπεδο καταγραφής.
- Dom4j: Το σύστημα εισάγει κλάσεις από το πακέτο org.dom4j για ανάγνωση και χειρισμό εγγράφων XML.
- Apache Jena: Το σύστημα εισάγει κλάσεις από το πακέτο org.apache.jena.riot, το οποίο αποτελεί μέρος της βιβλιοθήκης Apache Jena, για εργασία με δεδομένα RDF (Resource Description Framework) και σειριοποίηση.

Συνολικά, το σύστημα χρησιμοποιεί βιβλιοθήκες πυρήνων Java για χειρισμό αρχείων, ανάλυση XML και καταγραφή. Περιλαμβάνει επίσης προσαρμοσμένες βιβλιοθήκες για εργασία με ODRL και χρησιμοποιεί Apache Jena για σειριοποίηση RDF.

Τέλος, θα ήθελα να αναφέρω το Εργαλείο πολιτικής XACML (διαθέσιμο στη διεύθυνση https://github.com/gsoultos/policy-tool). Αυτό το εργαλείο έχει συμβάλει στην απλοποίηση της διαδικασίας δημιουργίας πολιτικών XACML, επιτρέποντάς μου να δημιουργήσω πολιτικές που ευθυγραμμίζονται με τις προδιαγραφές ελέγχου πρόσβασης πιο αποτελεσματικά.

Παράδειγμα χρήσης

Η ανάγκη για έλεγχο πρόσβασης ψηφιακού περιεχομένου

Στην τεράστια σφαίρα των ψηφιακών εκδόσεων, ένας διάσημος εκδοτικός οίκος αντιμετώπισε μια πιεστική πρόκληση. Καθώς η ζήτηση για τα επιστημονικά του άρθρα αυξήθηκε στα ύψη, συνειδητοποίησαν την κρίσιμη σημασία της διατήρησης του ελέγχου των δικαιωμάτων πρόσβασης ακόμη και μετά τη λήψη του περιεχομένου από τους χρήστες. Αναζήτησαν μια λύση που θα έφερνε μια ισορροπία μεταξύ της δυνατότητας πρόσβασης και της προστασίας της πνευματικής ιδιοκτησίας τους.

Καθοδηγούμενος από την ανάγκη για ένα ισχυρό σύστημα ελέγχου πρόσβασης, ο εκδοτικός οίκος ξεκίνησε μια προσπάθεια να βρει έναν τρόπο να προστατεύσει το ψηφιακό τους περιεχόμενο. Μια ταλαντούχα ομάδα μηχανικών υπολογιστών συγκεντρώθηκαν για να σχεδιάσουν ένα σύστημα που θα μπορούσε να διαχειρίζεται απρόσκοπτα τα δικαιώματα ελέγχου πρόσβασης μετά τη λήψη.

Η ομάδα εμβάθυνε στις περιπλοκές των πλαισίων ελέγχου πρόσβασης, μελετώντας διάφορα βιομηχανικά πρότυπα. Στόχος τους ήταν να δημιουργήσουν ένα σύστημα που θα μπορούσε να μετατρέψει τις πολιτικές ελέγχου πρόσβασης σε πολιτικές διαχείρισης ψηφιακών δικαιωμάτων, διασφαλίζοντας ολοκληρωμένο έλεγχο στη χρήση και τη διανομή του ψηφιακού περιεχομένου τους.

Μετά από εκτεταμένη έρευνα και ανάπτυξη, η ομάδα ανέπτυξε ένα πρωτοποριακό σύστημα που εύστοχα ονομάστηκε "AccessGuard". Αυτό το σύστημα αξιοποίησε μηχανισμούς επιβολής πολιτικής για να παρέχει ένα ασφαλές περιβάλλον για το ψηφιακό περιεχόμενο του εκδότη.

Το AccessGuard λειτουργεί μετατρέποντας τις πολιτικές ελέγχου πρόσβασης σε πολιτικές διαχείρισης ψηφιακών δικαιωμάτων. Αυτή η μετατροπή επέτρεψε στον εκδοτικό οίκο να εκχωρήσει συγκεκριμένα δικαιώματα και άδειες στους χρήστες ακόμη και μετά τη λήψη του περιεχομένου. Το σύστημα επέτρεψε λεπτομερή έλεγχο σε διάφορες πτυχές, συμπεριλαμβανομένων των προνομίων προβολής, των περιορισμών κοινής χρήσης και της πρόσβασης με χρονικό περιορισμό.

Με τη λειτουργία του AccessGuard, ο εκδοτικός οίκος θα μπορούσε να διανέμει με σιγουριά το ψηφιακό περιεχόμενό του, διασφαλίζοντας παράλληλα τη διατήρηση των δικαιωμάτων πνευματικής ιδιοκτησίας του. Οι χρήστες επωφελήθηκαν από μια ασφαλή και προσαρμοσμένη εμπειρία πρόσβασης, σεβόμενοι τα δικαιώματα και τους περιορισμούς που περιγράφονται στις πολιτικές διαχείρισης ψηφιακών δικαιωμάτων.

Καθώς ο εκδοτικός οίκος εφάρμοζε το πρωτοποριακό του σύστημα, το AccessGuard, η πραγματική δύναμη της λύσης τους έγινε εμφανής. Η AccessGuard μετέφρασε απρόσκοπτα τις αρχές και τους στόχους των πολιτικών ελέγχου πρόσβασης σε πρακτικές πολιτικές διαχείρισης ψηφιακών δικαιωμάτων. Οι μετασχηματιστικές δυνατότητες του συστήματος επέτρεψαν στον εκδοτικό οίκο να επιβάλει συγκεκριμένους κανόνες και άδειες ακόμη και αφού οι χρήστες κατέβασαν τα επιστημονικά τους άρθρα. Ας εξετάσουμε μερικά παραδείγματα τέτοιων κανόνων στη φυσική γλώσσα, που απεικονίζουν την απρόσκοπτη μετατροπή από XACML σε ODRL:

1. Κανόνας 1:
   - XACML: Επιτρέπεται η πρόσβαση στο ληφθέν αρχείο εάν ο ρόλος του χρήστη είναι "κάτοχος" ή "διαχειριστής".
   - ODRL: Επιτρέπεται στον χρήστη με το ρόλο του "κατόχου" ή "διαχειριστή" να αποκτήσει πρόσβαση στο ληφθέν αρχείο.
2. Κανόνας 2:
   - XACML: Απαγορεύεται η πρόσβαση στο ληφθέν αρχείο εάν η συνδρομή του χρήστη έχει λήξει.
   - ODRL: Επιτρέπεται η πρόσβαση στο ληφθέν αρχείο εφόσον ο χρήστης έχει ενεργή συνδρομή.
3. Κανόνας 3:
   - XACML: Επιτρέπεται η εκτύπωση του ληφθέντος αρχείου εάν ο χρήστης είναι μέλος της ομάδας "premium".
   - ODRL: Επιτρέπεται στους χρήστες της ομάδας "premium" να εκτυπώσουν το ληφθέν αρχείο.
4. Κανόνας 4:
   - XACML: Απαγορεύεται η αντιγραφή ή η προώθηση του ληφθέντος αρχείου σε οποιαδήποτε εξωτερική συσκευή ή παραλήπτη.
   - ODRL: Περιορισμός της αντιγραφής ή της προώθησης του ληφθέντος αρχείου σε εξωτερικές συσκευές ή παραλήπτες.
5. Κανόνας 5:
   - XACML: Επιτρέπεται η πρόσβαση στο ληφθέν αρχείο για ερευνητικούς σκοπούς από χρήστες που συνδέονται με εκπαιδευτικά ιδρύματα.
   - ODRL: Επιτρέπεται η πρόσβαση στο ληφθέν αρχείο για ερευνητικούς σκοπούς από χρήστες που συνδέονται με εκπαιδευτικά ιδρύματα.

Παράδειγμα Μετατροπής

Ας δούμε τώρα ένα παράδειγμα μετατροπής μίας XACML πολιτικής στην αντίστοιχη πολιτική ODRL. Έστω ότι θέλουμε οι πόροι να είναι προσβάσιμοι αν ο χρήστης θέλει να τους χρησιμοποιήσει για ερευνητικούς σκοπούς. Δίνεται η ακόλουθη XACML πολιτική:

```
1     <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2     <Policy PolicyId="research-access" Version="1" RuleCombiningAlgId=""
3  MaxDelegationDepth="0"
4  xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
5        <Description>Policy to allow access to the downloaded file for
6  research purposes</Description>
7        <Target>
8           <AnyOf>
9              <AllOf>
10                <Match
11 MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
12                   <AttributeValue DataType="string">User</AttributeValue>
13                   <AttributeDesignator
14 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
15 AttributeId="user" DataType="string" Issuer="" MustBePresent="true"/>
16                </Match>
17                <Match
18 MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
19                   <AttributeValue
20 DataType="string">FileinQuestion</AttributeValue>
21                   <AttributeDesignator
22 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
23 AttributeId="fileinquestion" DataType="string" Issuer=""
24 MustBePresent="true"/>
25                </Match>
26                <Match
27 MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
28                   <AttributeValue
29 DataType="string">AccessforResearchPurposes</AttributeValue>
30                   <AttributeDesignator
31 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
32 AttributeId="accessforresearchpurposes" DataType="string" Issuer=""
33 MustBePresent="true"/>
34                </Match>
35             </AllOf>
36          </AnyOf>
37       </Target>
38       <Rule RuleId="research-access" Effect="Permit">
```

```
        <Description>Rule regarding file access for research
purposes</Description>
        <Target>
          <AnyOf>
            <AllOf>
              <Match
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="string">User</AttributeValue>
                <AttributeDesignator
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:subject"
AttributeId="user" DataType="string" Issuer="" MustBePresent="true"/>
              </Match>
              <Match
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue
DataType="string">FileinQuestion</AttributeValue>
                <AttributeDesignator
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
AttributeId="fileinquestion" DataType="string" Issuer=""
MustBePresent="true"/>
              </Match>
              <Match
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue
DataType="string">AccessforResearchPurposes</AttributeValue>
                <AttributeDesignator
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
AttributeId="accessforresearchpurposes" DataType="string" Issuer=""
MustBePresent="true"/>
              </Match>
            </AllOf>
          </AnyOf>
        </Target>
      </Rule>
    </Policy>
```

Για την εξαγωγή της ακόλουθης ODRL πολιτικής χρησιμοποιήθηκε το εργαλείο που ανέπτυξα κατά την διάρκεια της εκπόνησης της πτυχιακής μου εργασίας. Δίνεται η ακόλουθη πολιτική ODRL:

```
@prefix cc:    <http://creativecommons.org/ns#> .
@prefix void:  <http://rdfs.org/ns/void#> .
@prefix dct:   <http://purl.org/dc/terms/> .
@prefix rdf:   <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs:  <http://www.w3.org/2000/01/rdf-schema#> .
@prefix ldr:   <http://purl.oclc.org/NET/ldr/ns#> .
@prefix gr:    <http://purl.org/goodrelations/> .
```

```
@prefix odrl:  <http://www.w3.org/ns/odrl/2/> .
@prefix dcat:  <http://www.w3.org/ns/dcat#> .
@prefix prov:  <http://www.w3.org/ns/prov#> .

<http://salonica.dia.fi.upm.es/ldr/constraint/3ae73149-7b44-434c-8897-
ec4642d52368>
      a            odrl:Constraint ;
      <User>       "user" ;
      odrl:operator  <eq> .

<User>  a      odrl:Party .

<http://salonica.dia.fi.upm.es/ldr/policy/0c975ead-5c62-453b-a016-64c50ffb5845>
      a              odrl:Policy , odrl:Set ;
      rdfs:label     "0c975ead-5c62-453b-a016-64c50ffb5845" ;
      odrl:permission  [ a              odrl:Permission ;
                  odrl:action     <AccessforResearchPurposes> ;
                  odrl:assignee    <User> ;
                  odrl:constraint
<http://salonica.dia.fi.upm.es/ldr/constraint/3ae73149-7b44-434c-8897-
ec4642d52368> ;
                  odrl:target     "FileinQuestion"
                ] .
```

Τώρα ας εμβαθύνουμε στη διαδικασία αντιστοίχισης των στοιχείων για την παραγωγή της τελικής πολιτικής ODRL. Αρχικά, το σύστημα εξάγει τις τιμές χρήστη (Subject, Resource, Action) από την πολιτική XACML, όπως υποδεικνύεται από τις γραμμές 46, 54 και 63, αντίστοιχα. Αυτές οι εξαγόμενες τιμές χρησιμεύουν ως βάση για τη δημιουργία της πολιτικής ODRL.

Στην περίπτωση που υπάρχουν πολλοί κανόνες στην πολιτική XACML, κάθε κανόνας αντιστοιχεί σε ένα permission αντικείμενο στην πολιτική ODRL που προκύπτει (γραμμές 23-30 στην πολιτική ODRL). Έτσι, μετά την επιτυχή εξαγωγή των απαραίτητων στοιχείων, πρέπει να δημιουργηθεί ένα αντικείμενο permission για κάθε τριάδα στοιχείων που βρήκαμε στο προηγούμενο βήμα (Subject, Resource, Action).

Για τη δημιουργία των permission αντικειμένων, η διαδικασία μετατροπής ακολουθεί έναν πίνακα αντιστοίχισης που περιγράφεται στην ενότητα Αλγόριθμος Μετατροπής. Αυτοί οι κανόνες καθορίζουν την αντιστοίχιση των στοιχείων XACML στα αντίστοιχα της ODRL.

Κάθε permission αντικείμενο στην ODRL περιλαμβάνει ένα Action, ένα Subject, ένα Constraint και ένα Target. Οι τιμές εκχωρούνται με βάση τους κανόνες αντιστοίχισης. Εάν δεν υπάρχουν constraints που καθορίζονται στον κανόνα

XACML, όπως γίνεται και στο παράδειγμα μας, ενδέχεται να χρησιμοποιηθούν προεπιλεγμένες τιμές ή τιμές null στην πολιτική ODRL.

Τέλος, αξίζει να σημειωθεί ότι η επίτευξη πλήρους μετατροπής από XACML σε ODRL δεν είναι πάντα εφικτή, καθώς οι δύο γλώσσες έχουν εγγενείς διαφορές που ενδέχεται να περιορίσουν την έκταση της μετατροπής.

Συμπεράσματα και Μελλοντική Εργασία

Συμπερασματικά, η παρούσα πτυχιακή διερεύνησε την επιβολή κανόνων ελέγχου πρόσβασης χρησιμοποιώντας τεχνολογία διαχείρισης ψηφιακών δικαιωμάτων, με στόχο την ανάπτυξη ενός συστήματος που θα μπορούσε να διαχειρίζεται τα δικαιώματα ελέγχου πρόσβασης ακόμη και μετά τη λήψη του περιεχομένου, διασφαλίζοντας τον πλήρη έλεγχο της χρήσης και διανομής ψηφιακού περιεχομένου. Το παράδειγμα που παρουσιάστηκε στην προηγούμενη ενότητα κατέδειξε τη μετατροπή από XACML σε ODRL, δείχνοντας πώς το σύστημα επιτρέπει την επιβολή κανόνων και αδειών μετά τη λήψη περιεχομένου. Εξουσιοδοτώντας τους εκδότες να επιβάλλουν κανόνες που βασίζονται σε διάφορους παράγοντες, όπως ρόλους χρήστη, κατάσταση συνδρομής, ιδιότητα μέλους ομάδας και ιδρύματα, το σύστημα διασφαλίζει τη συμμόρφωση με τις απαιτήσεις ελέγχου πρόσβασης.

Η επιτυχής εφαρμογή αυτού του συστήματος υπογραμμίζει το ευρύτερο δυναμικό και τη σημασία της επιβολής κανόνων ελέγχου πρόσβασης με χρήση της τεχνολογίας DRM. Αποτελεί παράδειγμα της πρακτικής εφαρμογής της τεχνολογίας DRM, τονίζοντας τη σημασία της διατήρησης του ελέγχου του ψηφιακού περιεχομένου στον σημερινό διασυνδεδεμένο και ψηφιοποιημένο κόσμο. Αυτό το επίτευγμα ενισχύει περαιτέρω το DRM ως ζωτικής σημασίας εργαλείο για οργανισμούς και βιομηχανίες που επιδιώκουν να προστατεύσουν τα ψηφιακά τους στοιχεία, ενώ παράλληλα εξισορροπούν την προσβασιμότητα και την προστασία στην ψηφιακή εποχή.

Προχωρώντας προς τα εμπρός, η μελλοντική έρευνα θα μπορούσε να επικεντρωθεί στην ενίσχυση των δυνατοτήτων του συστήματος και στη διερεύνηση της ενσωμάτωσής του με άλλες τεχνολογίες DRM ή πλαίσια ελέγχου πρόσβασης. Επιπλέον, η διερεύνηση των πτυχών επεκτασιμότητας και απόδοσης του συστήματος θα ήταν πολύτιμη για να διασφαλιστεί η καταλληλότητά του για εφαρμογές μεγαλύτερης κλίμακας. Συνολικά, αυτή η πτυχιακή συμβάλλει στο πεδίο παρέχοντας μια αρχική προσέγγιση για την επιβολή κανόνων ελέγχου πρόσβασης χρησιμοποιώντας την τεχνολογία DRM. Τα ευρήματα και οι ιδέες που παρουσιάζονται θέτουν τις βάσεις για περαιτέρω προόδους στη διασταύρωση του ελέγχου πρόσβασης και της διαχείρισης ψηφιακών δικαιωμάτων, ωφελώντας τις βιομηχανίες και τους οργανισμούς στην προσπάθειά τους να προστατεύσουν το ψηφιακό περιεχόμενο, ενώ παράλληλα επιτρέπουν την ελεγχόμενη πρόσβαση και διανομή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Access Control (Sabrina De Capitani di Vimercati, Pierangela Samarati, Ravi S. Sandhu -- Computing Handbook, 3rd ed., 2014).
2. Managing digital rights with rights expression languages by Demian Hess.
3. These Are Your Rights -- A Natural Language Processing Approach to Automated RDF Licenses Generation Elena Cabrio, Alessio Palmero Aprosio and Serena Villata.
4. A beginner's guide to XACML https://medium.com/identity-beyond-borders/a-beginners-guide-to-xacml-6dc75b547d55
5. eXtensible Access Control Markup Language (XACML) Version 3.0 http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
6. ODRL COMMUNITY GROUP https://www.w3.org/community/odrl/
7. ODRL Information Model 2.2 https://www.w3.org/TR/odrl-model/
8. ODRLAPI https://oeg-upm.github.io/odrlapi/
9. ODRL2.0 Simple API https://oeg-upm.github.io/odrlapi/htmldoc/html/annotated.html
10. Flexible XML framework for Java https://dom4j.github.io/