ACCESS CONTROL MODEL BASED ON TRUST, PURPOSE, AND ROLE IN MATERIALIZED VIEW FOR PRIVACY PROTECTION

MOHD RAFIZ BIN SALJI

FSKTM 2019 47

ACCESS CONTROL MODEL BASED ON TRUST, PURPOSE, AND ROLE IN MATERIALIZED VIEW FOR PRIVACY PROTECTION

By

MOHD RAFIZ BIN SALJI

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

May 2019

DEDICATIONS

This thesis is dedicated to my lovely wife, daughter, families, and friends for their endless support, encouragement and patience.

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

ACCESS CONTROL MODEL BASED ON TRUST, PURPOSE, AND ROLE IN MATERIALIZED VIEW FOR PRIVACY PROTECTION

By

MOHD RAFIZ BIN SALJI

May 2019

Chair: Nur Izura Binti Udzir, Ph.D.

Faculty of Computer Science and Information Technology

Data privacy is one of the fundamental needs of the people. In a computing environment, there are various issues of data privacy protection in the enterprise. To enforce automation of privacy and legal policies, access control has become a common subject that are always been applied. Despite the recent advances in access control models, there are still issues that impede the development of effective access control. Among them is the lack of assessments for the user to authorize access, which comprises reliance on identity, purpose, and role.

This study focuses on data privacy protection in materialized view. Materialized view is a replica of a table which is created in a very large system where data are replicated from the master tables. Role-based access control model in materialized view has been proposed to protect customer's data. However, relying on role only is insufficient and inefficient to protect data especially sensitive attributes. This may lead to the risk of privacy disclosure to unauthorized and untrusted users.

Previous access control models based on purpose and trust also do not consider protecting sensitive attributes.

Quantification methods have been proposed to quantify certain user properties to specify user's trustworthiness. However, these quantification methods have limitation as they provide a general formula of calculation to quantify certain user properties to specify user's trustworthiness. Therefore, a new quantification method needs to be proposed which provides specific calculation of the user properties to specify user's trustworthiness. A quantification method is proposed to quantify the seniority and behaviour of the user by using the evidences and ten user behaviour categories to specify user's trustworthiness. The method is developed and tested to calculate both properties, and the result shows that the proposed method provides detail calculation of both properties to specify user's trustworthiness. The proposed method is validated by comparing the calculation of the user properties to specify user's trustworthiness with previous studies, and the result shows that the proposed method is stricter in specifying user's trustworthiness. Therefore, this work offers a solution by providing a quantification method with specific calculation of the seniority and behaviour to specify user's trustworthiness.

A trust, purpose, and role-based access control model in materialized view is proposed to efficiently protect data especially sensitive attributes. In the proposed model, purpose and role are applied to permit access to data, while trust is applied to control access to sensitive attributes. An algorithm is discussed to describe the access control mechanism by first, authenticating user's role, purpose, and trust, before authorizing access of authorized and trusted user. A prototype system is developed and tested, and the result shows that sensitive attributes are protected. The experiment is conducted to validate the proposed model by comparing it with the previous model. The result shows that the proposed model is efficient and improve privacy protection. Therefore, this research solves the issue of protection data especially sensitive attributes in materialized view.

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

MODEL KAWALAN AKSES BERASASKAN KEPERCAYAAN, TUJUAN, DAN PERANAN UNTUK MELINDUNGI PRIVASI DI PANDANGAN JELMAAN

Oleh

MOHD RAFIZ BIN SALJI

Mei 2019

Pengerusi: Nur Izura Binti Udzir, Ph.D.

Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat

Privasi data adalah salah satu keperluan manusia. Dalam persekitaran pengkomputeran, terdapat pelbagai isu perlindungan privasi data di dalam enterpris. Untuk menguatkuasakan dasar privasi dan undang-undang secara automasi, kawalan akses adalah salah satu subjek yang diberi keutamaan. Walaupun terdapat pelbagai kemajuan terkini dalam model-model kawalan capaian, tetapi masih terdapat isu yang menghalang pembangunan kawalan capaian yang berkesan. Antaranya adalah kekurangan beberapa penilaian untuk pengguna bagi membenarkan akses, yang terdiri daripada kebergantungan terhadap identiti, tujuan, dan peranan.

Penyelidikan ini memfokuskan kepada perlindungan privasi data di pandangan jelmaan. Pandangan jelmaaan adalah salinan jadual yang dicipta dalam sistem yang besar di mana data disalin dari jadual induk. Kawalan capaian berasaskan peranan telah diperkenalkan di pandangan jelmaan bagi melindungi data pelanggan. Walaubagaimanapun, penggunaan peranan sahaja adalah tidak mencukupi dan tidak cekap untuk melindungi data terutama atribut sensitif. Ini boleh menyebabkan risiko pendedahan privasi kepada pengguna yang tidak dibenarkan dan tidak dipercayai. Model kawalan capaian terdahulu berasaskan tujuan dan kepercayaan juga tidak mempertimbangkan untuk melindungi atribut sensitif.

Kaedah pengkuantitian diperkenalkan untuk mengira beberapa sifat pengguna untuk menentukan kebolehpercayaan pengguna. Walau bagaimanapun, kaedah pengkuantitian mempunyai kelemahan di mana ia memperkenalkan formula pengiraan secara umum bagi mengira beberapa sifat pengguna untuk menentukan kebolehpercayaan pengguna. Oleh yang demikian, kaedah pengkuantitian baharu perlu dicadangkan dengan dilengkapi pengiraan secara khusus beberapa sifat pengguna bagi menentukan kebolehpercayaan pengguna. Kaedah pengkuantitian diperkenalkan bagi mengira kekananan dan tingkahlaku pengguna dengan menggunakan bukti dan sepuluh kategori tingkahlaku pengguna untuk menentukan kebolehpercayaan pengguna. Kaedah tersebut dibangunkan dan diuji untuk mengira kedua-dua sifat tersebut, dan keputusannya menunjukkan kaedah yang dicadangkan memberikan pengiraan terperinci kedua-dua sifat tersebut untuk menentukan kepercayaan pengguna. Kaedah yang dicadangkan disahkan dengan membandingkan pengiraan sifat pengguna untuk menentukan kebolehpercayaan pengguna dengan kerja terdahulu, dan hasil dapatan menunjukkan kerja yang dicadangkan adalah lebih ketat dalam menentukan kebolehpercayaan pengguna. Oleh itu, kerja ini adalah satu penyelesaian dengan menyediakan kaedah pengkuantitian yang dilengkapi pengiraan khusus kekananan dan tingkahlaku untuk menentukan kebolehpercayaan pengguna.

Model kawalan akses berdasarkan kepercayaan, tujuan, dan peranan di pandangan jelmaan diperkenalkan bagi melindungi data dengan lebih cekap terutama atribut sensitif. Dalam model yang dicadangkan, tujuan dan peranan digunakan untuk mencapai data, sementara kepercayaan digunakan untuk mengawal capaian kepada atribut sensitif. Algoritma dibincangkan bagi menerangkan mekanisme kawalan capaian dengan terlebih dahulu mengesahkan peranan, tujuan, dan kepercayaan pengguna, sebelum membenarkan capaian oleh pengguna yang disahkan dan dipercayai. Satu sistem prototaip telah dibangunkan dan diuji, dan hasilnya menunjukkan atribut sensitif dilindungi. Eksperimen telah dikendalikan untuk mengesahkan model yang dicadangkan dengan membandingkannya dengan model terdahulu. Hasil dapatan menunjukkan model yang diperkenalkan adalah lebih cekap dan meningkatkan perlindungan privasi. Oleh itu, penyelidikan ini menyelesaikan masalah perlindungan data terutama atribut sensitif di pandangan jelmaan.

ACKNOWLEDGEMENTS

During the implementation process of this thesis, I have faced several challenges to finish it. At that moment, I felt angry, stress, sad, depress, and there have mix feeling, and there was at one time I thought about quitting. However, thank Almighty Allah for His guidance and strength to allow me to continue this journey until I have successful preparing this thesis.

This thesis would not have been possible without the help and support of many people over many years.

I would like to express my sincere gratitude and appreciation to my supervisor Associate Professor Dr. Nur Izura Udzir for teach me how to initiate and develop ideas into realistic goals. She has given inspiration, encouragement and support me throughout my PhD learning process. I feel very fortunate and appreciative to have worked under her supervision. I would like to thank to committee members: Dr. Mohd Izuan Hafez Ninggal, Associate Professor Dr. Nor Fazlida Mohd. Sani and Professor Dr. Hamidah Ibrahim for their valuable advice and suggestions.

Special thanks to Universiti Teknologi MARA (UiTM) (my workplace) especially to Faculty of Information Management for giving me opportunity to further PhD study, and to the Scholarship Department, Ministry of Higher Education, Malaysia for funding my study.

I extend my sincere and deep appreciation to my beloved wife, Siti Nor Ain Seri

Masran and my daughter Lana Cassandra Mohd Rafiz for their patience and continuous support. They have always been here with love and compassion to comfort me.

At last, but not the least, I wish to express my appreciation to my parents, Salji Alang Ahmad and Norhiyati Osman, my brother, sister, friends and relatives for their prayers, love and encouragement.

I certify that a Thesis Examination Committee has met on **May 2019** to conduct the final examination of **Mohd Rafiz bin Salji** on his thesis entitled "**Access Control Model Based on Trust, Purpose, and Role in Materialized View for Privacy Protection**" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the **Doctor of Philosophy**.

Members of the Thesis Examination Committee were as follows:

Azizol Bin Hj Abdullah, Ph.D.
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Zuriati Binti Ahmad Zukarnain, Ph.D.
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Mohd Taufik Bin Abdullah, Ph.D.
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Jemal Abawajy, Ph.D.
Professor
School of Information Technology Faculty of Science, Engineering and Built Environment
Deakin University
Australia
(External Examiner)

RUSLI ABDULLAH, Ph.D.
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of **Doctor of Philosophy**.

The members of the Supervisory Committee were as follows:

Nur Izura Binti Udzir, Ph.D.
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Mohd Izuan Hafez Bin Ninggal, Ph.D.
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Nor Fazlida Binti Mohd. Sani, Ph.D.
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Hamidah Binti Ibrahim, Ph.D.
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH YUNUS, Ph.D.
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

MOHD RAFIZ BIN SALJI

Date:

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIP	Allowable Intended Purpose
AP	Access Purpose
CIP	Conditional Intended Purpose
COPPA	Children’s Online Privacy Protection Act
CPBAC	Conditional Purpose-Based Access Control
CrePBAC	Credential Purpose-Based Access Control
DAC	Discretionary Access Control
DBMSs	Database Management Systems
DPBAC	Dynamic Purpose-Based Access Control
EHR	Electronic Health Records
HDB	Hippocratic Database
HIPAA	Health Insurance Portability and Accountability Act
HSC	Head of Studies Center
IoT	Internet of Things
IP	Intended Purpose
IPUMS	Integrated Public Use Microdata Series
MAC	Mandatory Access Control
MAGLel	Maximum Allowed Generalization Level
ML	Maximal Generalization Level
MTBAC	Mutual Trust Based Access Control
NIST	National Institute of Standards and Technology
P2P	Peer-to-Peer
P3P	Platform for Privacy Preferences

PBAC	Purpose-Based Access Control
PBFW	Policy-Based Access Control Model for Workflow Management System
PIP	Prohibited Intended Purpose
P-RBAC	Privacy-Aware Role-Based Access Control
PuRBAC	Purpose and Role-Based Access Control
RBAC	Role-Based Access Control
TA-RBAC	Trust-Aware Enhancement of RBAC
TBAC	Trust-Based Access Control
TPRBAC	Trust, Purpose, and Role-Based Access Control
TrustRBAC	Trust Role Based Access Control
UAC	Usage Access Control
UiTM	Universiti Teknologi MARA
URH	User Role History
VDM	Vienna Development Method

CHAPTER 1
INTRODUCTION

1.1 Preface

Nowadays, information technology is growing rapidly, with increasing number of hardware and software invented to facilitate people in their daily task. This technology allows people to protect their data privacy by using many types of applications. Data can be collected, stored, and used for their personal use or for work purpose. By using information technology, people can share data with the same interest party without any limitation of boundary.

Data privacy is increasingly becoming one of the very important issues in data management. People or customers are now more conscious about how their data are being protected by the organization. This awareness is increasingly highlighted when sharing and collecting data become seamless and prevalent by the omnipresence of Internet connection. In general, the organization collects, stores and uses customers' data for various purposes; and according to the Federal Trade Commission, US, 97 percent of websites collected at least one type of identifying information such as name, e-mail address, or postal address of customers (ANSI, 2004). This could lead to misuse of customer's data and less control of their information. It may create privacy violation and fear to the customer (Byun et al., 2005). Thus, data privacy should be protected in such a way that only authorized users can access the data. To protect the data privacy, a relevant mechanism needs to be introduced by the company to build a solid trust with customers. The mechanism should be equipped with minimum requirements of reasonable access for privacy and security as stipulated in the Health Insurance Portability and Accountability Act (HIPAA, 1996). In this research, data privacy is referring to customer data, i.e., age, address, and zip code that need to be protected from unauthorized user.

There are many approaches to preserve privacy, but access control is the most common approach to protect customers' data by preventing unauthorized access to the resources of the system (Bertolissi and Fernández, 2014; Crampton and Sellwood, 2014; Sandhu et al., 2000; Hung, 2005; Kayes et al., 2013; Lazouski et al., 2010; Ruj et al., 2012; Samarati, 2001). Many studies related to access control have been proposed to protect privacy, however, there are still issues highlighted in this study that impede the development of efficient access control models. The main issue is the lack of assessment granularity in authorizing access, which comprises reliance on identity, role and purpose-based access control schemes. Observing these challenges in protecting data, purpose, role, and trust must play a major role to control access of the data especially sensitive attributes.

Access control models have been developed in many environments, for example, cloud environment, web-based environment and Internet of Things (IoT) to solve the issue of privacy protection. Many access control models, for example, dynamic purpose-based access control (DPBAC) model (Peng et al., 2008), conditional purpose-based access control (CPBAC) model (Kabir and Wang, 2009), and role-involved purpose-based access control (RPAC) model (Kabir et al., 2012) have been proposed to protect the privacy in internal organization or at master tables, however, these models have been applied for a small system and covers a limited number of users.

In line with the above view, this research proposes an access control model based on role, purpose, and trust in materialized view to protect data especially sensitive attributes from unauthorized and untrusted access. Purpose and role are rather straightforward to identify, either the user authorizes to access data or vice versa, while trust needs to be quantified to specify either the user is trusted or not to access sensitive attributes. A method to calculate the user properties is also considered in this study to specify user's trustworthiness.

1.2 Why Access Control in Materialized View?

Materialized view is a replica of a table which is created in a very large systems such as data warehouses or distributed systems where data are replicated from the master tables or base relations located in a main database if the user requests to access it (Yousafi, 2013). The user can access data by querying the materialized view in the same manner as querying in base relations. In this context, ensuring privacy of data in materialized view level is as important as ensuring privacy of data in base relations.

Until now, only two access control models have been proposed in materialized view (Bahloul et al., 2011; Yousafi, 2013). One of the benefits of access control model in materialized view is it can be applied in a very large system (Bahloul et al., 2011).

In this study, there are two reasons of focusing on access control in materialized view. The reasons are as follows:

1. Existing access control models in materialized view is insufficient and inefficient in protecting data especially sensitive attributes in authorization view.

   Currently, two access control models (Bahloul et al., 2011; Yousafi, 2013) in materialized view have been proposed to protect data in authorization view. An access control model in materialized view using deductive rule (Bahloul et al., 2011) has been proposed to ensure confidentiality of data at the level of materialized view. This framework allows fine-grained authorization at the cell level. However, the administration of such systems is time consuming and cumbersome in a large environment as an administrator needs to define rules to each user to control access in materialized view (Yousafi, 2013). Subsequently, RBAC model (Yousafi, 2013) has been proposed to allow users to access data in materialized view based on role, i.e., a job function or job title instead of assigning access to a single user. However, it is still insufficient and inefficient in protecting data especially sensitive attributes in authorization view because user's purpose and trustworthiness were not taken into consideration to protect it. This may cause the risk of privacy disclosure to unauthorized and untrusted user. Authorization view specifies the data's accessibility by projecting specific columns in addition to selecting rows. It means that the selected data are allowed to be accessed by the user in authorization view. Moreover, previous access control models based on purpose or reason to access or use data (Peng et al., 2008; Kabir et al., 2012, 2011; Kabir and Wang, 2009; Sun and Wang, 2012; Sun et al., 2012; Abdul Ghani, 2013; Wang et al., 2014b; Elgendy et al., 2017) and trust or firm believe to someone or something (Toahchoodee et al., 2009; Li et al., 2009b, 2012) also do not consider sensitive attributes protection. Due to limitations of the previous works, a finer-grained access control model in materialized view needs to be proposed to protect data especially sensitive attributes in authorization view. A finer-grained access control model in this study refers to the access control model, which is not generally considered protecting data, but also refers specifically to protecting sensitive attributes.

2. A new deductive rule needs to be proposed in materialized view to limit access of data without involving sensitive attributes in authorization view.

   Previous work by Bahloul et al.(2011) proposes deductive rule to act as an access control to avoid data to be accessed as the same manner as in the database (base relations). Deductive rule is the rule to hide certain attributes, i.e., personal and sensitive information to be accessed by the user in materialized view (Bahloul et al., 2011). The system allows users to access the resources from external organization by applying deductive rule in materialized view compared to non-materialized view in order to ensure confidentiality of data in materialized view. Therefore, when a user requests to access data in materialized view, a user will not obtain sensitive values, such as, income and medical condition/information, unlike if a user requests at base relations. In this research, a new deductive rule needs to be proposed to deduct certain data, for example, age without involving sensitive attributes because trust is applied in the proposed access control model to control access of sensitive attributes.

1.3 Research Problem

In the RBAC model (Yousafi, 2013), a fine-grained access control in materialized view permits user access to the data based on role, i.e., job title or job function. In this model, the administrator uses the role to set the deductive rule where different roles can access certain data in authorization view. However, in this model all users with the same role can be allowed to access customers' data in authorization view without considering their purpose. For example, medical doctors can access patients' data; but, not all medical doctors are authorized to access all patients' data. Thus, only certain medical doctors with purpose can access certain patients' data or the patients under their purview. Purpose means ”for what reason data are accessed or used” (Agrawal et al., 2002; Jafari et al., 2014; Peng et al., 2008; Masoumzadeh and Joshi, 2008). To access data, user needs to be evaluated based on the purpose of the usage. Purpose-based access control (PBAC) is a common access control model, which considers the purpose of access as an essential factor in deciding whether to permit or deny access to the resources. Many PBAC models

(Peng et al., 2008; Kabir et al., 2012, 2011; Kabir and Wang, 2009; Sun and Wang, 2012; Sun et al., 2012; Abdul Ghani, 2013; Wang et al., 2014b; Elgendy et al., 2017) have been proposed to preserve data privacy. In these models, purpose is considered in order to allow certain users to access certain data to avoid privacy violation. There are three options which the customer can set the level of privacy in the PBAC model before permitting or denying user access to the data, to allow, conditionally allow, or prohibit access (Kabir et al., 2012, 2011; Kabir and Wang, 2009). For example, a customer Alice allows her age, i.e., 37 to be accessed by users for admin purpose; but, she prohibits users to access it for marketing purpose. Subsequently, she may conditionally allow her age, i.e., 35-40 to be accessed by users for purchase purpose. Based on this example, customer data should be accessed by the user based on role and purpose, not based on role only to protect customer privacy. Therefore, a new access control model needs to be proposed that considers the user's purpose to protect data.

Data in nature is a sensitive information, but sensitive attributes must remain safe (Maheshwarkar et al., 2012). In general, data are divided into three types of attributes, namely, de-identified, quasi identifier, and sensitive (Sweeney, 2002b). De-identified data are the obvious identifying records that need to be concealed, for instance social security number. In contrast, quasi identifier such as race, age, and zip code is a non-key attribute that needs to be generalized before it can be released. Meanwhile, sensitive attributes such as medical condition and income are classified data which privately belong to a customer. Data that are released to the public may contain sensitive and non-sensitive attributes (Maheshwarkar et al., 2012). Sensitive attributes are those attributes which may remain hidden from external usage, while non-sensitive attributes are the same as quasi identifier. Therefore, sensitive attributes require critical restricted access in the system and access to this attribute is limited to trusted users only. However, existing access control models (Yousafi, 2013; Peng et al., 2008; Kabir et al., 2012, 2011; Kabir and Wang, 2009; Sun and Wang, 2012; Sun et al., 2012; Abdul Ghani, 2013; Wang et al., 2014b; Elgendy et al., 2017) do not focus on protecting sensitive attributes. Unfortunately, not all authorized users can be trusted, and they can access sensitive attributes. This may lead to the risk of inappropriate access and use of sensitive attributes. Therefore, a mechanism is needed to permit only trusted users to access sensitive attributes. In access control model, one of the common types of access control called trust-based access control (TBAC) is applied to protect the resources of the system. TBAC is inspired by an important aspect in human life, which is trust. In this study, trust refers to firm believe to a user in an organization. By this concept, a user that is highly trusted will be granted access to more resources. However, trust is mutable in response to the changing situations. Therefore, it is paramount to design an efficient access control model that can capture the dynamic nature of human trustworthiness. Based on previous literature, access control models based on trust (Toahchoodee et al., 2009; Li et al., 2009b, 2012) have been proposed to protect data, but not specifically protecting sensitive attributes. Therefore, a new access control model needs to be proposed to consider trust to protect sensitive attributes.

Besides privacy protection issue, specifying user's trustworthiness is also taken into consideration to ensure sensitive attributes as discussed previously is protected by using a trust. In order to access sensitive attributes, certain user properties need to be quantified to specify user's trustworthiness on accessing it or vice versa. However, the issue is how to quantify certain user properties to specify user's trustworthiness. Quantification methods (Toahchoodee et al., 2009; Li et al., 2009b, 2012) have been proposed to quantify certain user properties to specify user's trustworthiness. If authorized users achieve highly trusted based on the calculation of user properties, they are permitted to access the data. However, these previous works provide a general calculation without showing the detail elements used to calculate the user properties to specify user's trustworthiness. For example, Toahchoodee et al. (2009) suggested using recommendation to specify user's trustworthiness, however, previous work does not provide what are the elements need to be quantified by the recommender to specify user's trustworthiness. By showing the detail elements, this research can contribute to provide a better result from the calculation of user properties to specify user's trustworthiness as compared to the previous works. Therefore, a new quantification method needs to be proposed to provide specific calculation of user properties to specify user's trustworthiness.

Based on previous discussion, the main problem highlighted in this research is the inability to achieve better data privacy protection by previous access control models. Therefore, the issues highlighted in this study are as follows:

1. Existing quantification methods are too general in calculating or quantifying certain user properties to determine user's trustworthiness.
2. Access control model in materialized view is insufficient and inefficient based on role only to protect data, which may cause privacy disclosure to unauthorized and untrusted user, while access control models based on purpose and trust also do not focus protecting sensitive attributes.

1.4 Research Objectives

The main objective of this study is to propose an access control model in materialized view to achieve better data privacy protection in authorization view.

Specific objectives of the study are as follows:

1. To propose a quantification method which provides specific calculation of the two user properties, namely: seniority and behaviour to specify user's trustworthiness.

2. To propose an efficient access control model in materialized view based on trust, purpose, and role to protect data especially sensitive attributes in authorization view.

1.5 Scope of the Research

To achieve the research objectives, it is necessary to determine the scope of the research. This thesis covers the following items, which are:

1. Utilize access control

   In general, there are many available mechanisms used to protect data, for example, encryption and digital signatures (Abdul Ghani, 2013). However, this study focuses on access control to protect data as this mechanism is the most common approach to protect data from unauthorized user.

2. Materialized view

   Materialized view has many functions in database systems, for example, to speed up queries and storing query results (Alur et al., 2002). Because of the great performance of materialized view in managing database and covers wide area; much research has been conducted on how to keep materialized view consistent with the source tables (Løland and Hvasshovd, 2006). However, this research focuses on protecting data in materialized view.

1.6 Significance of Study

Based on the explanation in the previous sections, the importance of this study can be pointed as follows:

1. To solve the issue of previous quantification methods by proposing a quantification method, which provides specific calculation of the two user properties, namely, seniority and behaviour to specify user's trustworthiness.

2. To solve the issue of privacy protection in materialized view by proposing an efficient trust, purpose, and role-based access control (TPRBAC) model in materialized view to protect data especially sensitive attributes in authorization view.

1.7 Research Contributions

The main contribution of this work is that a finer-grained access control model using trust, purpose, and role in materialized view is proposed to improve data privacy protection. This main contribution is divided into two contributions, which are expected to be achieved in this study:

1. A quantification method is proposed to specify user's trustworthiness by providing specific calculation of the seniority and behaviour.

    (a) Seniority is proposed to specify the user seniority, either junior or senior.

    (b) Behaviour is proposed to determine the user behaviour, either trust or mistrust.

2. An efficient trust, purpose, and role-based access control (TPRBAC) model in materialized view is proposed to protect data especially sensitive attributes in authorization view.

(a) A deductive rule is proposed to deduct certain data without involving sensitive attributes because trust is considered to protect it.

In summary, the problems, objectives, and contributions of this thesis are shown in Table 1.1.

1.8 Thesis Organization

The rest of this thesis is organized as follows:

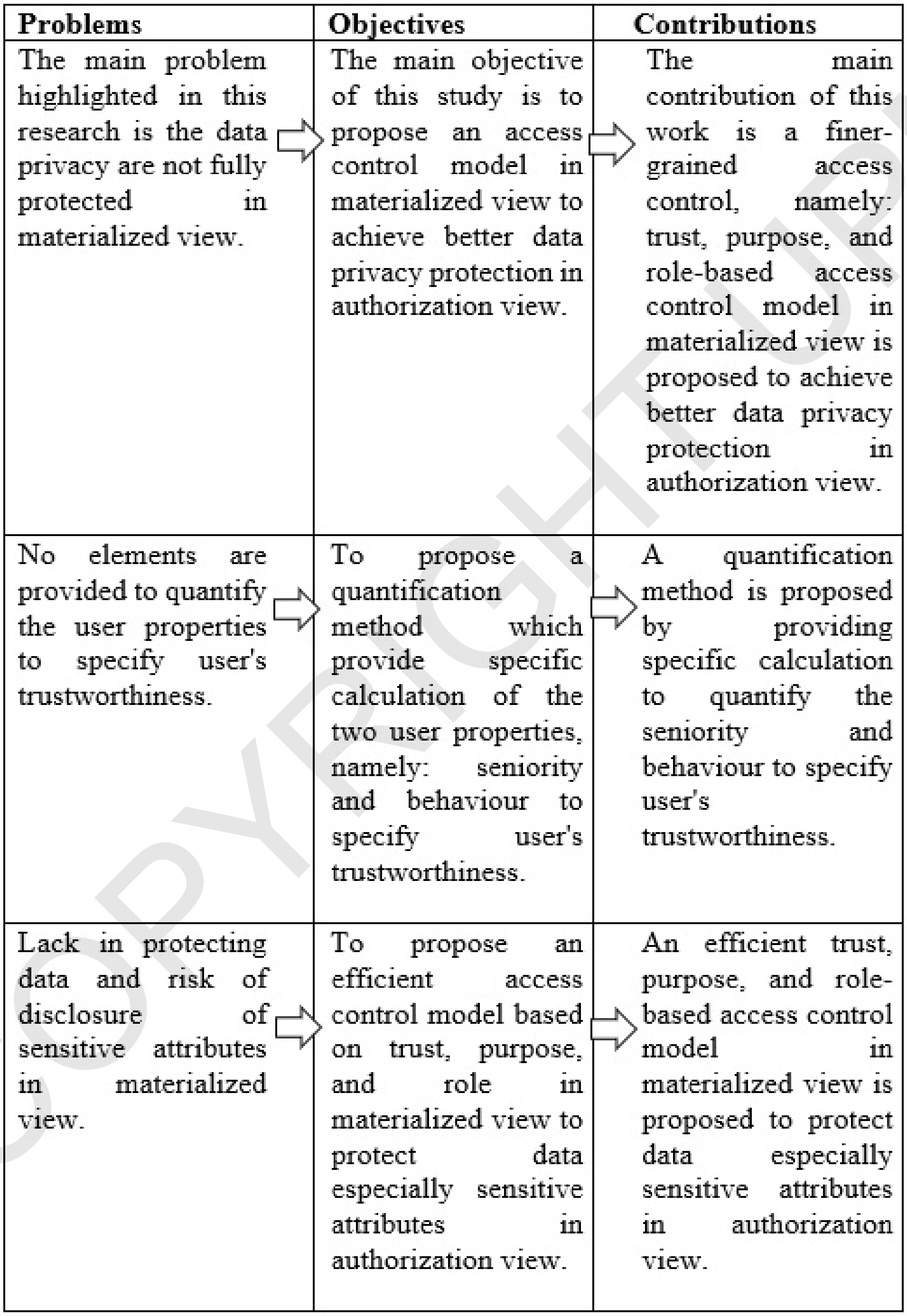
Chapter 2 reviews on access control mechanisms. In this chapter, the data privacy is defined, while access control and the early models are explained. Then, this chapter discusses the privacy, purpose, and access control, and explains the purpose-based access control models. This chapter also discusses the trust and access control, and presents the previous trust-based access control models. The materialized view and related works are defined and discussed. A comparative analysis of access control models is explained, and finally, the chapter is concluded with a summary.

Chapter 3 presents the research methodology used in this study. In this chapter, the research development phases are explained.

Chapter 4 discusses the proposed quantification method of user trustworthiness. First, the requirements for the development of the proposed quantification method is discussed. Next, this chapter discuss on the user properties, while user's trustworthiness and access to the resources is explained. Then, quantification method and the process of the proposed quantification method are discussed and presented.

Chapter 5 describes the proposed trust, purpose, and role-based access control (TPRBAC) model in materialized view. First, the requirement for the develop-

Table 1.1: Summary of the problems, objectives, and contributions



Problems	Objectives	Contributions
The main problem highlighted in this research is the data privacy are not fully protected in materialized view.	The main objective of this study is to propose an access control model in materialized view to achieve better data privacy protection in authorization view.	The main contribution of this work is a finer-grained access control, namely: trust, purpose, and role-based access control model in materialized view is proposed to achieve better data privacy protection in authorization view.
No elements are provided to quantify the user properties to specify user's trustworthiness.	To propose a quantification method which provide specific calculation of the two user properties, namely: seniority and behaviour to specify user's trustworthiness.	A quantification method is proposed by providing specific calculation to quantify the seniority and behaviour to specify user's trustworthiness.
Lack in protecting data and risk of disclosure of sensitive attributes in materialized view.	To propose an efficient access control model based on trust, purpose, and role in materialized view to protect data especially sensitive attributes in authorization view.	An efficient trust, purpose, and role-based access control model in materialized view is proposed to protect data especially sensitive attributes in authorization view.

ment of the TPRBAC model in materialized view is discussed, and the specification of access control model components is explained. Then, the TPRBAC model in materialized view, and authorization and verification are presented and discussed.

Next, this chapter explains the access decision, and presents the query modification. Finally, this chapter discusses the access control policy of the TPRBAC model.

Chapter 6 covers the explanation on how to test the proposed quantification method of user's trustworthiness and test and validation of the TPRBAC model. First, the evaluation of the proposed quantification method is presented. Next, the testing and validation of the proposed access control model in materialized view is presented.

Chapter 7 provides the conclusion, contributions and discusses the potential of future works.

BIBLIOGRAPHY

Abdul Ghani, N. 2013. *Credential Purpose-Based Access Control for Personal Data Protection in Web-Based Applications*. PhD thesis, Universiti Teknologi Malaysia, Faculty of Computing.

Agrawal, R., Kiernan, J., Srikant, R. and Xu, Y. 2002. Hippocratic Databases. In *VLDB'02: Proceedings of the 28th International Conference on Very Large Databases*, 143–154. Elsevier.

Al-Dabbagh, B., Scornavacca, E., Sylvester, A. and Johnstone, D. 2016. The effect of ICT self-discipline in the workplace. *arXiv preprint arXiv:1606.00894* .

Al-Fedaghi, S. S. 2007. Beyond Purpose-based Privacy Access Control, 23–32. Darlinghurst, Australia, Australia: Australian Computer Society, Inc.

Alur, N., Haas, P., Momiroska, D., Read, P., Summers, N., Totanes, V. and Zuzarte, C. 2002. DB2 UDBs High Function Business Intelligence in e-business. *IBM Redbook Series* .

ANSI. 2004. American National Standard for Information Technology Role Based Access Control. *ANSI INCITS* 359–2004.

Ardagna, C. A., Cremonini, M., De Capitani di Vimercati, S. and Samarati, P. 2008. A Privacy-Aware Access Control System. *Journal of Computer Security* 16 (4): 369–397.

Asmawi, A., Affendey, L., Udzir, N. and Mahmod, R. 2014. Enhance Security in XML Databases: XLog File for Severity-Aware Trust-Based Access Control. *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering* 8 (6): 961–963.

Bahloul, S. N., Coquery, E. and Hacid, M.-S. 2011. Access Control to Materialized Views: An Inference-Based Approach. In *Proceedings of the 2011 Joint EDBT/ICDT Ph. D. Workshop*, 19–24. ACM.

Bai, S., Hao, B., Li, A., Yuan, S., Gao, R. and Zhu, T. 2013. Predicting Big Five Personality Traits of Microblog Users. In *Proceedings of the 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)-Volume 01*, 501–508. IEEE Computer Society.

Barker, S. and Stuckey, P. J. 2003. Flexible Access Control Policy Specification with Constraint Logic Programming. *ACM Transactions on Information and System Security (TISSEC)* 6 (4): 501–546.

Bates, A., Mood, B., Valafar, M. and Butler, K. 2013. Towards secure provenance-based access control in cloud environments. In *Proceedings of the third ACM conference on Data and application security and privacy*, 277–284. ACM.

Behera, P. K. and Khilar, P. M. 2017. A Novel Trust Based Access Control Model for Cloud Environment. In *Proceedings of the International Conference on Signal, Networks, Computing, and Systems*, 285–295. Springer.

Beimel, D. and Peleg, M. 2011. Using OWL and SWRL to represent and reason with situation-based access control policies. *Data & Knowledge Engineering* 70 (6): 596–615.

Benbasat, I. and Wang, W. 2005. Trust in and Adoption of Online Recommendation Agents. *Journal of the Association for Information Systems* 6 (3): 4.

Bertino, E., Ghinita, G., Kamra, A. et al. 2011. Access Control for Databases: Concepts and Systems. *Foundations and Trends® in Databases* 3 (1–2): 1–148.

Bertino, E. and Sandhu, R. 2005. Database Security-Concepts, Approaches, and Challenges. *IEEE Transactions on Dependable and Secure Computing* 2 (1): 2–19.

Bertolissi, C. and Fernández, M. 2014. A Metamodel of Access Control for Distributed Environments: Applications and Properties. *Information and Computation* .

Braghin, S., Coen-Porisini, A., Colombo, P., Sicari, S. and Trombetta, A. 2008. Introducing Privacy in a Hospital Information System. In *Proceedings of the Fourth International Workshop on Software Engineering for Secure Systems*, 9–16. ACM.

Bruhn, J. G. 2001. *Trust and the Health of Organizations*. Springer Science & Business Media.

Byun, J.-W. and Bertino, E. 2006. Micro-Views, or on How to Protect Privacy while Enhancing Data Usability: Concepts and Challenges. *ACM SIGMOD Record* 35 (1): 9–13.

Byun, J.-W., Bertino, E. and Li, N. 2005. Purpose Based Access Control of Complex Data for Privacy Protection. In *Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, 102–110. New York, NY, USA: ACM.

Byun, J.-W. and Li, N. 2008. Purpose Based Access Control for Privacy Protection in Relational Database Systems. *The VLDB Journal* 17 (4): 603–619.

Castano, S. and Ferrari, E. 2003, In Web-Powered Databases, In *Web-Powered Databases*, 299–330, IGI Global, 299–330.

Center, M. P. 2017, Integrated Public Use Microdata Series, International: Version 6.5 [dataset].

Chakraborty, S. and Ray, I. 2006. TrustBAC: Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems. In *Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies*, 49–58. ACM.

Chaves, L. W. F., Buchmann, E., Hueske, F. and Böhm, K. 2009. Towards Materialized View Selection for Distributed Databases. In *Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology*, 1088–1099. ACM.

Chen, M.-Y., Yang, C. C. and Hwang, M.-S. 2013. Privacy Protection Data Access Control. *IJ Network Security* 15 (6): 411–419. Cited kabir2011.

Cheng, Y., Park, J. and Sandhu, R. 2014. Attribute-Aware Relationship-Based Access Control for Online Social Networks. In *IFIP Annual Conference on Data and Applications Security and Privacy*, 292–306. Springer.

Colombo, P. and Ferrari, E. 2014. Enforcement of Purpose Based Access Control within Relational Database Management Systems. *Knowledge and Data Engineering, IEEE Transactions on* 26 (11): 2703–2716.

Crampton, J. and Sellwood, J. 2014. Path Conditions and Principal Matching: A New Approach to Access Control. In *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies*, 187–198. ACM.

Didriksen, T. 1997. Rule Based Database Access Control-A Practical Approach. In *Proceedings of the Second ACM Workshop on Role-Based Access Control*, 143–151. ACM.

Duckworth, A. L. and Seligman, M. E. 2006. Self-discipline gives girls the edge: Gender in self-discipline, grades, and achievement test scores. *Journal of educational psychology* 98 (1): 198.

Einarsen, S., Hoel, H. and Cooper, C. 2003. *Bullying and emotional abuse in the workplace: International perspectives in research and practice*. CRC Press.

Elgendy, R., Morad, A., Elmongui, H. G., Khalafallah, A. and Abougabal, M. S. 2017. Role-Task Conditional-Purpose Policy Model for Privacy Preserving Data Publishing. *Alexandria Engineering Journal* 56 (4): 459–468.

Ercan, T. and Yıldız, M. 2010. Semantic Access Control for Corporate Mobile Devices. In *International Conference on Algorithms and Architectures for Parallel Processing*, 198–207. Springer.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R. and Chandramouli, R. 2001. Proposed NIST Sstandard for Role-Based Access Control. *ACM Transactions on Information and System Security (TISSEC)* 4 (3): 224–274.

Gajanayake, R., Iannella, R. and Sahama, T. 2014. Privacy Oriented Access Control for Electronic Health Records. *electronic Journal of Health Informatics* 8 (2): 15.

Ganesan, S. and Weitz, B. A. 1996. The Impact of Staffing Policies on Retail Buyer Job Attitudes and Behaviors. *Journal of Retailing* 72 (1): 31–56.

Gkountouna, O., Angeli, S., Zigomitros, A., Terrovitis, M. and Vassiliou, Y. 2014. K M-Anonymity for Continuous Data Using Dynamic Hierarchies. In *Privacy in Statistical Databases*, 156–169. Springer.

Gollmann, D. 2011. From Access Control to Trust Management, and Back–A Petition. In *IFIP International Conference on Trust Management*, 1–8. Springer.

Gopalan, R., Antón, A. and Doyle, J. 2012. UCONLEGAL: A Usage Control Model for HIPAA, 227–236. New York, NY, USA: ACM.

Guarda, P. and Zannone, N. 2009. Towards the Development of Privacy-Aware Systems. *Information and Software Technology* 51 (2): 337–350.

Harris, S. 2002. *Mike Meyers' CISSP Certification Passport*. McGraw-Hill/Osborne.

Hung, P. C. 2005. Towards a Privacy Access Control Model for e-Healthcare Services. In *Third Annual Conference on Privacy, Security and Trust, October 12-14, 2005, The Fairmont Algonquin, St. Andrews, New Brunswick, Canada, Proceedings*.

Jafari, M., Fong, P. W., Safavi-Naini, R., Barker, K. and Sheppard, N. P. 2011. Towards Defining Semantic Foundations for Purpose-Based Privacy Policies. In *Proceedings of the First ACM Conference on Data and Application Security and Privacy*, 213–224. ACM.

Jafari, M., Safavi-Naini, R., Fong, P. W. L. and Barker, K. 2014. A Framework for Expressing and Enforcing Purpose-Based Privacy Policies. *ACM Trans. Inf. Syst. Secur.* 17 (1): 3:1–3:31.

Jafari, M., Safavi-Naini, R. and Sheppard, N. P. 2009. Enforcing Purpose of Use via Workflows, 113–116. New York, NY, USA: ACM.

Jin, X., Sandhu, R. and Krishnan, R. 2012. RABAC: Role-Centric Attribute-Based Access Control. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, 84–96. Springer.

Kabir, M., Wang, H. and Bertino, E. 2012. A Role-Involved Purpose-Based Access Control Model. *Information Systems Frontiers* 14 (3): 809–822.

Kabir, M. E. and Wang, H. 2009. Conditional Purpose Based Access Control Model for Privacy Protection. In *Proceedings of the Twentieth Australasian Conference on Australasian Database-Volume 92*, 135–142. Australian Computer Society, Inc.

Kabir, M. E., Wang, H. and Bertino, E. 2011. A Conditional Purpose-Based Access Control Model with Dynamic Roles. *Expert Syst. Appl.* 1482–1489.

Kayes, A., Han, J. and Colman, A. 2013. A Semantic Policy Framework for Context-Aware Access Control Applications. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on*, 753–762.

Kayes, A., Han, J. and Colman, A. 2015. An Ontological Framework for Situation-Aware Access Control of Software Services. *Information Systems* .

Kim, M., Seo, J., Noh, S. and Han, S. 2012. Identity Management-Based Social Trust Model for Mediating Information Sharing and Privacy Enhancement. *Security and Communication Networks* 5 (8): 887–897.

Kohlmayer, F., Prasser, F., Eckert, C., Kemper, A. and Kuhn, K. A. 2012. Flash: Efficient, Stable and Optimal K-Anonymity. In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, 708–717. IEEE.

Lampson, B., Abadi, M., Burrows, M. and Wobber, E. 1992. Authentication in Distributed Systems: Theory and Practice. *ACM Transactions on Computer Systems (TOCS)* 10 (4): 265–310.

Lazouski, A., Martinelli, F. and Mori, P. 2010. Usage Control in Computer Security: A Survey. *Computer Science Review* 4 (2): 81–99.

LeFevre, K., A. R. E. V. R. R. X. Y. . D. D. 2004. Limiting Disclosure in Hippocratic Databases. *In: 30th International Conference on Very Large Databases* 10817119.

Li, J., Wang, B., Ding, N. and Jin, S. 2011a. Access Control Model Based on Multi-Role and Task. In *Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011 2nd International Conference on*, 2756–2759. IEEE.

Li, M., Sun, X., Wang, H. and Zhang, Y. 2012. Multi-Level Delegations with Trust Management in Access Control Systems. *Journal of Intelligent Information Systems* 39 (3): 611–626.

Li, M., Sun, X., Wang, H., Zhang, Y. and Zhang, J. 2011b. Privacy-Aware Access Control with Trust Management in Web Service. *World Wide Web* 14 (4): 407–430.

Li, M., Wang, H. and Plank, A. 2009a. Privacy-aware Access Control with Generalization Boundaries, 105–112. Darlinghurst, Australia, Australia: Australian Computer Society, Inc.

Li, M., Wang, H. and Ross, D. 2009b. Trust-Based Access Control for Privacy Protection in Collaborative Environment. In *e-Business Engineering, 2009. ICEBE'09. IEEE International Conference on*, 425–430. IEEE.

Løland, J. 2007. *Materialized View Creation and Transformation of Schemas in Highly Available Database Systems*. PhD thesis, Citeseer.

Løland, J. and Hvasshovd, S.-O. 2006. Online, non-blocking relational schema changes. In *International Conference on Extending Database Technology*, 405–422. Springer.

Ma, G., Wu, K., Zhang, T. and Li, W. 2011. A Flexible Policy-Based Access Control Model for Workflow Management Systems. In *Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on*, 533–537. IEEE.

Maheshwarkar, N., Pathak, K. and Choudhari, N. S. 2012. K-anonymity model for multiple sensitive attributes. *International Journal of Computer Applications (IJCA)* .

Marchiori, M., Cranor, L., Langheinrich, M., Presler-Marshall, M. and Reagle, J. 2002. The Platform for Privacy Preferences 1.0 (P3P1. 0) Specification. *World Wide Web Consortium Recommendation REC-P3P-20020416* .

Masoumzadeh, A. and Joshi, J. B. 2008. PuRBAC: Purpose-aware role-based access control. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, 1104–1121. Springer.

Mavridis, I. 2011. Deploying Privacy Improved RBAC in Web Information Systems. *Int. J. Inf. Technol. Syst. Appoach* 4 (2): 70–87.

Mirabi, M., Ibrahim, H., Mamat, A. and Udzir, N. I. 2011. Integrating Access Control Mechanism with EXEL Labeling Scheme for XML Document Updating. In *Networked Digital Technologies*, 24–36. Springer.

Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.-M., Karat, J. and Trombeta, A. 2010. Privacy-aware Role-based Access Control. *ACM Trans. Inf. Syst. Secur.* 13 (3): 24:1–24:31.

Ni, Q., Trombetta, A., Bertino, E. and Lobo, J. 2007. Privacy-Aware Role Based Access Control. In *Proceedings of the 12th ACM Symposium on Access Control Models and Technologies*, 41–50. New York, NY, USA: ACM.

Oleshchuk, V. 2012. Trust-Aware RBAC. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, 97–107. Springer.

Peng, H., Gu, J. and Ye, X. 2008. Dynamic purpose-based access control. In *Parallel and Distributed Processing with Applications, 2008. ISPA'08. International Symposium on*, 695–700. IEEE.

Pottinger, R. and Levy, A. Y. 2000. A Scalable Algorithm for Answering Queries Using Views. In *VLDB*, 484–495.

Potts, C. and Tech, G. 2001. What is privacy .

Research, F. 2001. Privacy concerns cost e-commerce $15 billion. *Technical report* .

Ruj, S., Stojmenovic, M. and Nayak, A. 2012. Privacy Preserving Access Control with Authentication for Securing Data in Clouds. In *Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on*, 556–563. IEEE.

Samarati, P. 2001. Protecting Respondents Identities in Microdata Release. *Knowledge and Data Engineering, IEEE Transactions on* 13 (6): 1010–1027.

Sandhu, R., Ferraiolo, D. and Kuhn, R. 2000. The NIST Model for Role-Based Access Control: Towards a Unified Standard. In *ACM Workshop on Role-based Access Control*.

Sandhu, R. S. and Samarati, P. 1994. Access Control: Principle and Practice. *IEEE communications magazine* 32 (9): 40–48.

Senese, S. V. 2015. A Study of Access Control for Electronic Health Records .

Sicari, S., Rizzardi, A., Grieco, L. and Coen-Porisini, A. 2015. Security, Privacy and Trust in Internet of Things: The Road Ahead. *Computer Networks* 76: 146–164.

Singh, T. and Kumar, R. 2011. Database and Information Security Concerns. *International Journal of Computer Science & Technology.* 4 (2): 211–215.

Smari, W. W., Clemente, P. and Lalande, J.-F. 2014. An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system. *Future Generation Computer Systems* 31: 147–168.

Sodiya, A. S. and Onashoga, A. S. 2009. Components-Based Access Control Architecture. *Issues in Informing Science & Information Technology* 6.

Stigler, G. J. 1980. An Introduction to Privacy in Economics and Politics. *The Journal of Legal Studies* 9 (4): 623–644.

Sun, L. and Wang, H. 2012. A Purpose-Based Access Control in Native XML Databases. *Concurrency and Computation: Practice and Experience* 24 (10): 1154–1166.

Sun, L., Wang, H., Soar, J. and Rong, C. 2012. Purpose Based Access Control for Privacy Protection in E-Healthcare Services. *Journal of Software* 7 (11).

Sun L., L. Y. 2008. Using Usage Control to Access XML Database. *International Journal of Information Systems in the Service Sector* 1: 3244.

Sweeney, L. 2002a. Achieving K-Anonymity Privacy Protection using Generalization and Suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10 (05): 571–588.

Sweeney, L. 2002b. K-Anonymity: A Model for Protecting Privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10 (05): 557–570.

Szoka, B. M. and Thierer, A. D. 2009. COPPA 2.0: The New Battle Over Privacy, Age Verification, Online Safety & Free Speech .

Thakur, G. and Gosain, A. 2011. A Comprehensive Analysis of Materialized Views in a Data Warehouse Environment. *International Journal of Advanced Computer Science and Applications (IJACSA)* 2 (5).

Theodoratos, D. and Sellis, T. 1999. Dynamic Data Warehouse Design. In *International Conference on Data Warehousing and Knowledge Discovery*, 1–10. Springer.

Toahchoodee, M., Abdunabi, R., Ray, I. and Ray, I. 2009. A Trust-Based Access Control Model for Pervasive Computing Applications. In *Data and Applications Security XXIII*, 307–314. Springer.

Tschantz, M. C., Datta, A. and Wing, J. M. 2011. On the Semantics of Purpose Requirements in Privacy Policies. *arXiv preprint arXiv:1102.4326* .

Uikey, C. and Bhilare, D. 2017. TrustRBAC: Trust Role Based Access Control Model in Multi-Domain Cloud Environments. In *Information, Communication, Instrumentation and Control (ICICIC), 2017 International Conference on*, 1–7. IEEE.

Vidyalakshmi, B., Wong, R. K. and Chi, C.-H. 2013. Decentralized Trust Driven Access Control for Mobile Content Sharing. In *Big Data (BigData Congress), 2013 IEEE International Congress on*, 239–246. IEEE.

Vimercati, S. D. C. D., Foresti, S., Jajodia, S., Paraboschi, S., Psaila, G. and Samarati, P. 2012. Integrating Trust Management and Access Control in Data-Intensive Web Applications. *ACM Transactions on the Web (TWEB)* 6 (2): 6.

Wang, H. and Sun, L. 2010. Trust-Involved Access Control in Collaborative Open Social Networks. In *Network and System Security (NSS), 2010 4th International Conference on*, 239–246. IEEE.

Wang, H., Sun, L. and Bertino, E. 2014a. Building Access Control Policy Model for Privacy Preserving and Testing Policy Conflicting Problems. *J. Comput. Syst. Sci.* 80 (8): 1493–1503.

Wang, W., Han, J., Song, M. and Wang, X. 2011. The Design of a Trust and Role Based Access Control Model in Cloud Computing. In *Pervasive Computing and Applications (ICPCA), 2011 6th International Conference on*, 330–334. IEEE.

Wang, Y., Zhou, Z. and Li, J. 2014b. A Purpose-Involved Role-Based Access Control Model, 1119–1131. Springer Berlin Heidelberg.

Warren, S. D. and Brandeis, L. D. 1890. The Right to Privacy. *Harvard law review* 193–220.

Weber, H. A. 2003. Role-Based Access Control: The NIST Solution. *SANS institute InfoSec Reading Room* .

Westin, A. 1970. Privacy and Freedom. 1967. *Atheneum, New York* .

Ya-Jun, G., Fan, H., Qing-Guo, Z. and Rong, L. 2005. An Access Control Model for Ubiquitous Computing Application .

Yang, J., Karlapalem, K. and Li, Q. 1997. Algorithms for Materialized View Design in Data Warehousing Environment. In *VLDB*, 136–145.

Yang, N. 2011. *Formalism of Privacy Preserving Access Control*. PhD thesis, University of Manchester.

Yang, N., Barringer, H. and Zhang, N. 2007. A Purpose-Based Access Control Model. In *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on*, 143–148. IEEE.

Younis, Y. A., Kifayat, K. and Merabti, M. 2014. An Access Control Model for Cloud Computing. *Journal of Information Security and Applications* 19 (1): 45–60.

Yousafi, H. 2013. A Role-Based Access Control Schema for Materialized Views. Master's thesis, University of Windsor.

Zhang, Q., Koudas, N., Srivastava, D. and Yu, T. 2007. Aggregate Query Answering on Anonymized Tables. In *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on*, 116–125. IEEE.