UNIVERSITI PUTRA MALAYSIA

HETEROGENEITY POLICY EVALUATION WITH MODALITY CONFLICT ANALYSIS

TEO POH KUANG

FSKTM 2017 69

HETEROGENEITY POLICY EVALUATION WITH MODALITY CONFLICT ANALYSIS

By

TEO POH KUANG

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Doctor of Philosophy

March 2017

© COPYRIGHT UPM

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

HETEROGENEITY POLICY EVALUATION WITH MODALITY CONFLICT ANALYSIS

By

TEO POH KUANG

March 2017

Chairperson : Hamidah Ibrahim, PhD
Faculty : Computer Science and Information Technology

Policy evaluation is a process to determine whether a request satisfies the access control policies. There are two main phases in the policy evaluation, namely: (i) matching the attribute values of a request and a policy, and (ii) detecting modality conflict. Existing policy evaluation engines utilized a simple string equal matching function, but they do not explore naming heterogeneity. The authorizations could be propagated according to the inheritance relationships between concepts along not only subject, resource, action, but also location hierarchies. This thesis aimed to propose matching functions which are not limited to string equal matching function that aim to resolve naming heterogeneity, namely: synonym equal, hyponym, syntactical-synonym equal, syntactical-hyponym, syntactical equal, hyponym common word, and abbreviation equal. An authorization propagation rule is proposed to identify the applicable policies, which relies on inheritance relationships between concepts, on the basis of the partially ordered structures obtained by classifying subject, resource, action, and condition attributes. Our solution assists the policy administrators in filtering out the irrelevant policies which helps them to resolve the modality conflict among the applicable policies before the actual policy evaluation taken place. We have evaluated the effectiveness of our proposed solution on real XACML policies for university, conference management, and health-care domain. Our solution resulted lower percentage of *R* but higher percentage of *P* and *F* for all sets of policies when more attributes are considered in retrieving the applicable policies and in detecting the modality conflict compared when these constraints are not considered. Our solution achieved the higher percentage of *P*, *R* and *F* in matching the attribute values of a request and a policy, in retrieving the applicable policies, and in detecting modality conflict as compared to the previous work. The accuracy of the proposed solution indicates that our proposed solution is better than the Sun's XACML implementation in policy evaluation.

© COPYRIGHT UPM

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PENILAIAN POLISI KAWALAN CAPAIAN PENAMAAN KEPELBAGAIAN DENGAN ANALISI KONFLIK MODALITI

Oleh

TEO POH KUANG

Mac 2017

Pengerusi : Hamidah Ibrahim, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Penilaian polisi adalah satu proses untuk menentukan sama ada permintaan memenuhi polisi kawalan capaian. Terdapat dua fasa utama dalam penilaian polisi, iaitu: (i) memadan nilai atribut permintaan dan polisi, dan (ii) mengesan konflik modaliti. Enjin penilaian polisi sedia ada menggunakan fungsi *string equal matching* yang mudah, tetapi mereka tidak meneroka kepelbagaian penamaan. Kebenaran boleh disebarkan berdasarkan hubungan warisan di antara konsep bukan sahaja subjek, sumber, dan tindakan, tetapi juga lokasi hierarki. Tesis ini adalah bertujuan untuk mencadangkan fungsi pemadanan yang tidak terhad kepada fungsi *string equal matching* yang bertujuan untuk menyelesaikan kepelbagaian penamaan, iaitu: *synonym equal*, *hyponym*, *syntactical-synonym equal*, *syntactical-hyponym*, *syntactical equal*, *hyponym common word*, and *abbreviation equal*. Peraturan penyebaran kebenaran dicadangkan untuk mengenal pasti polisi yang boleh dilaksanakan, yang bergantung kepada hubungan warisan antara konsep, atas dasar struktur turutan separa yang diperolehi dengan mengklasifikasikan atribut subjek, sumber, tindakan, dan keadaan. Penyelesaian kami adalah untuk membantu polisi pentadbir dalam menapis polisi yang tidak berkaitan dengan membantu mereka menyelesaikan konflik modaliti di antara polisi yang boleh dilaksanakan sebelum penilaian polisi yang sebenar berlaku. Kami telah menilai keberkesanan penyelesaian kami ke atas polisi XACML yang sebenar untuk domain universiti, pengurusan persidangan, dan kesihatan. Penyelesaian kami menghasilkan peratusan yang lebih rendah *R* tetapi peratusan yang lebih tinggi *P* dan *F* untuk semua polisi set apabila sifat-sifat yang lebih terlibat dalam mancapai polisi yang boleh dilaksanakan dan mengesan konflik modaliti berbanding apabila kekangan ini tidak terlibat. Penyelesaian kami mencapai peratusan yang lebih tinggi *P*, *R* and *F* dalam memadankan nilai atribut permintaan dan polisi, dalam mancapai polisi yang boleh dilaksanakan, dan dalam mengesan konflik modaliti. Ketepatan penyelesaian yang dicadangkan menunjukkan bahawa penyelesaian yang dicadangkan adalah lebih baik daripada pelaksanaan Sun's XACML dalam penilaian polisi.

© COPYRIGHT UPM

ACKNOWLEDGEMENTS

First and foremost, all praise to the almighty God for his blessings and merciful that enables me to learn.

I am sincerely grateful to my supervisor, Prof. Dr. Hamidah Ibrahim, for giving me the great opportunity and confidence to work under her professional and thorough supervision, for her genuine interest in my research and career, for never being too busy to set regular time aside for getting together, for stimulating conversations, for providing invaluable advices on many topics and for her patience. Besides, I would like to express my sincere thanks and appreciation to the supervisory committee members, Assoc. Prof. Dr. Fatimah Sidi and Assoc. Prof. Dr. Nur Izura Udzir for their continued patience, guidance, suggestions and advices throughout the journey.

My PhD study was supported by a grant fellowship (GRF) from the School of Graduate Studies at University Putra Malaysia. I would like to take this opportunity to thank the University for the generous financial support.

I cannot end without thanking my family. I owe so much to my dear mother and father, who are always my source of inspiration and who encourage me to learn and support me throughout my life. I would also like to thank my brother, my sister and my sister in law for their patience.

Teo Poh Kuang

July 2017

© COPYRIGHT UPM

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Hamidah Binti Ibrahim, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Fatimah Sidi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Nur Izura Binti Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

____

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

© COPYRIGHT UPM

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work
- quotations, illustrations and citations have been duly acknowledged;
- ownership of intellectual property from the thesis is as stipulated in the Memorandum of Agreement (MoA), or as according to the Universiti Putra Malaysia (Research) Rules 2012, in the event where the MoA is absent;
- permission from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) are required prior to publishing it (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ________________________ Date: __________________

Name and Matric No: Teo Poh Kuang (GS23442)

© COPYRIGHT UPM

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: ___________________________
Name of
Chairman of
Supervisory
Committee: Prof. Dr. Hamidah Binti Ibrahim

Signature: _________________________
Name of
Member of
Supervisory
Committee: Assoc. Prof. Dr. Fatimah Sidi

Signature: _________________________________
Name of
Member of
Supervisory
Committee: Assoc. Prof. Dr. Nur Izura Binti Udzir

© COPYRIGHT UPM

TABLE OF CONTENTS

© COPYRIGHT UPM

© COPYRIGHT UPM

LIST OF TABLES

© COPYRIGHT UPM

© COPYRIGHT UPM

© COPYRIGHT UPM

© COPYRIGHT UPM

© COPYRIGHT UPM

LIST OF FIGURES

© COPYRIGHT UPM

LIST OF ABBREVIATIONS

A+	Positive Authorization
A-	Negative Authorization
ABAC	Attributed-Based Access Control
ACOOS	Access Control Oriented Ontology System
DAC	Discretionary Access Control
DL	Description Logic
EGEE	Enabling Grids for E-science
GIS	Geographic *Information System*
GML	Geography Markup Language
GTRBAC	Generalized Temporal Role Based Access Control
IDF	Inverse Document Frequency
MAC	Mandatory Access Control
MOs	Managed Objects
MTBDD	Multi-Terminal Binary Decision Diagram
NLP	Natural Language Processing
O+	Positive Obligation
O-	Negative Obligation
OASIS	Organization for the Advancement of Structured Information Standards
OSG	Open Science Grid
OWL	Web Ontology Language
P2CR	Policy Composition and Conflict Resolution framework
PAP	Policy Administration Point
PCA	Policy Combining Algorithm
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
RBAC	Role-Based Access Control
RCA	Rule Combining Algorithm
RDF	Resource Description Framework
SACPL	Semantic Access Control Policy Language
SAML	Security Assertion Markup Language
SAP	Systems, Applications & Products
SOD	Separation Of Duty
SWAT	Semantic Web and Agent Technologies
SWC	Semantic Web Conference
SWRL	*Semantic Web Rule Language*
TESL	Teaching English as a Second Language
TF	Term Frequency
TF-IDF	*Term Frequency-Inverse Document Frequency*
XACML	eXtensible Access Control Mark-up Language
XML	Extensible Markup Language

© COPYRIGHT UPM

CHAPTER 1

INTRODUCTION

1.1 Overview

With the fast advancement of information technology, collaborative applications such as distributed, heterogeneous, or autonomous systems have been developed for sharing information and services. Most business organizations from small and medium sized to large multinational corporations can hardly go into operation without having to rely on information. Each of these business organizations will produce their own high volumes of data. A distributed system is a collection of independent computers that appears to its users as a single coherent system for data sharing and resource provisioning. Distributed system often belongs to different security domain, which is governed by different authorities employing heterogeneous protocols, vocabularies, data models, and organization structures. Moreover, distributed systems are often dynamic, with systems joining and leaving the collaboration at runtime. These collaborations are not fixed a priori, but can dynamically change over time as new parties join, leave, or change their responsibilities and objectives. Thus, there is a growing concern for security of data for supporting a widespread distribution of resources and collaboration of autonomous systems in a distributed environment to avoid unintended security leakages by unauthorized disclosure.

Access control is the process of mediating every request to resources and data maintained by a system which determine whether the request should be granted or denied (Samarati & di Vimercati, 2001). The authorization decision is enforced by a mechanism implementing regulations established by an access control policy. An access control policy determines who is authorized to have access to what resources and under what conditions. Policy-based management has emerged as a software model that simplifies and automates the administration of computing systems by incorporating decision-making process into its management components (Liu et al., 2011). A common requirement is represented by the need to assure security for the shared resources through access control policy. Policy languages fulfill such requirement by offering formalisms and related tools supporting the specification and analysis of such rule sets. Various types of access control policy have emerged, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attributed-based Access Control (ABAC) which defined what should, and what should not, be allowed, and, in some sense, to different definitions of what ensuring security means (Samarati & di Vimercati, 2001). DAC policies control access based on the identity of the requestor and on access rules stating what requestors are (or are not) allowed to do (Bokefode Jayant et al., 200 9999914). MAC policies control access based on mandated regulations determined by a central authority. RBAC policies control access depending on the roles that users have within the system and on rules stating what accesses

© COPYRIGHT UPM

are allowed to users in given roles. ABAC defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes (user, resource, environment, etc) together. ABAC provides fine-granularity, high flexibility, rich semantics and easily extended to support RBAC model for organizations that need greater collaboration and data sharing (Cavoukian et al., 2015).

We focus our work on access control system which is based on DAC model. The eXtensible Access Control Mark-up Language (XACML) is used to specify the policy since it is the OASIS standard language and the standard defines a declarative access control policy language implemented in XML format, which is able to express a policy in terms of rules over different kind of attributes of entities. Rules are then collected into policies and combined with rule combining algorithms. Such algorithms are used to define precedence in the application of rules if more than one of them is applicable for a single request. However, even the creation of XACML policies is well supported, it is still an ongoing work and no standard approaches have been widely accepted to evaluate and verify the authorization decision of a policy.

Policy evaluation is a process to determine whether a request satisfies the access control policies. The attribute values of a policy are compared to the attribute values of a request. The policy is considered applicable to the request if these values matched with each other. A practical distributed policy evaluation framework should be able to support autonomy in policy specification as well as interoperability among parties and policy portability (Trivellato et al., 2009). The issue of interoperability arises as policies have to be understood by all parties. In other words, each party shall be able to interact with other unambiguously and express its policy autonomously regardless of which parties have already joined the collaboration. When heterogeneous systems form coalitions that transgress the traditional boundaries among organizational, cultural, and legal units, interoperability process is required to enable mutual understanding among parties. Consider a collaborative scenario in which system partners need to compare their access control policies in order to understand if similar kind of users has similar capabilities. These kinds of requests are of particular interest in a distributed environment where users belonging to partner organizations may have the rights to access shared resources.

Matching the attribute values of a request and a policy and resolving modality conflict are two main phases in the policy evaluation that need considerable attention as the outcomes from these phases influence the correctness and completeness in defining the authorization decision to either authorize the request or deny the request. XACML policy evaluation process basically works as follows: A subject (e.g. a professor) wants to perform an action (e.g. modify) on a protected resource (e.g. grades). The subject submits this request to the Policy Enforcement Point (PEP) that manages the protected resource. The PEP formulates such a request using the XACML request language. Then, the PEP sends the XACML request down to the Policy Decision Point (PDP). The

© COPYRIGHT UPM

PDP checks the request with its XACML policy and determines whether the XACML request should be permitted or denied.

Finally, the PDP formulates our solution aimed to resolve the naming heterogeneity in matching the attribute values of the requests and the policies and detecting modality conflict among the applicable policies. Our solution is a filtering step to filter out the irrelevant policies which helps the policy administrators to resolve the modality conflict with these potentially applicable policies during policy evaluation.

1.2 Problem Statement

Due to the dynamism and complexity of collaborative applications, the authoring and implementation of policies are usually a distributed process (Bertino et. al, 2009) because each of the distributed organization would likely be designing their policies autonomously to serve their particular authority principle concern regardless of which parties have already joined the coalition. However, there are a lot of obstacles such as lack of mutual trust and lack of understanding of each other's needs in this collaboration environment. Each site of the distributed organizations has autonomous processing capability by enforcing its own security considerations. Thus, the policy across multiple organizations may be stated using different terms and hence, naming heterogeneity and modality conflict may exist.

An issue to be addressed is naming heterogeneity, which in turn depends on the types of variation that occur between attribute values. Naming heterogeneity arises owing to the use of different combinations of characters to represent the same term (syntactic variations), including for instance typographical errors, or similar terms belonging to different grammar categories, and different terms which have the same meaning (terminological variations) (Castano et al., 2004; Ferrini, 2009). If two parties use the same vocabulary for expressing their respective attribute values, then the process is straight forward. As a first step towards enabling mutual understanding and thus interoperability among parties in a distributed environment, syntactically and terminologically approaches are important to use for aligning their vocabularies. Existing works (Mazzoleni et al., 2008; Rao et al., 2011; Dia & Farkas, 2012; Zhao, 2012; Proctor, 2004; Liu et al., 2011; Ngo et al., 2015) assumed a complete agreement among the parties on the vocabulary used to denote attribute values and to describe the concepts and relationships that characterize a given application domain.

The works by Mazzoleni et al. (2008), Rao et al. (2011), Zhao (2012), and Dia & Farkas (2012) simply adopted simple syntactical analysis to identify policies specifying the same target attribute and their conditions are mutually satisfiable in their policy integration methodology. While some of the works focused on the simple syntactical analysis on the action and condition attributes but more

© COPYRIGHT UPM

complex semantic analysis on the subject and resource attributes (Ioannidis, 2005; Shafiq et al., 2005). However, we cannot expect such policies to be integrated and harmonized beforehand because policies may dynamically change in large dynamic environments. Policies integration methods among various collaborating parties could get very complex due to domain heterogeneity and different vocabulary of each organization provided for their policies.

Several works argued that the collaborative partners may need to perform policy similarity by comparing their access control policies in order to determine which requests will be permitted among the policies and which will not (Lin et al., 2007; Ferrini, 2009; Lin et al., 2013). The policies being compared for similarity may use different vocabularies and, hence, have syntactic or terminological variations of attribute names and categorical values. Nevertheless, the look-up thesaurus used in these works (Lin et al., 2007; Ferrini, 2009; Lin et al., 2013) needs user intervention to specify a domain interest. As a result, the models that utilized external resources such as domain specific thesaurus are not general enough. The look-up thesaurus is usually specified manually based on domain specific knowledge. This is a tedious, time consuming and error-prone process, which is a growing problem given the rapidly increasing number of policies. Furthermore, these works required different collaborative parties to provide their individual and independent policies that may be misused by adversaries to reveal sensitive information among those policies that may lead to unintended breach of privacy.

Due to the difficulty of integrating different schemas from different organizations into a global schema, it is necessary for us to explore the idea of making heterogeneous interoperable without using a global schema (Zisman & Kramer, 1995). A string matching function is the primary function in policy evaluation in identifying the relationships between a request and the policies based on the string elements. Existing policy evaluation engines (Proctor, 2004; Liu et al., 2011; Ngo et al., 2015) utilized a simple string equal matching function for dynamic policy evaluation which fits in the large scale of distributed systems, but they are still limited since they do not explore naming heterogeneity and they assumed that different terms represent different concepts in matching an attribute value of a request to an attribute value of a policy. It would be unrealistic to assume that different organizations from different security domains would share the same vocabulary to represent their policies. More complex matching function which attempts to achieve effectiveness, has been one of the main tasks in policy evaluation. Existing works still lacked solution to automatically resolve naming heterogeneity and it is yet to validate whether the results returned by the evaluation engines are accurate. According to Shvaiko & Euzenat (2005), string-based, language-based techniques and linguistic resources can be used to automatically resolve the naming heterogeneity instead of using look-up thesaurus in order to reduce human involvement.

With the increasing popularity of distributed systems and collaborative applications, there is a need to apply a conflict analysis method in policy

© COPYRIGHT UPM

evaluation. Modality conflict is another issue in policy evaluation which arises because of the existence of both positive and negative authorizations for a given subject-object[1] pair in policy evaluation. Traditional modality conflict is determined by authorizations of opposite effect (indicated by + and -) that is applied to the same subject, object, and action simultaneously (Moffett & Sloman, 1994; Lupu & Sloman, 1997; Damianou et al., 2002; Boutaba & Aib, 2007; Damiani et al., 2006). However, the authorizations could be propagated according to the inheritance relationships between concepts, on the basis of the partially ordered structures obtained by classifying not only subject, resource, and action, but also condition. This is required to ensure consistency in authorization decision as the multiple inheritance paths in the hierarchy may lead to the same requested attribute value (Mohan et al., 2011).

Several studies focused on the design, implementation and evaluation of a mechanism that can be used by policy administrators to proactively detect conflict XACML policies among a set of policies in a policy database (Kamoda et al., 2005; Russello et al., 2007; Adi et al., 2009; Singh & Singh, 2010; Brodecki et al., 2012; Xia, 2012; Hu et al., 2013; Neri et al., 2012; Shaikh et al., 2016; Stepien & Felty, 2016). Nevertheless, these works are mainly focused on the modality conflict detection and resolution among the attribute values of policies once a new party joined the collaboration. The conflict analysis is generally much slower during policy design time especially for an organization which contains policies of larger sizes (Mohan. et al., 2011).

Several works have been devoted to the topic of propagation of authorizations in distributed systems according to the inheritance relationships between concepts which may cause modality conflict (Bertino et a1., 1998; Jajodia et al., 2001; Damiani et al., 2006; Adi et al., 2009; Mohan et al., 2011; Brodecki et al., 2012; Shaikh et al., 2016). Typically in a large distributed system, when a user sends a request to execute an action, if there is no explicit authorization specified for the user, there must be some way to propagate authorizations for the user (Jajodia et al., 2001). In other words, the authorization policies may be propagated according to the inheritance relationships between concepts which may cause inconsistencies.

The concern of these works (Bertino et a1., 1998; Jajodia et al., 2001; Damiani et al., 2006; Mohan et al., 2011; Brodecki et al., 2012; Shaikh et al., 2016) is only on the authorization propagation on the subject, resource, and action attributes, but not on the condition attributes and thus affects the result of authorization decision. These works are limited to simple condition evaluation in which string equal function is used. In addition, none of these works could provide an effective modality conflict detection method which can derive an implicit authorization propagation policy based on subject hierarchy, resource hierarchy, action hierarchy, and location hierarchy. This caused modality conflict could not be detected properly. Adi et al. (2009) argued that sometimes

[1]The terms object and resource are being used interchangeably in this thesis.

© COPYRIGHT UPM

it is required to consider additional temporal as well as spatial constraints on the permission inheritance hierarchy in order to restrict policy permission. The senior role should be able to invoke the permissions of the junior role provided the senior role satisfies the spatio-temporal constraints of the inheritance hierarchy and also the spatio-temporal constraints needed to acquire the permissions of the junior role. In addition, complex condition elements such as semantic relationships between spatial or temporal elements are necessary to take into account in the modality conflict detection process.

In summary, effective matching functions are needed which can resolve naming heterogeneity based on syntactical and terminological variations. Besides that, an authorization propagation rule is needed in order to identify the applicable policies during policy evaluation, which relies on inheritance relationship between the attribute values of a request and a policy which is able to detect the modality conflict among the applicable policies. The authorization propagation rule can assist policy evaluation to investigate the class-subclass relationships between the attribute values of a request and a policy based on the hierarchical structures in which policy attributes (subject, resource, action, and condition) are organized, so that an authorization decision produces by the policy evaluation engine will not lead to unsafe authorization access.

As a conclusion, this thesis addresses the following issues:

- The problem of naming heterogeneity which may exist in matching the attribute values of a request and a policy during policy evaluation due to distributed organizations designed their policies autonomously.
- The problem of identifying the applicable policies and detecting the modality conflict when temporal and spatial constraints are specified in the policies.

1.3 Objectives

The objectives of the research are:

i. To propose matching functions for resolving naming heterogeneity between the attribute values of a request and a policy during policy evaluation. The proposed solution is domain independent as it does not rely on any specific rules of a particular domain and hence a predefined knowledge of the domain is not required.

ii. To propose an authorization propagation rule to identify the applicable policies during policy evaluation. The modality conflict is detected among explicit and implicit applicable policies. The authorization propagation rule relies on the inheritance relationships between concepts, on the basis of the partially ordered structures obtained by classifying subject, resource, action, and condition attributes.

© COPYRIGHT UPM

1.4 Scope of Study

In this research, policies and requests are presented based on the syntax and structure of XACML since it is one of the prominent languages for defining access control policies and the most widely used policy specification language for access control (St-Martin & Felty, 2012).

This thesis attempts to explore the attributes of policy during the matching process in policy evaluation. These elements include subject, resource, action, and condition. XACML has standard functions for various primitive data types. In this thesis, we focus on the issues of naming heterogeneity and modality conflict specifically for the string elements to match the attribute values of a request and a policy during policy evaluation. We contribute solutions to the problems of naming heterogeneity and modality conflict where matching the attribute values of the requests and the policies and detecting modality conflict have been identified as the main phases during policy evaluation when dealing with interoperability and cooperation among distributed database system. The proposed solution is domain independent as it does not rely on any specific rules of a particular domain and hence a predefined knowledge of the domain is not required.

Various types of access control policy have emerged, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attributed-based Access Control (ABAC) which defined what should, and what should not, be allowed, and, in some sense, to different definitions of what ensuring security means (Samarati & di Vimercati, 2001). We focus our work on XACML policy language which is based on DAC model since it is highly flexible and currently most widely used (Joshi, 2015).

Distributed systems are often dynamic, with systems joining and leaving the collaboration at runtime. These collaborations are not fixed a priori, but can dynamically change over time as new parties join, leave, or change their responsibilities and objectives. It is a time consuming process to perform policy matching in policy design stage especially for an organization which contains policies of larger sizes since policy matching needs to be reprocessed once a new party joined the collaboration. Hence, we mainly focus on a process before the actual policy evaluation to assist the policy administrators during policy evaluation. Our solution attempts to filter out the irrelevant policies which helps the policy administrators to resolve modality conflict among these potentially applicable policies. The modality conflict will be reported accordingly so that the policy administrators can resolve them according to their priority to better protect sensitive and private data. Therefore, access control is not the concern of this study.

Entity resolution enables the organizations to enforce data governance and quality policies of collaborative entities across system by performing policy matching. String-based techniques, language-based techniques, and linguistic resources used for entity resolution are suitable to be applied in resolving

© COPYRIGHT UPM

naming heterogeneity automatically in syntactic and semantic level. *N-gram* (string-based) and WordNet (linguistic resource) are adopted in this study to resolve the naming heterogeneity. *N-gram* is effective in matching terms with minor syntactic differences (Giunchiglia & Yatskevich, 2004) based on the following intuition: the more similar the strings, the more likely they denote the same concept. *N-gram* can be used for abbreviation terms by computing the number of common *N*-grams (i.e. sequences of *n* characters) between them. While WordNet is adopted as a linguistic resource for matching an attribute value of a request and a policy because WordNet has been widely applied in the research area of lexical semantics that provides semantic information for lexical terms, especially synonyms, hypernyms, and hyponyms. Thus, WordNet could identify the equivalence and inheritance relationships between the attribute values of a request and a policy.

The modality conflict detection model contains subject, resource, action, location hierarchies that supports a more adequate representation of their semantics. Our work assumes that a semantic relationship (i.e. class-subclass) exists among these concepts. These hierarchies are formed based on the matching results collected from human experts. Each policy that is specified on a superclass is enforced for all of its subclasses.

Four types of rule or policy combining algorithms that are predefined by policy administrators to resolve modality conflict are enforced, namely: "Permit-overrides", "Deny-overrides", "First-applicable", and "Only-one-applicable". For the "First-applicable" policy or policy set, the authorization decision of the first applicable rule or policy is returned. For the "Only-one-applicable" policy or policy set, the authorization decision of the only applicable rule or policy is returned; "Indeterminate" (which indicates an error) is returned if there are more than one applicable rules or policies. For the "Deny-overrides" policy or policy set, "Deny" is returned if any of the rules or policy returned deny; "Permit" is returned if all rules or policies returned permit. For the "Permit-overrides" policy or policy set, "Permit" is returned if any of the rules or policy returned "Permit"; "Deny" is returned if all rules or policies returned "Deny". For all of these combining algorithms, "Not Applicable" is returned if no rule or policy is applicable.

1.5 Thesis Organization

This chapter serves as an essential introduction of this study by presenting the problem statements, objectives, and scope of study. The rest of this thesis is organized as follows:

Chapter 2 provides a brief background on XACML policy language specification. In addition, this chapter presents the concepts related to entity resolution, policy evalu
ation, authorization propagation, and modality conflict detection. The previous works related to this dissertation are reviewed, which include those works that

© COPYRIGHT UPM

focus on access control policy models and related languages. We reviewed the policy evaluation methods and authorization propagation that were proposed by previous studies for detecting modality conflict. The limitations of each work are then identified.

Chapter 3 is dedicated to the description of the methodology applied in this thesis. It describes how this research is conducted to improve the accuracy in matching an attribute value of a request and a policy, as well as in retrieving the applicable policies and in detecting modality conflict. The discussion on the measurements used to evaluate the performance of the proposed solution is also given.

Chapter 4 presents in details our proposed matching functions which are not limited to string equal function that aim to resolve naming heterogeneity, namely: synonym equal, hyponym, syntactical-synonym equal, syntactical-hyponym, syntactical equal, hyponym common word, and abbreviation equal. An illustrative example based on the academy university domain is given to present our proposed matching functions in resolving naming heterogeneity.

Chapter 5 presents in details the proposed authorization propagation rule to identify the applicable policies during policy evaluation. The modality conflict is detected among explicit and implicit applicable policies. An illustrative example is presented based on the academy university domain in order to illustrate how modality conflict exists among access control policies when authorizations are being propagated.

Chapter 6 presents the evaluation of the proposed solution. This chapter evaluates the performance of the proposed matching functions and the authorization propagation rule and compared the results with the previous work.

Chapter 7 concludes the current study and sheds light on some directions which can be followed in the future.

© COPYRIGHT UPM

REFERENCES

[1] Adi, K., Bouzida, Y., Hattak, I., Logrippo, L., & Mankovskii, S. (2009). Typing for Conflict Detection in Access Control Policies. *Proceedings of the 4th International Conference on E-Technologies* (*MCETECH*), pp. 212-226.

[2] Agrawal, D., Giles, J., Lee, K. W., & Lobo, J. (2005). Policy Ratification. *Proceedings of the 6th IEEE International Workshop on Policies for Distributed Systems and Networks* (*POLICY*), pp. 223-232.

[3] Agreste, S., De Meo, P., Ferrara, E., & Ursino, D. (2014). XML Matchers: Approaches and Challenges. *Knowledge-Based Systems*, 66: 190-209.

[4] Algergawy, A., Nayak, R., & Saake, G. (2010). Element Similarity Measures in XML Schema Matching. *Information Sciences*, 180(24): 4975-4998.

[5] Almutairi, A., Sarfraz, M., Basalamah, S., Aref, W., & Ghafoor, A. (2012). A Distributed Access Control Architecture for Cloud Computing. *IEEE software*, 29(2): 36-44.

[6] Anderson, A. (2005). A Comparison of Two Privacy Policy Languages: EPAL and XACML. *Proceedings of the 3rd ACM Workshop on Secure Web Services* (*SWS*), pp. 53-60.

[7] Ardagna, C. A., Cremonini, M., Damiani, E., di Vimercati, S. D. C., & Samarati, P. (2006). Supporting Location-based Conditions in Access Control Policies. *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, pp. 212-222.

[8] Ardagna, C. A., Damiani, E., di Vimercati, S. D. C., & Samarati, P. (2004). XML-based Access Control Languages. *Journal Information Security Tech. Report*, 9(3): 35-46.

[9] Becker, M. Y., & Sewell, P. (2004). Cassandra: Distributed Access Control Policies with Tunable Expressiveness. *Proceedings of the 5th IEEE International Workshop on Policies for Distributed Systems and Networks* (*POLICY*), pp. 159-168.

[10] Benantar, M. (2006). *Access Control Systems: Security, Identity Management and Trust Models*. Springer-Verlag US. ISBN-13: 978-0-387-00445-7.

[11] Bertino, E., Brodie, C., Calo, S. B., Cranor, L. F., Karat, C., Karat, J., Li, N., Lin, D., Lobo, J., Ni, Q., & Rao, P. R. (2009). Analysis of Privacy and Security Policies. *IBM Journal of Research and Development*, 5(2): 3:1-3:18.

[12] Bertino, E., Buccafurri, F., Ferrari, E., & Rullo, P. (1998). An Authorization Model and Its Formal Semantics. *Proceedings of the 5th European Symposium on Research in Computer Security* (*ESORICS*), pp. 127-142.

[13] Bertino, E., Ghinita, G., & Kamra, A. (2011). Access Control for Databases: Concepts and Systems. *Foundations and Trends in Databases*, 3(1-2): 1-148.

[14] Bertino, E., & Sandhu, R. (2005). Database Security-concepts, Approaches, and Challenges. *IEEE Transactions on Dependable and Secure Computing*, 2(1): 2-19.

© COPYRIGHT UPM

[15] Bertolino, A., Le, T. Y., Lonetti, F., Marchetti, E., & Mouelhi, T. (2014). Validation of Access Control Systems. *Engineering Secure Future Internet Services and Systems, LNCS* (8431), pp. 210-233.

[16] Bilke, A., & Naumann, F. (2005). Schema Matching using Duplicates. *Proceedings of the 21st International Conference on Data Engineering* (*ICDE*), pp. 69-80.

[17] Blair, G. S., Paolucci, M., Grace, P., & Georgantas, N. (2011). Interoperability in complex distributed systems. *Formal Methods for Eternal Networked Software System*, *LNCS* (6659), pp. 1-26.

[18] Bokefode Jayant, D., Ubale Swapnaja, A., Modani Dattatray, G., & Apte Sulabha, S. (2014). Analysis of DAC MAC RBAC Access Control based Models for Security. *International Journal of Computer Applications*, 104(5): 6-13.

[19] Boutaba, R., & Aib, I. (2007). Policy Based Management: A Historical Perspective. *Journal of Network and Systems Management*, 15(4): 447-480.

[20] Brodecki, B., Szychowiak, M., & Sasak, P. (2012). Security Policy Conflicts in Service Oriented Systems. *New Generation Computing*, 30(2-3): 215-240.

[21] Butler, B., 2016. *Access Control System Specification and its Implications for Performance*, PhD thesis, Waterford Institute of Technology, Ireland.

[22] Carminatp, B., Ferrari, E., & Thuraisingham, B. (2006). Access Control for Web Data: Models and Policy Languages. *Annales Des Télécommunications*, 61(3-4): 245-2.

[23] Castano, S., Ferrara, A., Montanelli, S., & Racca, G. (2004). Semantic information interoperability in open networked systems. *Proceedings of the International Conference on Semantics of a Networked World* (*LCSNW*), *in cooperation with ACM SIGMOD*, pp. 215-230.

[24] Cavoukian, A., Chibba, M., Williamson, G., & Ferguson, A. (2015). The importance of ABAC (attribute based access control) to big data: Privacy and context. *Privacy and Big Data Institute*, *Ryerson University*, *Toronto*, *Canada*. URL: http://www.ryerson.ca/content/dam/pbdi/Resources/The%20Importance%20of%20ABAC%20to%20Big%20Data%2005-2015.pdf

[25] Chaudhuri, S., Ganti, V., & Xin, D. (2009). Mining Document Collections to Facilitate Accurate Approximate Entity Matching. *Proceedings of the Very Large Data Bases* (*VLDB Endowment*), pp. 395-406.

[26] Ciuciu, I., Zhao, G., Chadwick, D. W., Reul, Q., Meersman, R., Vasquez, C., Hibbert, M., Winfield, S., & Kirkham, T. (2011). Ontology Based Interoperation for Securely Shared Services: Security Concept Matching for Authorization Policy Interoperability. *Proceedings of the 4th IFIP International Conference on New Technologies*, *Mobility and Security* (*NTMS*), pp. 1-5.

[27] Cohen, W., Ravikumar, P., & Fienberg, S. (2003). A Comparison of String Distance Metrics for Name-Matching Tasks. *Proceedings Workshop Information Integration Web* (*IIWeb*) pp. 73-78.

© COPYRIGHT UPM

[28] Crampton, J., & Sellwood, J. (2015). Relationships, Paths and Principal Matching: A New Approach to Access Control. *ArXiv Preprint arXiv:1505.07945*, 61: 245-266.
[29] Damiani, E., di Vimercati, S. D. C., Fugazza, C., & Samarati, P. (2006). Modality Conflicts in Semantics Aware Access Control. *Proceedings of the 6th International Conference on Web Engineering* (*ICWE*), pp. 249-256.
[30] Damianou, N., Bandara, A., Sloman, M., & Lupu, E. (2002). A Survey of Policy Specification Approaches. *Technical Report, Department of Computing, Imperial College of Science Technology and Medicine, London*.
[31] Dasgupta, S., & Bagchi, A. (2012). A Graph-based Formalism for Controlling Access to a Digital Library Ontology. *Proceedings of the 11th IFIP TC 8 International Conference on Computer Information Systems and Industrial Management* (*CISIM*), pp. 111-122.
[32] di Vimercati, S. D. C., Samarati, P., & Jajodia, S. (2005). Policies, Models, and Languages for Access Control. *Proceedings of the 4th International Conference on Databases in Networked Information Systems* (*DNIS*), pp. 225-237.
[33] di Vimercati, S. D. C., Foresti, S., Jajodia, S., & Samarati, P. (2007). Access Control Policies and Languages in Open Environments. *Secure Data Management in Decentralized Systems*, pp. 21-58.
[34] Dia, O. A., & Farkas, C. (2012). A Practical Framework for Policy Composition and Conflict Resolution. *International Journal of Secure Software Engineering* (*IJSSE*), 3(4): 1-26.
[35] Do, H. H., Melnik, S., & Rahm, E. (2003). Comparison of Schema Matching Evaluations. *Web*, *Web-Services*, *and Database Systems*, *LNCS* (2593), pp. 221-237.
[36] Do, H. H. & Rahm, E. (2007). Matching Large Schemas: Approaches and Evaluation. *Information Systems*, 32(6): 857-885.
[37] Dong, C., Russello, G., & Dulay, N. (2008). Flexible Resolution of Authorisation Conflicts in Distributed Systems. *Proceedings of the 19th International Workshop on Distributed Systems: Operations and Management* (*DSOM*), pp. 95-108.
[38] Dong, X., Halevy, A., & Madhavan, J. (2005). Reference Reconciliation in Complex Information Spaces. *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pp. 85-96.
[39] Duchateau, F., Bellahsene, Z., Roantree, M., & Roche, M. (2007). An Indexing Structure for Automatic Schema Matching. *International Workshop on Self-Managing Database Systems* (SMDB-ICDE), pp. 485–491.

[40] Dupont, Y. (1994). Resolving Fragmentation Conflicts in Schema Integration. *Proceedings of the 13th International Conference on the Entity-Relationship Approach Business Modeling and Re-engineerin*g, *P. Loucopoulos*, *Ed.*, pp. 513-532.
[41] Fatema, K., & Chadwick, D. (2014). Resolving Policy Conflicts-Integrating Policies from Multiple Authors. *Proceedings of the International Conference on Advanced Information Systems Engineering* (*CAiSE*), pp. 310-321.

© COPYRIGHT UPM

[42] Ferrini, R. (2009). *EXAMS: An Analysis Tool for Multidomain Policy Sets*, PhD Thesis, University of Bologna, Italy.

[43] Ferrini, R., & Bertino, E. (2009). Supporting RBAC with XACML+OWL. *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies* (*SACMAT*), pp. 145-154.

[44] Geraci, A., Katki, F., McMonegal, L., Meyer, B., Lane, J., Wilson, P., Radatz, J., Yee, M., Porteous, H., & Springsteel, F. (1991). IEEE Standard Computer Dictionary: Compilation of IEEE Standard Computer Glossaries. *IEEE Press, Piscataway, NJ, USA*.

[45] Giunchiglia, F., & Yatskevich, M. (2004). Element Level Semantic Matching. *Proceedings of Meaning Coordination and Negotiation Workshop at the International Semantic Web Conference* (*ISWC*).

[46] Giunchiglia, F., Yatskevich, M., & Shvaiko, P. (2007). Semantic Matching: Algorithms and Implementation. *Journal on data semantics*, IX: 1-38.

[47] Gómez-Pérez, A., Ramos, J. A., Rodríguez-Pascual, A., & Vilches-Blázquez, L. M. (2008). The IGN-E case: Integrating Through a Hidden Ontology. *The 13th International Symposium on Spatial Data Handling* (*SDH*), pp. 417-435.

[48] Gonzalez, T., DiazHerrera, J., & Tucker, A. (2014). *Computing handbook: Computer science and software engineering, 3rd edition*. Chapman and Hall/CRC. ISBN: 9781439898529.

[49] Guha, S., Koudas, N., Marathe, A., & Srivastava, D. (2004). Merging the Results of Approximate Match Operations. *Proceedings of the 13th International Conference on Very Large Data Bases* (*VLDB Endowment*), pp. 636-647.

[50] Guo, Y., Pan, Z., & Heflin, J. (2004). An Evaluation of Knowledge Base Systems for Large OWL Datasets. *Proceedings of the 3rd International Semantic Web Conference* (*ISWC*), pp. 274-288.

[51] Hoffer, J. A., & McFadden, F. R. (2010). *Modern database management*, 10th edition. Prentice Hall, Upper Saddle River, NJ. ISBN: 0-13-608839-2.

[52] Hu, H., Ahn, G., & Kulkarni, K. (2013). Discovery and Resolution of Anomalies in Web Access Control Policies. *IEEE Transactions on Dependable and Secure Computing*, 10(6): 341-354.

[53] Hu, L., Ying, S., Jia, X., & Zhao, K. (2009). Towards an Approach of Semantic Access Control for Cloud Computing. *Proceedings of the* 1st *IEEE International Conference on Cloud Computing*, pp. 145-156.

[54] Husain, M. F., AlKhateeb, T., Alam, M., & Khan, L. (2011). Ontology Based Policy Interoperability in Geospatial Domain. *Computer Standards & Interfaces*, 33(3): 214-219.

[55] Ioannidis, S. (2005). *Security Policy Consistency and Distributed Evaluation in Heterogeneous Environments*, PhD Thesis, University of Pennsylvania, Philadelphia.

[56] Jajodia, S., Samarati, P., Sapino, M. L., & Subrahmanian, V. (2001). Flexible Support for Multiple Access Control Policies. *ACM Transactions on Database Systems* (*TODS*), 26(2): 214-260.

[57] Jin, X., Krishnan, R., & Sandhu, R. (2012). A Unified Attribute-based Access Control Model Covering DAC, MAC and RBAC. *Proceedings of the 26th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy* (*DBSec*), pp. 41-55.

© COPYRIGHT UPM

[58] Joshi, J. B. (2004). Access-control Language for Multidomain Environments. *IEEE Internet Computing*, 8(6): 40-50.

[59] Joshi, J. (2015). Overview of Access Control Models. IS 3350 Doctoral Seminar (Systems and Technology) *Focus*: Security and Privacy Assured Health Informatics.
http://sis.pitt.edu/jjoshi/courses/DocSem/Fall2015/OverviewAC.pdf

[60] Kamoda, H., Yamaoka, M., Matsuda, S., Broda, K., & Sloman, M. (2005). Policy Conflict Analysis using Free Variable Tableaux for Access Control in Web Services Environments. *Proceedings of the Policy Management for the Web Workshop at the 14th International World Wide Web Conference* (*WWW*), pp. 121-126.

[61] Kudo, M., & Hada, S. (2000). XML Document Security Based on Provisional Authorization. *Proceedings of the 7th ACM Conference on Computer and Communications Security* (*CCS*), pp. 87-96.

[62] Liang, F., Guo, H., Yi, S., & Ma, S. (2012). A Multiple Policy Supported Attribute Based Access Control Architecture within Large Scale Device Collaboration Systems. *Journal of Networks*, 7(3): 524-531.

[63] Lin, D., Rao, P., Bertino, E., & Lobo, J. (2007). An Approach to evaluate policy similarity. *Proceedings of the 12th ACM symposium on Access control models and technologies* (*SACMAT*), pp. 1-10.

[64] Lin, D., Rao, P., Ferrini, R., Bertino, E., & Lobo, J. (2013). A Similarity Measure for Comparing XACML Policies. *IEEE Transactions on Knowledge and Data Engineering*, 25(9): 1946-1959.

[65] Liu, A. X., Chen, F., Hwang, J., & Xie, T. (2011). Designing Dast and Scalable XACML Policy Evaluation Engines. *IEEE Transactions on Computers*, 60(12): 1802-1817.

[66] Liu, L., Zhang, S., Diao, L., & Cao, C. (2010). An Iterative Method of Extracting Chinese ISA Relations for Ontology Learning. *Journal of Computers*, 5(6): 870-877.

[67] Lorch, M., Proctor, S., Lepro, R., Kafura, D., & Shah, S. (2003). First Experiences using XACML for Access Control in Distributed Systems. *Proceedings of the 2003 ACM workshop on XML security* (*XMLSEC*), pp. 25-37.

[68] Lupu, E., & Sloman, M. (1997). Conflict Analysis for Management Policies. *Proceedings of the 5th IFIP/IEEE International Symposium on Integrated Network Management*, pp. 430-443.

[69] Machulak, M. P., Parkin, S. E., & van Moorsel, A. (2009). Architecting Dependable Access Control Systems for Multidomain Computing Environments. *Architecting Dependable Systems VI*, *LNCS* (5835), pp. 49-75.

[70] Marie, A., & Gal, A. (2008). Boosting schema matchers. *Proceedings of the 2008 Confederated International Conferences On the Move to Meaningful Internet Systems* (*OTM*), pp. 283-300.

[71] Martin, E., Xie, T., & Yu, T. (2006). Defining and Measuring Policy Coverage in Testing Access Control Policies. *Proceedings of the 8th International Conference on Information and Communications Security* (*ICICS*), pp. 139-158.

[72] Mazzoleni, P., Crispo, B., Sivasubramanian, S., & Bertino, E. (2008). XACML Policy Integration Algorithms. *ACM Transactions on Information and System Security* (*TISSEC*), 11(1): 1-29.

© COPYRIGHT UPM

[73] Melnik, S., Garcia-Molina, H., & Rahm, E. (2002). Similarity Flooding: A Versatile Graph Matching Algorithm and its Application to Schema Matching. *Proceedings of the 18th International Conference on Data Engineering* (*ICDE*), pp. 117-128.
[74] Miller, G. A. (1995). WordNet: A Lexical Database for English. *Communications of the ACM*, 38(11): 39-41.
[75] Moffett, J. D., & Sloman, M. S. (1994). Policy Conflict Analysis in Distributed System Management. *Journal of Organizational Computing and Electronic Commerce*, 4(1): 1-22.
[76] Mohan, A., & Blough, D. M. (2010). An Attribute-based Authorization Policy Framework with Dynamic Conflict Resolution. *Proceedings of the 9th Symposium on Identity and Trust on the Internet* (*IDTRUST*), pp. 37-50.
[77] Mohan, A., Blough, D. M., Kurc, T., Post, A., & Saltz, J. (2011). Detection of Conflicts and Inconsistencies in Taxonomy Based Authorization Policies. *Proceedings of the 2011 IEEE International Conference on Bioinformatics and Biomedicine* (*BIBM*), pp. 590-594.
[78] Naumann, F. (2013). Similarity Measures. *IT Systems Engineering*, *Hasso Plattner Institut*, *University of Potsdam*, *Germany*.URL: https://hpi.de/fileadmin/user_upload/fachgebiete/naumann/folien/SS13/DPDC/DPDC_12_Similarity.pdf
[79] Neri, M. A., Guarnieri, M., Magri, E., Mutti, S., & Paraboschi, S. (2012). Conflict Detection in Security Policies using Semantic Web Technology. *Proceedings of the 1st AESS European Conference on Satellite Telecommunications* (*ESTEL*), pp. 1-6.
[80] Ngo, C., Demchenko, Y., & Laat, C. D. (2015). Decision Diagrams for XACML Policy Evaluation and Management. *Journal of Computers and Security*, 49: 1-16.
[81] Pérez, J. M. M., Bernabé, J. B., Calero, J. M. A., Clemente, F. J. G., Pérez, G. M., & Skarmeta, A. F. G. (2011). Semantic-based authorization architecture for grid. *Journal Future Generation Computer Systems*, 27(1): 40-55.
[82] Priebe, T., Dobmeier, W., Schläger, C., & Kamprath, N. (2007). Supporting Attribute Based Access Control in Authorization and Authentication Infrastructures with Otologies. *Journal of Software*, 2(1): 27-38.
[83] Proctor, S. (2004). Sun's XACML implementation. URL: *http://sunxacml.sourceforge.net/.*
[84] Rahm, E., & Bernstein, P. A. (2001). A Survey of Approaches to Automatic Schema Matching. *The International Journal on Very Large DataBases*, 10(4): 334-350.
[85] Rahm, E. & Do, H. H. (2000). Data Cleaning: Problems and Current Approaches. *IEEE Data Engineering Bulletin*, *23*(4): 3-13.
[86] Rao, P., Lin, D., Bertino, E., Li, N., & Lobo, J. (2011). Fine-grained integration of access control policies. *Journal Computers & Security*, 30(2): 91-107.
[87] Ravari, A. N., Amini, M., & Jalili, R. (2008). A semantic aware access control model with real time constraints on history of accesses. *Proceedings of the International Multiconference on Computer Science and Information Technology* (*IMCSIT*), pp. 827-836.

© COPYRIGHT UPM

[88] Reul, Q., & Zhao, G. (2010). Enabling Access to Web Resources through SecPODE-based Annotations. *Proceedings of the 2010 Confederated International Conferences On the Move to Meaningful Internet Systems* (*OTM*), pp. 596-605.

[89] Reul, Q., Zhao, G., & Meersman, R. (2010). Ontology-based Access Control Policy Interoperability. *Proceeding of the 1st Conference on Mobility, Individualisation, Socialisation and Connectivity* (*MISC*).

[90] Røstad, L. (2008). *Access Control in Healthcare Information Systems*, PhD Thesis, Norwegian University of Science and Technology, Norway.

[91] Russello, G., Dong, C., & Dulay, N. (2007). Authorisation and conflict resolution for hierarchical domains. *Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks* (*POLICY*), pp. 201-210.

[92] Ryutov, T., & Neuman, C. (2000). Representation and Evaluation of Security Policies for Distributed System Services. *Proceedings of the 2000 DARPA Information Survivability Conference and Exposition* (*DISCEX*), pp. 172-183.

[93] Sabou, M., Lopez, V., & Motta, E. (2006). Ontology Selection for the Real Semantic Web: How to Cover the Queen's Birthday Dinner?. *Proceedings of the 15th International Conference on Managing Knowledge in a World of Networks* (*EKAW'06*), pp. 96-111.

[94] Saleem, K., Bellahsene, Z., & Hunt, E. (2008). Porsche: Performance Oriented Schema Mediation. *Information Systems*, 33(7): 637-657.

[95] Samarati, P. & di Vimercati, S. D. C. (2001). Access control: Policies, models, and mechanisms. *International School on Foundations of Security Analysis and Design*, *LNCS* (2171), pp. 137-196.

[96] Sandhu, R. S., Coynek, E. J., Feinsteink, H. L., & Youmank, C. E. (1996). Role Based Access Control Models. *IEEE Computer*, 29(2): 38-47.

[97] Sarawagi, S. & Kirpal, A. (2004). Efficient Set Joins on Similarity Predicates. *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pp. 743-754.

[98] Shafiq, B., Joshi, J. B., Bertino, E., & Ghafoor, A. (2005). Secure Interoperation in a Multidomain Environment Employing RBAC Policies. *IEEE Transactions on Knowledge and Data Engineering*, 17(11): 1557-1577.

[99] Shaikh, R. A., Adi, K., Logrippo, L., & Mankovski, S. (2010). Inconsistency Detection Method for access control policies. *Proceedings of the 6th International Conference on Information Assurance and Security* (*IAS*), pp. 204-209.

[100] Shaikh, R. A., Adi, K., & Logrippo, L. (2016). A Data Classification Method for Inconsistency and Incompleteness Detection in Access Control Policy Sets. *International Journal of Information Security*, 1-23.

[101] Shvaiko, P., & Euzenat, J. (2005). A survey of schema-based matching approaches. *Journal on data semantics IV*, 146-171.

[102] Singh, K., & Singh, S. (2010). Design and Evaluation of XACML Conflict Policies Detection Mechanism. *International Journal of Computer Science and Information Technology*, 2: 65-74.

[103] St-Martin, M. & Felty, A. P. (2012). *A Verified Algorithm for Detecting Conflicts in XACML Access Control Rules*, Master Thesis, University of Ottawa, Canada.

[104] Stepien, B., & Felty, A. (2016). Using Expert Systems to Statically Detect “Dynamic” conflicts in XACML. *Proceedings of the 11th International Conference on Availability, Reliability and Security* (*ARES*).

[105] Stoller, S. D., Yang, P., Ramakrishnan, C. R., & Gofman, M. I. (2007). Efficient Policy Analysis for Administrative Role Based Access Control. *Proceedings of the 14th ACM Conference on Computer and Communications Security* (*CCS*), pp. 445-455.

[106] Szymczak, M., Zadrożny, S., Bronselaer, A., & De Tré, G. (2015). Coreference Detection in an XML Schema. *An Internatioal Journal Information Sciences*, 296, pp. 237-262.

[107] Tahat, S., & Ahmad, K. (2013). Semi-automated Schema Integration (Icase): A Tool to Identify and Resolve Naming Conflicts. *Australian Journal of Basic & Applied Sciences*, 7(7), pp 515-519.

[108] Takabi, H. (2013). *A semantic based policy management framework for cloud computing environments*, PhD Thesis, University of Pittsburgh, USA.

[109] Tekli, J., Chbeir, R., & Yetongnon, K. (2009). Extensible User-Based XML Grammar Matching. *Proceedings of International Conference on Conceptual Modeling* (*ER*), pp. 294-314.

[110] Tejada, S., Knoblock, C. A., & Minton, S. (2001). Learning object identification rules for information integration. *Information Systems*, 26(8): 607-633.

[111] Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected cloud computing environments: Challenges, taxonomy, and survey. *Journal ACM Computing Surveys* (*CSUR*), 47(1): 1–47.

[112] Trivellato, D., Spiessens, F., Zannone, N., & Etalle, S. (2009). POLIPO: Policies & ontologies for interoperability, portability, and autonomy. *Proceedings of the 10th IEEE International Conference on Policies for Distributed Systems and Networks* (*POLICY*), pp. 110-113.

[113] Trivellato, D., Zannone, N., Glaundrup, M., Skowronek, J., & Etalle, S. (2013). A Semantic Security Framework for Systems of Systems. *International Journal of Cooperative Information Systems*, 22(1): 1-35.

[114] Turkmen, F., den Hartog, J., Ranise, S., & Zannone, N. (2015). Analysis of XACML Policies with SMT. *Proceedings of the 4th International Conference on Principles of Security and Trust* (*POST*), pp. 115-134.

[115] Weber, H. A. (2003). Role based access control: The NIST solution. *SANS Institute InfoSec Reading Room.* URL:https://www.sans.org/reading-room/whitepapers/sysadmin/role-based-access-control-nist-solution-1270

[116] Xia, X. (2012). A Conflict Detection Approach for XACML Policies on Hierarchical Resources. *Proceedings of the 2012 IEEE International Conference on Green Computing and Communications* (*GREENCOM*), pp. 755-760.

[117] Zannone, N., Jajodia, S., & Wijesekera, D. (2006). Creating Objects in the Flexible Authorization Framework. *Proceedings of the 20th IFIP*

© COPYRIGHT UPM

WG 11.3 Working Conference on Data and Applications Security (*DBSEC*), pp. 1-14.

[118] Zhao, H. (2012). *Security Policy Definition and Enforcement in Distributed Systems*, PhD Thesis, Columbia University, USA.

[119] Zisman, A., & Kramer, J. (1995). Towards Interoperability in Heterogeneous Database systems. *Technical Report 11, Department of Computing, Imperial College of Science, Technology and Medicine*.

© COPYRIGHT UPM

BIODATA OF STUDENT

Teo Poh Kuang was born in Johor, Malaysia, May 1985. She obtained her Bachelor Degree in Computer Science with the Major Computer System in 2008, from the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). She was a demonstrator in the Faculty of Computer Science and Information Technology, UPM from 2007 to 2014. In 2008 she joined the Faculty of Computer Science and Information Technology, Department of Computer Science, University Putra Malaysia (UPM) to pursue her PhD in a field of Database Systems under supervision of Professor Dr. Hamidah Ibrahim. She is received her graduate research fellowship from 2009 till 2011 during her Phd and assisted to guide final year undergraduate student's copyright and final year projects. During her PhD study, she investigated a research on XACML policy interoperability in distributed environment.

© COPYRIGHT UPM

LIST OF PUBLICATIONS

ORIGINAL CONTRIBUTION TO KNOWLEDGE

Teo Poh Kuang and Hamidah Ibrahim. (2009): Security privacy access control for policy integration and conflict reconciliation in health care organizations collaborations. *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services* (*iiWAS*), pp. 750-754.

Teo Poh Kuang, Hamidah Ibrahim, Fatimah Sidi, and Nur Izura Udzir. (2011). Heterogeneity XACML Policy Evaluation Engine. *Proceedings of the Second International Conference on Digital Enterprise and Information Systems* (*DEIS*), pp. 230-238.

Teo Poh Kuang, Hamidah Ibrahim, Fatimah Sidi, and Nur Izura Udzir. (2011). Policy Inconsistencies Detection Based on RBAC Model in Cross-Organization Collaboration. *Proceedings of the 3rd International Conference on Computing and Informatics* (*ICOCI*), pp. 333-338.

Teo Poh Kuang, Hamidah Ibrahim, Fatimah Sidi, and Nur Izura Udzir. Security Extensible Access Control Markup Language Policy Integration Based on Role-Based Access Control Model in Healthcare Collaborative Environments. (2011). *American Journal of Economics and Business Administrations*, 3(1): 101-111.

Teo Poh Kuang, Hamidah Ibrahim, Fatimah Sidi, and Nur Izura Udzir. (2014). Heterogeneity XACML policy evaluation engine. *Malaysian National Conference of Databases* (*MaNCoD*), pp. 230-238. [Best Paper Awarded]

Teo Poh Kuang, Hamidah Ibrahim, Fatimah Sidi, and Nur Izura Udzir. (2014). XACML Policy Evaluation Inconsistency Analysis and Resolution. *Proceedings of the 3th International Conference on Data Management Technologies And Applications* (*DATA*), pp. 133-138.

Teo Poh Kuang, Hamidah Ibrahim, Fatimah Sidi, and Nur Izura Udzir. An Effective Modality Conflict Model for Identifying Applicable Policies during Policy Evaluation. (2018). *Journal of Advances in Computer Engineering and Technology*, 4(4): 255-266.

© COPYRIGHT UPM

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION : ____________________

TITLE OF THESIS / PROJECT REPORT :

HETEROGENEITY POLICY EVALUATION WITH MODALITY CONFLICT ANALYSIS

NAME OF STUDENT : TEO POH KUANG

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as :

*Please tick (√)

☐	**CONFIDENTIAL**	(Contain confidential information under Official Secret Act 1972).
☐	**RESTRICTED**	(Contains restricted information as specified by the organization/institution where research was done).
☐	**OPEN ACCESS**	I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for :

☐	**PATENT**	Embargo from ____________ (date) until ____________ (date)

Approved by:

____
(Signature of Student)
New IC No/ Passport No.:

Date :

____
(Signature of Chairman of Supervisory Committee)
Name:

Date :

[Note : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]