CREDENTIAL PURPOSE-BASED ACCESS CONTROL FOR PERSONAL DATA PROTECTION IN WEB-BASED APPLICATIONS

NORJIHAN BINTI ABDUL GHANI

A thesis submitted in fulfilment
of the requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

APRIL 2013

To my husband, and our children.

Also to my mother and father.

Their patience, understanding, and dedication are well appreciated.

ACKNOWLEDGEMENT

The preparation of this thesis has been made possible through various individuals. First of all, Alhamdulillah, praise to Allah who has given me good health and time for going through this challenging period of my life.

Many thanks go to Associate Professor Dr. Harihodin Selamat, the main supervisor for this research, and my co-supervisor, Associate Professor Dr. Zailani Mohamed Sidek. Their patience, understanding, encouragement, and especially the constructive criticisms and suggestions make the process of conducting this research run smoothly.

Special thanks also go to University of Malaya, my employer, which has given me the opportunity to take up this PhD study. Also for the Ministry of Higher Education for funding my Ph.D study. And the rest, staff and colleagues at FSKTM, University of Malaya, many thanks for their assistance that make this research fruitful.

Lastly, my appreciation is also to those who were directly or indirectly involved in this research. These include my parents, Abdul Ghani b. Yusoff and Russini bt Hassan, my husband, Zahir b. Mohd. Jaafar. Also for my children, thank you for understanding me.

Their involvements have shaped the research project in many ways. May Allah bless you all for your kindness and willingness to help in completing this research.

ABSTRACT

Web-based applications enable users to carry out their business transactions virtually at any time and place whereby users are required to disclose almost all their personal information which result in greater risks of information disclosure. Therefore, protecting personal information is of utmost importance. Enforcing personal information protection in databases requires controlled access to systems and resources and granted only to authorized users. Traditional access control systems cannot be used in achieving full personal data protection. Current purpose-based access control systems provide insufficient protection of personal data especially in web-based applications. This is mainly due to the absence of user authentication in these systems and the fact that data subjects have less control over their information. This research is an effort to overcome this problem in which the Credential Purpose-Based Access Control (CrePBAC) system is introduced. This system implements a two-phase security and an access control mechanism with a model and security policy implementation. The two-phase security model involves user authentication using personal credential and data authorization based on purpose. The organization's security and privacy policies are implemented using metadata technique in Hippocratic Databases. The metadata technique utilizes a data labeling scheme based on purpose and control data access through query modification. The model and mechanism were successfully implemented. The results from the two types of case studies tested showed that the access control mechanism provides users with more rights and control over their data. In conclusion, this research has introduced a new approach in purpose-based access control with a two-phase security model and mechanism that provides greater control for personal data protection in web-based applications.

ABSTRAK

Aplikasi berasaskan-web membolehkan pengguna menjalankan urusniaga perniagaan secara maya pada bila-bila masa dan tempat di mana pengguna dikehendaki mendedahkan hampir semua maklumat peribadi yang menyebabkan risiko lebih besar dalam pendedahan maklumat. Oleh itu, melindungi maklumat peribadi adalah sangat penting. Penguatkuasaan perlindungan maklumat peribadi dalam pangkalan data memerlukan capaian kepada sistem dan sumber dikawal dan diberi hanya kepada pengguna yang berhak sahaja. Sistem kawalan capaian tradisional tidak boleh digunakan dalam mencapai perlindungan penuh data peribadi. Sistem kawalan capaian berasaskan-tujuan, pada masa ini tidak dapat memberi perlindungan sepenuhnya ke atas data peribadi terutama dalam aplikasi berasaskan web. Ini adalah disebabkan ketidakhadiran pengesahan pengguna dalam sistem dan empunya data (*data subject*) tidak mempunyai kawalan sepenuhnya terhadap maklumat mereka. Kajian ini adalah satu usaha untuk mengatasi masalah ini yang mana sistem *Credential Purpose-Based Access Control (CrePBAC),* diperkenalkan. Sistem ini melaksanakan keselamatan dua-fasa dan mekanisma kawalan capaian dengan satu model dan pelaksanaan polisi keselamatan. Model keselamatan dua-fasa ini melibatkan pengesahan pengguna menggunakan kredential peribadi dan kebenaran data berasaskan tujuan. Polisi keselamatan dan privasi organisasi dilaksanakan menggunakan teknik metadata dalam Pangkalan Data Hippocratic. Teknik metadata menggunakan skim pelabelan data berasaskan tujuan dan mengawal capaian data melalui pengubahsuaian kueri. Model dan mekanisma telah berjaya dilaksanakan. Pengujian ke atas dua jenis kes kajian menunjukkan mekanisma kawalan capaian ini memberikan pengguna hak dan kawalan yang lebih ke atas data mereka. Kesimpulannya, kajian ini telah memperkenalkan pendekatan baru dalam kawalan capaian berasaskan-tujuan dengan model keselamatan dua-fasa dan mekanisme yang memberikan kawalan yang lebih baik bagi melindungi data peribadi dalam aplikasi berasaskan web.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xiii
	LIST OF FIGURES	xv
	LIST OF ABBREVIATIONS	xvii
	LIST OF TERMINOLOGIES	xviii
	LIST OF APPENDICES	xxi
1	**INTRODUCTION**	**1**
	1.1 Preface	1
	1.2 Background of the Problem	3
	1.2.1 The Nature of Web-based Applications	3
	1.2.2 Purpose-based Access Control for Data Privacy	5
	1.2.3 Personal Information and User’s Right	6
	1.3 Problem Statement	7
	1.4 Research Questions	8
	1.5 Research Objectives	9
	1.6 Scope of the Research	10
	1.7 Importance of the Research	11
	1.8 Thesis Outline	12

1.9 Summary 13

2 LITERATURE REVIEW 15

2.1 Introduction 15

2.2 Data Privacy 16

2.2.1 Personal Data Protection 18

2.2.2 Privacy and Data Protection Regulations 20

2.3 Access Control 23

2.3.1 Access Control: Model, Policies and Mechanism 24

2.3.2 Identification, Authentication and Authorization 26

2.3.3 Traditional Access Control Model 27

2.3.4 Problems and Motivations towards Purpose-Based Access Control 29

2.4 Privacy Protection Access Control 30

2.4.1 Hippocratic Database 31

2.4.1.1 Hippocratic PostgreSQL 34

2.5 Purpose-Based Access Control 35

2.5.1 Basic Purpose-Based Access Control 35

2.5.2 Purpose-aware Role-Based Access Control 36

2.5.3 Dynamic Purpose Based Access Control 38

2.5.4 Conditional Purpose Based Access Control 39

2.5.5 Purpose Based Usage Access Control Model 39

2.5.6 Reason Based Access Control Model 41

2.5.7 Assessment Criteria for Privacy Protection Access Control 41

2.5.8 Non Purpose based Access Control 45

2.5.8.1 Self-Managed Access Control 45

2.5.8.2 Cryptography Based Access Control 46

2.5.8.3 Credential-based Access Control 47

2.6 Access Control in Web-based Applications 49

2.6.1 Access Control in E-Health Applications 50

2.6.2 Access Control in E-Learning Applications 51

2.6.3 Access Control in E-commerce Applications 52

2.7 Summary 53

3 **RESEARCH METHODOLOGY** **55**

3.1 Introduction 55

3.2 Research Development Phases 55

3.3 Specifying the Access Control Model and Policies 57

3.3.1 Specification of Access Control Components 57

3.3.2 Modeling the Access Control Model 58

3.3.3 Specify and Deriving the Access Control Policies 59

3.4 Design and Development of Access Control Mechanism 61

3.4.1 System Architecture Design 61

3.4.2 Database Design and Implementation 62

3.4.3 Analysis of Data Labeling Scheme 63

3.4.4 Web-based Applications Prototyping 64

3.4.5 Analysis of Query Modification 66

3.5 Testing and Validation 66

3.6 Summary 67

4 **DESIGN OF ACCESS CONTROL MODEL AND POLICIES** **68**

4.1 Introduction 68

4.2 Requirements for the Development of Credential Purpose -Based Access Control 69

4.3 Specification of Access Control Model Components 72

4.3.1 Users 73

4.3.2 Personal Credentials 74

4.3.2.1 Credential-types of Personal Credential 75

4.3.2.2 Personal Credential Properties 76

4.3.3 Purpose 77

4.3.3.1 Purpose and Purpose Tree 77

4.3.4 Actions 79

4.3.5 Objects 79

4.3.6 Access Decision Evaluation 80

4.4 CrePBAC Access Control Model 80

4.4.1 Definition of CrePBAC Access Control Model 82

4.4.2 User Authentication Phase 84

4.4.3 Data Authorization Phase 85

4.4.4 CrePBAC Access Decision 86

4.5 Specifying and Deriving Access Control Policies 88

4.5.1 Requirement for Access Control Policies Web-based Applications 90

4.5.2 Specifying the Access Control Policies 91

4.5.3 Deriving the Access Control Policy 92

4.5.3.1 Functional Requirements Method 92

4.5.3.2 Data Privacy Needs Method 93

4.5.4 Elements of Access Control Policies 95

4.5.4.1 Access Control Rule 95

4.5.4.2 Access Control Condition 97

4.6 Summary 98

5 IMPLEMENTATION OF ACCESS CONTROL MECHANISM 99

5.1 Introduction 99

5.2 Design Principles for CrePBAC 100

5.3 CrePBAC System Architecture 101

5.3.1 Module 1: Privacy Policy Setting 102

5.3.2 Module 2: Data Collection and Credential Creation 104

5.3.3 Module 3: Data Access Module 107

5.4 Federated Database Design in CrePBAC 110

5.4.1 HDB for CrePBAC 112

5.4.1.1 Privacy Metadata Tables 113

5.4.1.2 Credential Metadata Table 113

5.4.2 User Data 114

5.5 An Implementation of CrePBAC Mechanism 115

5.5.1 A Use Scenario 115

5.5.2 Translating the Privacy Policy using *IBM P3P Tool* 116

5.5.3 Creating the Privacy Metadata Tables 118
5.5.4 Creating the Credential_Metadata 120
5.5.5 Creating the User Database 121
5.5.6 Prototype Implementation 122
5.6 Access Control 122
5.6.1 Data Labeling Scheme 123
5.6.2 Query Modification 126
5.7 Summary 129

6 RESULT AND DISCUSSIONS 131
6.1 Introduction 131
6.2 Query Processing in CrePBAC System 132
6.3 Tests and Validation on CrePBAC Mechanism Implementation 134
6.3.1 Case Study #1 139
6.3.1.1 Case Study #1 with Condition #1 139
6.3.1.2 Case Study #1 with Condition #2 141
6.3.1.3 Case Study #1 with Condition #3 143
6.3.2 Case Study #2 143
6.3.2.1 Case Study #2 with Condition #1 144
6.3.2.2 Case Study #2 with Condition #2 145
6.3.2.3 Case Study #2 with Condition #3 147
6.4 Evaluation of CrePBAC Model and Policies 148
6.4.1 Evaluation on the CrePBAC Model 148
6.4.1.1 CrePBAC Model Evaluation #1 149
6.4.1.2 CrePBAC Model Evaluation #2 151
6.4.2 Evaluation on the CrePBAC Policies 154
6.4.2.1 CrePBAC Policies Evaluation #1 154
6.4.2.2 CrePBAC Policies Evaluation #2 155
6.5 Results of CrePBAC Implementation with Its Design Principles 155
6.5.1 Purpose Specification and Consent 156
6.5.2 Collection Limitation 156

6.5.3 Limited Disclosure 158
6.5.4 Limited Retention 159
6.5.5 Data Subject Right 160
6.6 Comparative Analysis 162
6.7 Summary 162

7 CONCLUSION 165
7.1 Introduction 165
7.2 Research Contributions 166
7.3 Future Works 172
7.4 Conclusion 173

REFERENCES 175
Appendices A-E 184-191

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	A Summary of Privacy Regulations	21
2.2	A Comparative Analysis of Purpose-based Access Control Model	44
4.1	Policies for Customer	94
4.2	Access Control Conditions for Access Control Rules	97
5.1	Privacy Metadata Schema	113
5.2	Credential Metadata Schema	114
5.3	Database Schema for Online Bookstore	114
5.4	*privacy_authorized* Table	119
5.5	*privacy_policy* Table	119
5.6	*credential_metadata* Table	120
5.5	A Part of *customer* Table	121
5.7	*customer* Table with Cell-level Labeling Scheme	125
6.1(a)	*transaction* Table	135
6.1 (b)	*customer* Table	136
6.2	Access Decision Evaluation	139
6.3	Query Processing for Case Study #1 with Condition #1	140
6.4	Result for Case Study #1 with Condition #1	141
6.5	Query Processing for Case Study #1 with Condition #2	142
6.6	Query Processing for Case Study #1 with Condition #3	143
6.7	Query Processing for Case Study #2 with Condition #1	144
6.8	Result for Case Study #2 with Condition #1	145
6.9	Query Processing for Case Study #2 with Condition #2	146
6.10	Query Processing for Case Study #2 with Condition #3	147

6.11 User Authentication Process for Case Study #1 with Condition #1 149
6.12 Data Authorization Process for Case Study #1 with Condition #1 149
6.13 User Authentication Process for Case Study #2 with Condition #2 151
6.14 Data Authorization Process for Case Study #1 with Condition #2 152
6.15 Result for DML *Insert* Operation 157
6.16 Result for Collection Limitation Principle 158
6.17 Result for Limited Disclosure Principle 159
6.18 Result for Data Subject Right Principle 161
6.19 A Comparative Analysis of CrePBAC system with PBAC systems 163

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Data Security Research Area	17
2.2	Relations among Access Control Models, Access Control Policies and Access Control Mechanisms (Hwang e*t al.*, 2010)	25
2.3	HDB Strawman Architecture (Agrawal *et al.*, 2002)	32
2.4	Hippocratic Postgre SQL Architecture (Padma *et al.*, 2009)	34
2.5	Purpose and Purpose Tree	36
2.6	PURBAC Family Model (Masoumzadeh *et al.*, 2008)	37
2.7	Dynamic Purpose-based Access Control Model (Peng *et al.*, 2008)	38
2.8	Authorization Model (Sun *et al.*, 2010)	40
2.9	Credential Based Access Control	48
3.1	Research Development Phases	56
3.2	Two Phases in Access Control Process	59
3.3	Three Tiers in Web-based Applications	65
4.1	Six Components in CrePBAC Model	73
4.2	An Example of Individual Attributes	74
4.3	Credential-types Hierarchy for *customer*	75
4.4	Credential Profiles for *customer*	76
4.5	An Example of Purpose Tree for Online Purchasing	78
4.6	CrePBAC Access Control Model	82
5.1	CrePBAC System Architecture	102
5.2	Credential Translator Module	106
5.3	User Authentication Process	108
5.4	Data Authorization Process	109
5.5	Access Decision Point	110
5.6	CrePBAC Federated Databases	111

5.7 HDB for CrePBAC 112

5.8 Three Files Created using *IBM P3P Tool* 117

5.9 Uploading Three Files into w3c Server Folder 117

5.10 Query Modification Algorithm 127

5.11 User’s Interaction with the Database System Using Query Modification 129

6.1 Steps in Processing a High-level Query (Elmasri and Navathe, 2007) 133

6.2 CrePBAC Query Execution 133

6.3 Flowchart for Access Decision Process 137

6.4 Actual Result for Case Study #1 with Condition #1 for ABC Online Bookstore 141

6.5 Actual Result for Case Study #2 with Condition #1 for ABC Online Bookstore 145

6.6 An Example of Privacy Policy Created in *privacy_metadata* Tables 160

LIST OF ABBREVIATIONS

CrePBAC	-	Credential Purpose-Based Access Control
DAC	-	Discretionary Access Control
DBMS	-	Database Management System
DML	-	Data Manipulation Language
HDB	-	Hippocratic Database
MAC	-	Mandatory Access Control
MySQL	-	My Structured Query Language
MPDPA	-	Malaysia Personal Data Protection Act
OECD	-	Organization Of Economic Cooperation And Development
P3P	-	Platform for Privacy Preferences
PBAC	-	Purpose Based Access Control
PHP	-	Personal Home Page
PURBAC	-	Purpose-Aware Role-Based Access Control
RBAC	-	Role-Based Access Control
SQL	-	Structured Query Language
W3C	-	World Wide Web Consortium
WWW	-	World Wide Web

LIST OF TERMINOLOGIES

Access Control

a process of mediating every request to resources and data maintained by a system and determining whether the request should be granted or denied

Access Control Mechanism

a technique defines the functions that implement the controls imposed by the policy and formally stated in the model

Access Control Model

a written model to describe properties of access control that provides a formal representation of the access control policy and its working

Access Control Policy

a high-level requirements for specifying access control for any organizations must be regulated

Access Purpose

a purpose for accessing data, is a reason for accessing a data item, and it must be determined by the system when a data access is requested

Action

a right that users can be granted to access on the tables exist in the database.

Authentication

a process used to verify whether the claim of identity is correct or not

Authorization	a process of assigning authenticated subjects access and the right to carry out specific operations, depending upon their preconfigured access rights and permissions outlined in an access control policies
Credential-type	a hierarchy that determines the properties of the personal credential certifies
Data labelling scheme	a unit of data with which purposes can be associated.
Data usage purpose:	a specified usages for which data objects are accessed
Discretionary Access Control	a policy control access based on the identity of the requestor and on access rules stating what requestors are (or are not) allowed doing
Hippocratic Database	a concept of database technology that incorporate privacy protection as a founding tenet in relational database systems
Identification	an activity of the subject supplying information to identify itself
Mandatory Access Control	a policy control access based on mandated regulations determined by a central authority
Object	a table and views of the personal database that being protected
Personal Credential	an attribute belongs to a specific person

Personal Information
any information that can be used to identify a person such as name, address, telephone number

Privacy
a right of an individual, group or institution to determine when, how and for what purpose information concerning himself/itself can be collected, stored and released to other people or entities

Purpose
a reason of data collection or data access

Purpose-based Access Control
an access control system that use the concept of purpose is used as the basis of access control policy

Query Modification
a technique that modifies the queries in order to prevent the release of personal information to unauthorized users

Role-based
an control access depending on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

User
an individual who own the data and also an individual who access and receive the access

Web-based application
an application that is accessed over a network such as the Internet or an intranet.

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Refer to Personal Data Protection Bill 2009	184
B	Ten Guiding Principles of HDB	185
C	Three Basic Processes Involved in Online Purchasing	186
D	Steps Creating the policy file, reference file and html file using IBM P3P	188
E	Limited Retention Principle Code	191

CHAPTER 1

INTRODUCTION

1.1 Preface

Organizations have increased their adoption of database systems as a key data management technology for their day-to-day operations and decision makings. There is an increasing growth of web-based applications and information systems operating in open environments. Therefore, the security of data, especially personal data managed by these systems becomes crucial (Dagdee and Vijaywargiya, 2009b). Besides that, there has been a further increased in the risk exposures of databases. This demands for a more secure database systems than before due to the importance of data security requirements. In addition, Bertino and Sandhu (2005) identifies that securing databases in open environments are more challenging where data can be accessed anytime and from almost anywhere.

The existence and the rapid development of the World Wide Web (WWW) on the internet have literally transformed people lives in recent years. Web-based applications enable people to carry out their business activities virtually any time and from any place such as online shopping, electronic banking and even learning through online. These applications also provide the capabilities to collect and store many types of information related to personal and individuals in the course of the business activities. Every day, organizations are entrusted with the responsibility of collecting and managing many types of personal information including names, e-mail addresses, home addresses, genders, believes and the like from users. Indeed, a study conducted by the Federal Trade Commission in May 2000 (ANSI, 2004) shows that 97 percent of web sites were collecting at least one type of identifying information such as name, e-mail address, or postal address of consumers.

However, personal information once collected and stored, if used without any concern or awareness of its importance will create fear for privacy violation for users and many other people (Byun and Li, 2008). On the other hand, easy access to personal data poses a threat to individual privacy. More and more privacy related incidents occurs (Anton *et al.*, 2004; Chung and Paynter, 2002), individuals are afraid that their personal information might fall into the wrong hands and be abused against their will. Ceruti (2005) stated that data privacy becomes an issue when users are not comfortable to disclose their personal information even though it is needed. Easy access to personal information will cause the misuse of data, less control over their information, and many others. Furthermore, the rapid advances in database management systems and information technology have greatly increased the awareness of the need for protecting data especially personal data in the databases.

Data privacy issues become more important especially when it involves data relating to a person are collected, used and stored easily in databases. The challenge is to share data and at the same time able to protect these types of data. Therefore, personal data stored in the database must be protected from being accessed by unauthorized users. This personal data protection approach is known as access control. Access control is an approach when users try to access a data object, it will check the rights that the users have again a set of authorizations, stated usually by some security administrator (Bertino *et al.*, 2005). Protecting data in the databases can also be done through the use of specially designed databases called Hippocratic Databases (HDB). HDB is a new concept of databases introduced by Agrawal *et al.* (2002) with the objective of focusing on protecting the privacy of the individuals whose personal information are contained in the databases. The concept of purpose has been widely used in proposing an access control based on purpose. Observing these challenges in protecting the personal data, the concept of purpose must play a major role in controlling access towards personal data in the open databases.

In line with the above view, this research is to provide an appropriate approach in controlling the access with the purpose to protect personal data stored in open databases from unauthorized access. The research will consider various issues of data security and privacy with special emphasis on access control approach in protecting personal data stored in open databases.

This research work focuses on the requirements of data security and privacy. It emphasizes on controlling the access towards personal data in order to protect these type of data stored in open databases. The purpose of this research is to propose an access control model and then, is enforced by the implementation of an appropriate access control mechanism to provide high-assurance and confidentiality of personal data. With the brief introduction on personal data protection inside databases, Section 1.2 describes the background of the problem while Section 1.3 presents the problem statement. Section 1.4 develops the research questions which were derived from previous section. The objectives of the research are explained in Section 1.5 and Section 1.6 provides the scope of the research. Section 1.7 overviews the importance of the research that need to be considered. The outline of the research is given in Section 1.8, and Section 1.9 gives the summary of this chapter.

1.2 Background of the Problem

Discussions started by looking at the scenario in web-based applications which emphasize on current problems in access control. Then, this section continues the discussions on purpose-based access control in supporting data privacy. Finally, this section also discuss on the subject of personal information protection which it concentrates on the rights that users have regarding their own data.

1.2.1 The Nature of Web-based Applications

The ability of web-based applications to be accessed anytime, anywhere and by anyone is essential in modern economy but at the same time require higher security especially when being accessed by many unknown parties in the open environment. The most commonly used access control methods are based on identity and role based authentication which makes the system unsuitable for open access (Dagdee and Vijaywargiya, 2009b). This is caused by in web-based applications such as e-commerce, data access is required by anyone spontaneously. This traditional access control approach; known as identity-based authentication where it is assumed that the users are known to the provider through a process of registration. Bertino and Sandhu (2005) also claimed that the use of identity mechanism which is based on login and user names for qualifying the subjects to which a policy applies are no longer appropriate in that they would require the specification and management of large number of policies.

Dagdee and Vijaywargiya (2009a) stated that the major challenge is when in open environments; the requesters are not being identified by unique names but are identified by their attributes to gain access to resources. For example, requesters being proved as an owner of the information are more important rather than their identity in order to provide them an access on their personal data inside databases. Here, the requesters are required to submit the proof of ownership of personal data. The open and dynamic natures of these web-based applications require the development of secure access controls for protecting personal data (Ardagna *et al.*, 2010). These include implementing appropriate access mechanisms that will complement the confidentiality and privacy of personal information. Consequently, these models and its mechanism allow deciding which requesters are qualified to gain access to the personal data. On the other hand, which server is trusted to provide the requested personal data, on the basis of certified statements provided by the interacting parties is needed. For this purpose, Bertino and Sandhu, (2005) suggested that there is a need to use a more flexible user specification mechanism rather than user identity itself when determining the access decision. User specification mechanism based on user credential and profiles such as nationality, job position can be used besides their login names during the specification and enforcement of access control policies.

The expansions of web-based applications have heightened the need for the development of secure databases with the ability to protect the personal data. Both model and its mechanism are important in controlling accesses towards personal data in databases. There is a growing need for development of access control models and appropriate mechanism with the architectural design in protecting the personal data inside open databases. Accordingly, it realize the open access systems that enable easy access to personal data in web-based applications which this research about.

1.2.2 Purpose-based Access Control for Data Privacy

Access control is one of the fundamental security mechanisms for information systems. Access control enables us to manage the access at a very granular level. Today, even though data privacy becomes a major concern for both users and organizations, but, traditional access control such as Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-based Access Control (RBAC) cannot easily be used in achieving the personal data protection Yang *et al.* (2008). According to Chauduri *et al.* (2011), access control designed to protect personal data should focused on privacy policy that concerned with which data is used for which purpose. Unfortunately, traditional access control models focus on which user is performing which action on which data object.

Kabir and Wang (2009) pointed out the first reasons that privacy protection cannot be easily achieved by traditional access control as traditional access control such as RBAC focuses on which user is performing which action on which data object, but a reliable access control for protecting personal data is concerned with which data object is used for what purpose. According to Byun *et al.* (2005), in order to protect personal data stored in databases, the notion of purpose must play a major role in access control models. Due to this, more and more researches have been done in purpose based access control (PBAC) which was motivated by HDB (Byun *et al.*, 2005; Masoumzadeh and Joshi, 2008; Sun and Wang, 2010). Section 2.5 will discuss further on PBAC.

1.2.3 Personal Information and User's Right

Concern of privacy is an important issue for individuals when discussing on personal information. Privacy is closely related with personal data and its protection. Both privacy and personal information protection scope are directly related in this research. In the context of personal information, privacy is defined as an ability to control collection, retention and distribution of personal information that belongs to them (Goldberg *et al.,* 1997). Through web-based applications, organizations will collect various types of personal information and will use it for various purposes. This may leads to concern that personal information may be misused.

Privacy protection is a fundamental personal right of all individuals. Individuals have a right to expect that organizations will keep their personal information confidential. One way to ensure this is by requiring the organizations to collect, maintain, use, and disseminate personal information only as necessary to carry out their functions. In other words, organizations should be able to ensure that personal information contained in their databases is securely protected. This research is closely related with these issues since it proposes an appropriate data protection approach to ensure personal information privacy. One of the main challenges regarding personal data protection is to share this information while complying with data owner privacy preferences.

Besides data protection, users should be provided with their right and control towards own personal data stored in databases which is also will be highlighted in this research. Westin (1967) stated that users disagree when they lost all control over how personal information is collected and used by companies when using online transactions. According to Gates and Slonim (2003), it is not sufficient for users to own their personal information but they must be able to control access to this information. However, the difficulty that arises is when this information cannot be controlled by any technological means. As owners, users must have their right to their own information. The idea of users having control on access to their data when it stored in e-form has been viewed as a right (Barker, 2010). Right enable the owner (also known as data subject) of the data that it belongs, should be able to access their own information regardless for what purposes. As an owner of the data, they should have the control towards their own personal information either to access, update or delete their data. They should be able to access and participate in whatever data belongs to them stored in a database.

1.3 Problem Statement

Previous discussion has covered the background of the data privacy focusing on the importance of protection towards personal data stored in open databases and database management system (DBMS). Privacy has become an important requirement in any web-based applications and information systems that deal with personal data. Any personal data must be protected not only from unauthorized user but also from unauthorized access. According to Greenstadt and Smith (2005), once an individual chooses to release some portion of his or her personal information, individual must then rely on laws or mechanisms to control further distribution and subsequent use of that information.

Bertino *et al.* (2011) presents an access control as one of the available approaches in protecting personal data stored in the databases. According to Chauduri *et al.* (2011), through access control, the system can restrict the access to authorized users only and it can guarantee the protection of the data object. But there are several issues regarding the protection of personal data inside a database that arise with current access control system. From the previous discussion, this research has summarized the following issues:

- The use of traditional identity mechanisms for qualifying the users to which policy applies is no longer appropriate in that they would require the specification and management of a large number of policies,
- Traditional authorization based on roles and data objects does not fully support privacy and personal data protection. However, personal privacy and its data protection is the main concern in this research,
- Less control and participation from users towards their personal data once released via web-based application,

- Current access controls based on purpose does not support personal data protection especially user's right for web-based applications in open environment.

All of the above issues have led to the problem statement as follows:

> Traditional access controls cannot fully protect personal information stored in databases. The current purpose-based access control systems are also insufficient to protect personal data in web-based applications. In these types of applications, data subjects will also lose their right and control over their personal information released. How then can we formulate a solution to control access to personal information in web-based applications and its databases while ensuring personal data is protected and data subjects have full control over their personal data once released.

1.4 Research Questions

Based on the problem statement identified in Section 1.3, the following research questions have been formulated.

- What are the requirements that need to be considered when designing an access control model with the purpose to protect personal data in an open environment?
- How to design and implement the access control mechanism to enforce the access control policies in an open database for the protection of personal information?
- How to test and validate the new access control model, policies and mechanism for protecting personal information in open databases for web-based applications?

From the above research questions, the effort of this research is to introduce a new access control model and implement the access control mechanism in order to enforce the access control policies with the purpose to protect the personal data stored in an open database. The proposed access control system should be able to solve the current problems and issues of personal data protection as stated in Section 1.3. This research presents an access control for open database system that has the following characteristics in order to fulfill the privacy requirements introduced by Ardagna *et al.* (2006):

- Open: Allow unknown individual who able to prove as an authorized user to access personal data stored in the databases,
- Fine-grained: Provide an access control at a cell-level in order to protect other data
- Customizable: Allow individuals whose personal information is stored in the database to control and provides their preferences regarding their personal data stored in a database,
- Transparent: Make the query processing as transparent as possible, so that users know the data protection mechanisms available.

1.5 Research Objectives

The main objective of this research is to propose an access control system for protecting personal data stored in open databases and achieving the confidentiality requirement of data security.

The specific objectives of this research are:

i) to study the current issues in access control models and mechanisms for protecting personal information in web-based applications,

ii) to design and develop an access control model in an open environment that can support the protection of personal information,

iii) to design, develop and evaluate the access control mechanism in an open database for the purpose of protecting personal data in web-based applications.

1.6 Scope of the Research

In order to ensure that this research achieves its objectives within the stipulated timeframe, it is necessary to state the scope of the research. Firstly, this research is mainly concerned with protecting personal data stored in open databases. Guarda and Zannone (2009) introduced four types of data based on EU Directive, that is personal data, sensitive data, identification data and anonymous data. This research take into account three types of data which involves personal data, sensitive data and identification data where these data are associates with personal data types. Secondly, the purpose of this research is to protect personal data stored in the open databases. Although there are many available mechanisms to protect personal data such as data access control, encryption and using digital signatures (Bertino *et al.,* 2011), but this research focuses on access control. Thirdly, this research concentrates on user's rights towards their personal data stored in open databases. Even though there are other types of users described by Guarda and Zannone (2009), data subject is the main concern in this research. Data subject is the person who owns the data, which also refers as user. Users and data subjects will be used interchangeably throughout this research.

This research considers a complete solution for access control system must contain model, policies and mechanism. However, specifying and deriving the access control policies in web-based applications is a complex process because different organizations have set up a different privacy policies (Bhavani *et al.*, 2002). Due to this complexity, this research will not take into account the access control policy aspect. Yet, a set of assumptions on access control policies were made for the purpose of implementing the access control mechanism.

The final concern in this research is regarding the trust management in web-based applications. Trust is considered as an important feature in web-based applications. There are two aspects of trust in web-based applications, *i)* users established a trust with the system and willing to use the system and *ii)* users are considered as trusted parties and being allowed to use the system. Since this research focuses on controlling the access from unauthorized user towards personal data stored in web-based application, hence this research consider the second aspect that is, users are considered as trusted parties and being allowed to use the system. However, this research will not consider the trust aspect in web-based applications. For this reason, an assumption was made where users who are successfully authenticated to the system is also considered as trusted user to the system. This assumption indicates that all transactions occurred between users and service providers are considered as trusted communications once users are authenticated to the system.

1.7 Importance of the Research

Since the invention of the WWW in 1989, web-based applications have been transformed from a simple idea into reality. In these types of applications, personal information is collected, used, stored and disclosed for various types of business purposes. Today, there are a lot of personal information breaches happen around the world. An example of the breach happened when Citigroup admitted on June 8, 2011 (Gogoi, 2012), that an attack on its website allowed hackers to view customers' names, account numbers and contact information such as email addresses for about 210,000 of its cardholders in North America. Because of this breaches, privacy concerns towards personal data are become more important than before.

Privacy and personal data protection is a critical issue in web application since most data involved are about individual who is highly sensitive and private (Olivier, 2002). Inappropriate disclosure or misuse of those data will cause the privacy problems not only to individuals but also for organizations which in turn lead to serious problems. Thus, data protection is more important today. Therefore, more and more personal data acts have been introduced by countries in order to protect the personal information. The main purpose of these acts is to protect users' personal data, particularly after it was revealed to third parties. In addition, most of the acts protect the rights that users have regarding their own data as summarized in Table 2.1 in Section 2.2.2. As mentioned earlier, the enforcement of the data protection alone couldn’t solve the problem arise (Agrawal *et al.,* 2002). It should come together with the implemented technology to support these acts. These have led us to this research.

From the above explanation, it is clearly defined that this research is very much relevant and its importance can be re-stated as follows:

- To solve the problem of protecting personal information that is stored in the database as exposed through web-based applications,
- To provide an appropriate model and mechanism for controlling access towards personal data in databases,
- To design and implement an open database with the user's ability to control and have rights to their personal information.

1.8 Thesis Outline

The main purpose of this research is to propose a model and its mechanism for controlling the access towards personal data stored in databases via web-based applications. As such, this thesis shall present each component that contributes to the development of the research.

Chapter 2 provides a detailed review on the body of knowledge related to protection of personal data through access control mechanism. The discussion covers data privacy and its protection approaches. The chapter also presents the available privacy protection access control model for protecting personal data in open database system. An analysis on several access controls based on purpose was conducted in the aspects of features, strengths and weaknesses. A brief explanation on HDB is also given here.

Chapter 3 describes the research methods and procedures followed in conducting this research. The chapter presents the discussion of the research development phases which were conducted in this research.

Chapter 4 covers a details explanation on designing the access control model. The discussions start with a discussion on how the access control components were derived from a set of requirements that have been identified earlier. Then, the access control model was developed based on these components. Besides that, the specification of access control policies with two elements that is, access control rules and access control condition are also defined in this chapter.

Chapter 5 presents the implementation of access control mechanisms in order to enforce the access control policies which have been specified in the previous chapter. Federated database has been developed using the concept of HDB. The chapter describes the system architecture, design and implementation of the mechanism. Also discussed in this chapter is two implementation approaches in access control which is data labeling scheme and query modification technique.

Chapter 6 discusses the results obtained from testing and validation. The purpose of testing is to validate the access control system in terms of accuracy and validity. An evaluation is required to ensure that the proposed access control system developed is able to protect personal data when disclosed it via web-based applications.

Chapter 7 provides a summary of the research and highlights the research contributions and limitations exist in this research. In addition, some suggestions for future work are also given in this chapter. Finally, this chapter also concludes the research.

1.9 Summary

The advance use of database technology in web-based applications has increased data privacy concern. More and more data especially personal data are being collected, used and stored in these open databases. However, the collection of these types of data may cause various problems not only for the users itself but also for organizations. Due to this, data protection has increasingly important when individuals are more concern about the privacy of their data, especially when the disclosed it via web-based applications. The next chapter will discuss in detail the literature review done for this research purposes.

REFERENCES

Afyouni, H. A. (2006). *Database Security and Auditing: Protecting Data Integrity and Accessibility*. Boston, Massachusetts: Thomson Course Technology.

Agarwal, S., Sprick, B., and Wortmann, S. (2004). Credential Based Access Control for Semantic Web Services", *American Association for Artificial Intelligence*.

Agrawal, R., Bird, P., Grandison, T., Kiernan, J., Logan, S. and Y. Xu. (2005). Extending relational database systems to automatically enforce privacy policies. *Proceedings of the 21st International Conference on Data Engineering,* 1013-1022.

Agrawal, R., Evmievski, A., and Srikant, R. (2003). Information Sharing Across Private Databases. *In Proc. of The 2003 ACM SIGMOD Int. Conf. on Management of Data.* ACM Press.

Agrawal, R., Kiernan, J. and Srikant, R. (2002). *Hippocratic Database.* Proceedings of the 28th International Conference on Very Large Data Bases, 143-154.

Al-Fedaghi, S. S. (2005). Privacy as a Base for Confidentiality. *Proceedings of the 5th WSEAS International Conference on Applied Informatics and Communications*, 7-15.

Al-Fedaghi, S. (2007). Beyond Purpose-Based Privacy Access Control. 18th *Australasian Database Conference (ADC 2007), Ballarat, Australia. Conferences in Research and Practice in Information Technology*. 63.

Anciaux, N., Bouganim, L. and Pucheral, P. (2006). Data Confidentiality: To Which Extent Cryptography and Secured Hardware Can Help. ANN. Telecommunication 61(3-4), 267-283.

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

Anton, A., He, Q. and Baumer, D. L. (2004). Inside JetBlue's privacy policy violations. *Proceedings of the IEEE Security and Privacy*. 2(6), 12-18.

Ardagna, C. A., Damiani, E., di Vimercati, S. D. C., Foresti, S. and Samarati, P. Trust Management. In: Petkovic, M and Jonker, W. *Security, Privacy, and*

Trust in Modern Data Management. Berlin/DE. Springer-Verlag Berlin and Heidelberg GmbH & Co. KG. 103; 2010

Ardagna, C. A., Damiani, E., di Vimercati, S. D. C. and Samarati, P. (2006). Enhancing User Privacy Through Data Handling Policies. *Data and Applications Security XX. Lecture Notes in Computer Science*. 4127, 224-236.

Baraani-Dastjerdi, A., Pieprzyk, J. and Safavi-Naini, R. (1996). Security In Databases: A Survey Study

Barker, S. (2010). Personalizing Access Control by Generalizing Access Control. *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies.* 149-158.

Bedi, R. K. and Thengade, A. M. (2010). Purpose-based Access Control Exploits by HDB. *International Journal of Computer Applications.* 1(6). 87-91.

Bertino, E. (2005). Purpose Based Access Control for Privacy Protection in Database Systems. *Database Systems for Advanced Applications. Lecture Notes in Computer Science,* 3453, 1003-1007.

Bertino, E., Byun, J. W. and Li, N. (2005). Privacy-Preserving Database Systems. *Foundations of Security Analysis and Design III, Lecture Notes in Computer Science*. 3655: 178-206.

Bertino, E., Ghinita, G. and Kamra, A. (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.

Bhavani. T, Clifton, C., Gupta, A., Bertino, E. and Ferrari, E. (2002). Directions for Web and E-Commerce Applications Security (October 2002). MIT Sloan Working Paper No. 4259-02; Eller College Working Paper No. 1021-05. Available at SSRN: http://ssrn.com/abstract=333682 or http://dx.doi.org/10.2139/ssrn.333682

Borcea, K., Donker, H., Franz, E., Pfitzmann, A. and Wahrig, H. (2006). Towards Privacy-Aware eLearning. *Privacy Enhancing Technologies Lecture Notes in Computer Science.* 856, 167-178.

Bouganim, L. and Guo, Y. (2010). Database Encryption. Encyclopedia of Cryptography and Security. (2nd ed.) Springer.

Braghin, S., Coen-Porisini, A., Colombo, P., Sicari, S. and Trombetta, A. (2008). Introducing Privacy in a Hospital Information System. *Proceedings of The 4th International Workshop on Software Engineering for Secure Systems*. 9-16.

Byun, J. W. (2009). Toward Privacy-Preserving Database Management Systems – Access Control And Data Anonymization. PhD. Thesis. Purdue University; 2007.

Byun, J. W., Bertino, E. and Li, N. (2005). Purpose Based Access Control of Complex Data for Privacy Protection. *Proceedings of 10th ACM Symposium on Access Control Models and Technologies.* 102-110.

Byun, J.-W. and Li, N. (2008). Purpose Based Access Control for Privacy Protection in Relational Database Systems. *The International Journal on Very Large Data Bases*, 17(4), 603 - 619.

Camenisch, J., Modersheim, S., & Neven, G. (2009). Credential-Based Access Control Extensions to XACML, www.w3.org/2009/policyws/papers/Neven.pdf.

Castano, S. and Ferrari, E. Protecting Datasources Over the Web: Policies, Models, and Mechanisms. In: Tanian, D. *Web-Powered Databases.* Idea Group Inc. 299: 2003.

Castano, S., Fugini, M., Martella, D., and Samarati, P. (1995). *Database Security*. Wokingham, England: Addison-Wesley Publishing Company.

Ceruti, B. A. (2005). *Personal Privacy and Database Technology*. Paper presented at the 21st Computer Science Seminar.

Chauduri, S., Kaushik, R., and Ramamurthy, R. (2011). Database Access Control & Privacy: Is There A Common Ground. *Proceedings of the 5th Biennial Conference on Innovative Data Systems Research*. January 9-12. Asilomar, California, USA, 2010. 96-103.

Chung, W. and Paynter, J. (2002). Privacy issues on the Internet. *Proceedings of the 35th Hawaii International Conference on System Sciences*.

Culnan, Mary J. 2000. Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy and Marketing*, 19 (1) : 20-26.

Culnan, Mary J., and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. Organization Science, 10 (1): 104-115.

Dagdee, N., and Vijaywargiya, R. (2009a). Access Control Methodology for Sharing of Open and Domain Confined Data using Standard Credentials. *International Journal on Computer Science and Engineering.* 1(3), 148-155.

Dagdee, N. and Vijaywargiya, R. (2009b). Credential Based Hybrid Access Control Methodology for Shared Electronic Health Records. *International Conference on Information Management and Engineering*. 3-5 April. S.D. Bansal Coll. of Technol., Indore. 624-628.

Damiani, E., di Vimercati, S.D.C., and Samarati, P. (2005). New Paradigms for Access Control in Open Environments. *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology*, 2005. 21-21 Dec. 2005. Milan, 54-545.

Didriksen, T. (1997). Rule Based Access Control – A Practical Approach. *Role Based Access Control 1997.* 143-151.

Di Vimercati, S. D. C., Foresti, S., Jajodia, S., and Samarati, P. (2007). Access Control Policies and Languages in Open Environments. *Advances in Information Security*.

Di Vimercati, S. D. C., Foresti, S. and Samarati, P. Authorization and Access Control. In: Petkovic, M and Jonker, W. *Security, Privacy, and Trust in Modern Data Management*. Berlin/DE. Springer-Verlag Berlin and Heidelberg GmbH & Co. KG. 39; 2010

Di Vimercati, S. D. C., Foresti, S. and Samarati, P. (2002). Recent Advances in Access Control. *Proceedings of the Fifteenth Annual Working Conference on Database and Application Security*. 3 – 15.

Dwivedi, S., Menezes, B., and Singh, A. (2005). Database Access Control for E-Business – A case study. *Advances In Data Management*. 168-175.

El-Khatib, K., L. Korba, et al. (2003). Privacy and Security in E-Learning. *International Journal of Distance Education.* 1(4).

Elmasri, R., and Navathe, S. B. (2007). *Fundamentals of Database Systems*. (5th ed.) Addison-Wesley.

Evered, M. and Bogeholz, S. (2004). A Case Study in Access Control Requirements for a Health Information System. *Proceedings of the 2nd Australian Information Security Workshop*. 32, 53-61.

Ferrari, E., and Bhavani, M. T. (2004). Security and Privacy For Web Databases And Services. In: Proceedings of the 9th International Conference on Extending Database Technology, LNCS 2992, pp. 17-28. Springer, New York (2004).

Gates, C., and Slonim, J. (2003). Owner Controlled Information. Proceedings of the 2003 Workshop on New Security Paradigms.

Goffman, Erving. 1961. The Presentation of Self in Everyday Life. New York: AnchorDoubleday.

Goldberg, I., Wagner, O. and Brewer, E. (1997). *Privacy-Enhancing Technologies for the Internet.* Paper presented at the IEEE COMPCON '97.

Goldschlag, D, Reed, M. and Syverson, P. (1999). Onion routing for anonymous and private Internet connections. *Communications of the ACM.* 24(2), 39–41.

Gogoi, P (2012). What The Citigroup Data Breach Means For Credit Card Users. Retrieved on June 11, 2012, from http://www.huffingtonpost.com/2011/06/11/citigroup-hack-credit-card-users_n_875417.html

Graf, F. (2002). Providing security for eLearning. *Computers & Graphics.* 26(2): 355 - 366.

Grandison, T., Johnson, C., and Kiernan, J. (2008). Hippocratic Databases: Current Capabilities and Future Trends. In *Handbook of Database Security* (pp. 409-429): Springer US.

Greenstadt, R., and Smith, M. D. (2005). Protecting Personal Information: Obstacles and Directions. *Proceedings of the Fourth Annual Workshop on Economics and Information Security, Cambridge, Massachusetts, May 2005*.

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 Companies.

He, Q. (2005). *Requirements-Based Access Control Analysis and Policy Specification*. Doctor of Philosophy, North Carolina State University.

Hung, P. C. K. (2005). Towards a Privacy Access Control Model for E-Healthcare Services. *Proceedings of the 3rd Annual Conference on Privacy, Security and Trust*.

Hwang, J., Martin, E., Xie, T., and Hu, V. C. (2010). Policy Based Testing. *Entry in Encyclopedia of Software Engineering*, 673-683.

Jajodia, S. (1996). Database Security and Privacy. *ACM Computing Surveys,* 28(1), 129-131.

Kabir, M. E. (2009). Access Control Management and Privacy-Preserving. PhD. Thesis. University of Southern Queensland; 2009.

Kabir, M. E., and Wang, H. (2009). Conditional Purpose Based Access Control Model for Privacy Protection. *Proc. 20th Australasian Database Conference*. 92, 135-142.

Katt, B., Breu, R., Hafner, M., Schabetsberger, T., Mair, R., and Wozak, F. (2008). eHealth 2008, September 8th and 9th, 2008.

Kobsa, A. (2000). Personalized hypermedia and international privacy. *Communications of the ACM.*

LeFevre, K., Agrawal, R., Ercegovac, V. and Ramakrishnan, R. (2004). Limiting Disclosure in Hippocratic Databases. *Proceedings of the Thirtieth International Conference on Very Large Data Bases*. 30, 108-119.

Laura-Silva, Y and Aref, W. G. (2007). Realizing Privacy-Preserving Features in Hippocratic Databases. Proceedings of the 2007 IEEE 23rd International Conference on Data Engineering Workshop, 198-206**.**

Lu, S., Hong, Y., Liu, Q., Wang, L. and Dassauli, R. (2008). Securing Telehealth Applications in a Web-Based e-Health Portal. *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security*, 3-9.

Malaysia (2009). *Malaysia Personal Data Protetcion Act.* D.R. 35/2009.

Masoumzadeh, A. and Joshi, J.B.D. (2008) PuRBAC: Purpose-Aware Role-Based Access Control. *Proceedings of the OTM 2008 Confederated International Conferences*. 1104-1121.

Mattsson, U. T. (2005). Database Encryption-How to Balance Security with Performance. February 25, 2005.

Matysiewicz, J. and Smyczek, S. (2009). Consumer Trust– Challenge for E-Healthcare. *Fourth International Conference on Cooperation and Promotion of Information Resources in Science and Technology*. 333-338.

Maurer, U. (2004). The Role of Cryptography in Database Security. *Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data*. 5-10

Mohammad, A., Khdour, T., Kanaan. and G. Kanaan. (2011). Ontology-Based Access Control Model for Semantic Web Services. *Journal of Information and Computing Science.* 6(3), 177-194.

Mohammad, A., Khdour, T., Kanaan., G. Kanaan. And Ahmad, S. B. (2011). Analysis of Existing Access Control Models from Web Services Applications's Perspective. *Journal of Computing.* 3(3), 10-16.

Mohania, M., Ananthanarayanan, R., Gupta, A. (2007). Some Issues in Privacy Data Management. *Data & Knowledge Engineering.* 63: 591–596.

Noninska, I. (2003). Access Control and Management in B2C Model of Electronic Commerce. *Proceedings of International Conference on Computer Systems and Technologies.* 391-394.

Organization for Economic Co-operation and Development. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980. Available at www1.oecd.org/publications/e-book/9302011E.PDF.

Olivier, M. S. (2002). Database Privacy Balancing Confidentiality, Integrity and Availability. *ACM SIGKDD Explorations Newsletter 4*(2), 20-27.

Padma, J., Silva, Y. N., Arshad, M. U., & Aref, W. G. (2009). *Hippocratic PostgreSQL*. IEEE International Conference on Data Engineering 09. 1555 – 1558.

Park, J. and Sandhu, R. (2002). Towards Usage Control Models: Beyond Traditional Access Control. *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies.* 57-64.

Peng, H., Gu, J., & Ye, X. 2008. Dynamic Purpose-Based Access Control. *Proceedings of the International Symposium on Parallel and Distributed Processing with Applications 08.* 695-700.

Pernul, G. (1994). Database Security. *Advances in Computers*, 38, 1-74.

Porter, P. A. Trust Negotiation for Open Database Access Control. Master of Science. Thesis. Brigham Young University; 2006

Potts, C. (2001). What is privacy? *North Carolina State University E-Commerce Seminars*, October. Available at http:// theprivacyplace. org/presentations/ ncsu01slides.pdf.

Rezgui, A., Bouguettaya, A. and Eltoweissy M. Y. (2003). Privacy on the Web: Facts, Challenges, and Solutions. *IEEE Security & Privacy*. 40-49.

Sandhu, R., Ferraiolo, D. and Kuhn, R. The NIST Model for Role-based Access Control: Towards a Unified Standard. In Proceedings of the 5th ACM Workshop on Role Based Access Control, Berlin, Germany, Jul 2000.

Samarati, P. and De Capitani, S. V. (2001). Access Control: Policies, Models, and Mechanisms. *Foundations of Security Analysis and Design*. 137-196.

Sandhu, R. and Samarati, P. (1996). Authentication, Access Control, and Audit. ACM Computing Surveys, 289(1). 241-243.

Saxena, R. (2004). Security and Online Content Management: Balancing Access and Security. 12th Biennial VALA Conference and Exhibition, Melbourne, Australia, Victorian Association for Library Automation (VALA).

Sengupta, A., Mazumdar, C. and Barik, M. S. (2005). e-Commerce security – A life cycle approach. *Sadhana*. 30(2), 119–140.

Shen, H., and Hong, F. (2006). An Attributes-Based Access Control Model for Web Services. *Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies.*

Shyni, E. C. and Swamynathan. S. (2011). Reason based Access Control for Privacy Protection in Object Relational Database Systems. *International Journal of Computer Theory and Engineering* 3(1), 32-37.

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

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

Stoupa, K., Simeoforidis, Z., and Vakali, A. (2006). Credential-Based Policies Management in an Access Control Framework Protecting XML Resources. , *Lecture Notes in Computer Science.* 4263, 603-612.

Sun, L. and Wang, H. (2010). Dynamic Purpose Based Usage Access Control. *World Academy of Science, Engineering and Technology 2010.* 619-624.

Thion, R. and Coulondre, S. (2010). A Relational Database Integrity Framework for Access Control Policies. *Journal of Intelligent Information Systems.* 3(1): 131-159.

Tolone, W., Ahn. G., Pai, T. and Hong, S. (2005). Access Control in Collaborative Systems. *ACM Computing Surveys,* 37(1), 29-41.

United States Federal Trade Commission. Privacy Online: Fair Information Practices in the electronic marketplace, May 2000. Available at www.ftc.gov/ reports/privacy2000/privacy2000.pdf.

Wang, H. (2004). Access Management in Electronic Commerce System. PhD. Thesis. University of Southern Queensland; 2004.

Warren, S., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review. *4(5).* Retrieved on July 19, 2008, from http://www.lawrence.edu/fast/boardmaw/ Privacy_brand_warr2.html.

Weitzner, D. J., Hendler, J., Berners-Iee, T. and Connoly, D. Creating the policy-aware Web: Discretionary, Rules-Based Access for World Wide Web. In: Ferrari, E. and Thuraisingham, B., Web and Information Security. IOS. Idea Group Inc., 2005.

Westin, A. F. (1967). *Privacy and Freedom*, 25, New York, Wash. & Lee L. Rev. 166 (1968).

White G. (2003). The changing landsacpe: E-learning in schools. *Technical Report*, Retrieved on April, 2012, from http://admin.edna edu.au/dspace/bitstream/2150/54787/1/ changing_landscape_gw.pdf.

Yang, C. and Zhang, C. N. (2003). Designing Secure E-Commerce with Role-based Access Control. *Proceedings of the IEEE International Conference on E-Commerce,* 2003.

Yang, C. and Zhang, C. N. (2007). Designing Secure E-Commerce with Role-based Access Control. *International Journal of Web Engineering and Technology*. Volume 3(1), 73-95.

Yang, N., Barringer, H., & Zhang, N. (2008). A Purpose-Based Access Control Model. *Journal of Information Assurance and Security*. 51-58.

Yu, T., Sivasubramanian, D. and Xie, T. (2009). Security Policy Testing via Automated Program Code Generation. *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies,* 2009.