“I hereby declare that I have read this project and in my
opinion this project is sufficient in terms of scope and quality for the
award of the degree of master of computer science (information security)”

Signature : ....

Name of Supervisor : DR IMRAN GHANI

Date : JUNE 10, 2012

ONTOLOGY DRIVEN PRIVACY ACCESS CONTROL FOR HEALTHCARE INFORMATION SYSTEM

AIDARUS MOHAMED IBRAHIM

A project submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JUNE 2012

I declare that this project entitled “Ontology Driven Privacy Access Control For Heathcare Information System” is the result of my own research except as cited in the references. The project report has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ....
Name : Aidarus Mohamed Ibrahim
Date : June, 2012

“Dedicated to my beloved family and friends, without their understanding, supports, and most of all love, the completion of this work would not have been possible.”

ACKNOWLEDGEMENT

I would like to express my gratitude to Allah for providing me the blessing to complete this work. Hence, I am deeply grateful to my supportive and helpful supervisor Dr Imran Ghani for assisting and guiding me in the completion of this project. With all truthfulness, without Allah then his support, this project would not have been a completed. Imran Ghani has always been my source of motivation and guidance. For that, I am truly grateful for his continual support and cooperation in assisting me all the way through the semester.

My thanks also extend to my friends, for their enlightening companionship and encouragement of trudging through all the moments from down to up the hill in the run to complete Master Project. I would not have done it without the help and motivation from all of them.

To my family, no words can describe my gratefulness for always being there despite of the distance. They have showered me with love and compassion and enrich my life like no other. They are the source of comfort and kept me focus the priorities in life and therefore, this work is dedicated to them.

ABSTRACT

Ontologies are common definitions for entities. As ontologies are needed for the standardization of the definition of different terms; they are also important for the understanding of healthcare applications by machines. Sharing the information brings for some security needs like privacy and access controls in healthcare. Hence, effective mechanisms are needed to ensure the privacy of healthcare information system. Developing a privacy access control model is essential for healthcare information system. So far many privacy access control models have been developed to protect the patient's medical records. This study is set out to consider different privacy access control model by looking their advantage and drawbacks. Pusat Kesihatan UTM has been chosen as the particular small-medium hospital to explore the problems in the patient's privacy to experiment the type of privacy access control model used. This is where the project comes in to; to study the current information system at UTM Clinic and to propose complete Privacy access control model to support the users involved in the system as well as keep patient's medical records protected. Qualitative method is used to get needed information and study the current situation of information system at the clinic. Internal interview was carried out with the TISMA (Total Information for Medical Administration) administrator to understand the Weaknesses of the current system within the clinic and also to recognize the expectations of system administrator TISMA. Through the analysis of different privacy access controls, this project comes up with policy ontology based privacy access control model which presents three aspects of healthcare Information system that include rights, ontology representation and Rei policy specification. Finally a prototype has been implemented to generate the result.

ABSTRAK

Ontologies adalah definisi biasa bagi entiti. Sebagai ontologies diperlukan untuk penyeragaman takrif syarat-syarat yang berbeza; mereka juga adalah penting untuk memahami aplikasi penjagaan kesihatan oleh mesin. Berkongsi maklumat yang membawa beberapa keperluan keselamatan seperti kawalan privasi dan akses dalam penjagaan kesihatan. Oleh itu, mekanisme yang berkesan diperlukan untuk memastikan privasi sistem maklumat penjagaan kesihatan.Membangunkan model kawalan akses privasi adalah penting untuk sistem maklumat penjagaan kesihatan. Setakat ini banyak model privasi kawalan akses telah dibangunkan untuk melindungi rekod perubatan pesakit. Kajian ini dibentangkan untuk mempertimbangkan model kawalan akses privasi yang berbeza dengan melihat kelebihan dan kelemahan mereka. Pusat Kesihatan UTM telah dipilih sebagai hospital kecil dan sederhana untuk meneroka masalah dalam privasi pesakit menguji jenis model kawalan akses privasi yang digunakan. Ini adalah di mana projek itu akan masuk untuk mengkaji sistem maklumat semasa di Klinik UTM dan mencadangkan model kawalan Privasi akses lengkap untuk menyokong pengguna yang terlibat dalam sistem seperti juga menyimpan rekod perubatan pesakit yang dilindungi. Kaedah kualitatif digunakan untuk mendapatkan maklumat yang diperlukan dan mengkaji situasi semasa sistem maklumat di klinik. Temuduga dalaman telah dijalankan dengan pentadbir TISMA untuk memahami kelemahan sistem semasa di dalam klinik dan juga mengiktiraf jangkaan pentadbir sistem TISMA. Melalui analisis kawalan akses privasi yang berbeza, projek ini datang dengan dasar privasi kawalan berasaskan ontologi model akses yang membentangkan tiga aspek sistem Maklumat penjagaan kesihatan yang termasuk hak, perwakilan ontologi dan spesifikasi dasar Rei. Akhirnya prototaip telah dilaksanakan untuk menjana hasil.

.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDIXES

CHAPTER 1

INTRODUCTION

1.1 Introduction

In recent years, advanced technologies that enable organizations to collect, store and manage massive amounts of data in digital form have been developed. Sometimes, the data maintained within an organization's databases is considered to be confidential. This is the case for patient health records, which may hold sensitive information. In such cases, the organization is responsible for establishing a data-access policy in order to maintain privacy.

Currently, healthcare services are moving from paper-based to electronic version of record king system (SCIMP, 2006).As medical personnel need to document increasing volumes of information as patients receive increasingly complex care involving a range of data from the intensive examinations and treatments paper-based systems are not sufficient to cope with this revolutionize. While technology advancements are available to transform healthcare record keeping in many positive ways, Privacy control of HIS pose unique concern. Healthcare records use to be considered private matter between the doctor and the patient. However, with the continuous growth of the organization who involved the in the healthcare maintenance, doctor nowadays are required to share these records with third party. Hence, health records are someway perused employers insurance companies and drug manufacturing companies. Since patient records contain sensitive information such as insurance number, social security number past drug use or genetic predisposition to various diseases, it is very important it is very important to prevent unauthorized access to these private and confidential data.

Commonly, some hospitals many people can have access to healthcare information system (HIS).Anyone from nursing staff to the lowest technicians can have look at those records. Therefore, a serious question is how completely is the patient's records is kept from unauthorized eyes from seeing medical records unnecessary? As medical records aggregated into electronic databases, there is mounting concern will have even more access to these records and these situations might threat to confidentiality of personal health information (Fratini, 2007).

In fact, modern electronic health records contain extremely personal and sensitive information regarding not only health history but also the dietary habits, sexual orientation, sexual activities, employment status, income, eligibility for public assistance and family history of a patient (Choi,Capitan, Krause, &Streeper, 2006).Patients understand the importance of retaining medical information to support and improve the delivery of health care even when they recognize both the sensitive nature of the collected data and the fact that information contended by computerized health information system becomes more accessible to health professionals, administrative and medical staff, and third parties (Conrick& Newell,2006). Patients expect secure health information systems in which personal data is protected and any disclosed information would be used only for health care purposes (Grain, 2006).

Security and privacy are thus increasing imperative for data and information so privacy related issues include building design for privacy issue include implementation privacy policy related.

Due to the importance for the patient's medical information and its privacy, healthcare information system must have privacy access controls which can enhance the functionality and trustworthiness between the patients and the healthcare information system staff. Otherwise, patient will worry about their information and this may decrease the satisfaction between the doctors and patients.

First of all, in this thesis various models related to privacy access control for healthcare information system (HIS) is discussed.

1.2 Background of the Problem

In a shared care environment, different health care units (HCU) are involved in the care process as well as in maintaining accurate medical records. Indeed, in modern healthcare environments different care services are offered by different HCU within the organization or in a healthcare network that involves multiple organizations. This requires the communication and cooperation among all actors involved in the administration of patients care (Choi, et al., 2006).Internet turns into a natural environment for such functionalities by allowing the exchange of EHRs and the interconnection of medical applications, thus facilitating better management of medical services as well as faster treatment of patients (Gritzalis and Lambrinoudakis, 2004).

As in paper-based health records, physicians have an ethical obligation of protecting patient information in order to prevent potential harm to an individual. Nevertheless, the nature of her/his transformed the duty of physician-patient confidentiality to a complex task. Despite thepersonal nature of health records, EHRs make patient’s information potentially available to anyone with access to a health information system (Anderson, 2007).

Therefore, the responsibility of protecting patient privacy has moved from an individual/local responsibility to a duty shared among the different entities that share the information. This tendency is altering the preexisting conception of the doctor–patient confidentiality and is threatening the quality of health care (Choi,et al., 2006). These apprehensions are also shared by the public whose primary concern is security, privacy, confidentiality and protection of their personal health information (Goldschmidt, 2005,Rash, 2005).

As an attempt to explore the problems related privacy access control for healthcare information system, this research will focus on particular small-medium hospital named UTM Clinic.

In this project, it has been emphasized the patient's information privacy by combining the suitable mechanisms to provide the patients high quality of medical services as well as keeping his information as private. Only those who have the suitable permission can access the system. Policy Ontology based privacy access control model have been proposed, to validate the model a prototype has been implemented.

1.3 Problem Statement

Clearly, it is very crucial point to understand the users who want to access the patient's information and related access controls. The different roles for healthcare Information system users in UTM Clinic are different from doctor to nursing staffs. To enhance the degree for privacy control in healthcare information system (His) in UTM Clinic we proposed policy ontology driven privacy access control model. The main problem is "Who can access the patient's medical records?"We have analyzed the categories of users Doctors and Nurses such with the read/write privileges in UTM clinic that can only view the records but also can edit.

1.4 Project Objectives

The objectives of the project include:

- To study the current UTM Clinic information system privacy control.
- To propose policy ontology based model for privacy control for healthcare information system.
- To develop prototype for policy ontology based privacy access control.

1.5 Scope of the Project

These are the important scopes which define the boundary of the project:

- This project looks at the healthcare system privacy control recognized in UTM Clinic and their existing system and the type of privacy access control model are used.
- This study focuses on analyzing the current status for the user privilege to access patient's information at UTM Clinic.

1.6 Significance of the project

The significance of the healthcare information system is paramount as it utilizes technology to provide added convenience to our daily lives. In the past, a patient would have to wait as the doctor and nurses retrieved their paper medical records. Now, doctors have instant access to our medical records with just click of mouse. However, the challenge of implementing of healthcare information system is the protecting the patient's privacy of the medical records. The consequences are great if the medical records if the medical records are leaked to outsiders. In here, we proposed model for Privacy control at UTM Clinic to ensure the right user who can access the system completely or partially by giving some certain privileges. This thesis contributes to the following factors:

- Helping Database administrators in hospitals to understand Patient's privacy and their roles as well as the way they can be adequately supported by information and communication technology.
- Supporting the Database administrators to control the privacy better in HIS
- Improving privacy access control for Patient's privacy.

1.7 Report Organization

The project contains six chapters. The chapters are organized according to the different work involved in this study. The detailed organization of the report is described in the following paragraphs. This section gives highlight the way different chapters are organized.

Chapter 1 describes a general outline of the project by giving a brief overview and the problem of the project. Statements of the objectives and aims of the project were presented. The scope and significance of the project have also stated. The project will be successfully achieved by successful developing these objectives and aims of the project.

Chapter 2 contains the review of the literature and the related the works done by the authors; it highlights the policy ontology based access controls in healthcare system. The author presented deeply by citing comparative study related in this project. The author identified the gap and proposed a model.

Chapter 3 highlighted the Methodology operational framework. This framework consists of three phases .the first phase contains the literature review and case study used for data collection. The second phase covers the proposed model and its implementation. The last phase outlines the project report writing and presenting the project.

Chapter 4 discussed a study related the current system in UTM Clinic. The author carried out real case study about the access controls in UTM clinic and the classification of user in the clinic based on the permission when accessing the system. The author met face to face the system administrator in TISMA system and interviewed the existing access controls practiced in TISMA system. After being understood the problem which is the output of the case study. The author proposed model which is designed based the results from the interview. The components of the proposed model also discussed in this chapter.

Chapter 5 focuses on the prototype implementation by generating the expected result. In this chapter, the modules which are the building blocks of this model have been produced and drawn their result. In here, the author produced three various results based on the modules on the model. Such as first module which is permissions, tasks, roles, assignments, operations. While the second module contains ontology representation based UTM Clinic. The final module contained the Rei policy specifications for management of the privacy access control.

Chapter 6 looks at the conclusion and the recommendations, as well as the judgment whether or not the objectives of the study are met.

REFERENCES

A. Toninelli, R. Montanari, L. Kagal, O. Lassila, Proteus.(2007). A Semantic Context-Aware Adaptive PolicyModel, IEEE Intl Workshop on Policies for Distributed Systems and Networks. 129-40.

Bandar S. Alhaqbani.(2010). Privacy and Trust Management for Electronic Health Records. Doctor Philosophy. Queensland University of Technology Brisbane, Australia.

B. Shields, O. Molloy, G. Lyons, J. Duggan(2006). Using Semantic Rules to Determine Access Control for WebServices.Proc 15th Intl Conference on World Wide Web (WWW 2006), (2006) 913-914.

B. Shields, O. Molloy, G. Lyons, J. Duggan, Using Semantic Rules to Determine Access Control for WebServices, *Proc 15th Intl Conference on World Wide Web (WWW 2006)*, (2006) 913-914.

C. Wolter, M. Menzel. A. Schaad, P. Miseldine, and C. Meine(2009). Model driven business process security requirements specification.Journal of Systems Architecture.

D. F. Ferraiolo, D. R. Kuhn and R. Chandramouli(2003). Role-Based Access Control.Artech House, 2003.

Engelbrecht Rolf, Geissbuhler A., Lovis C (2005). Connecting Medical Informatics and Bio-informatics: *Proceedings of MIE2005: the XIXth International Congress of the European Federation for Medical Informatics. IOS Press.*

Eukleenjungko, Hyungji and jeun woo lee(2007). Ontology and CDSS based intelligent health data management in healthcare server".

Farooq, K.; Hussain, A.; Leslie, S.; Eckl, C.; Slack W(2011)..Pervasive Computing Technologies for Healthcare (PervasiveHealth), *2011 5th International Conference on Publication Year: 2011 , Page(s): 283 – 286.*

G. Brox(2005). MPEG-21 as an access control tool for the National.Health Service Care Records Service", *Journal ofTelemedicine and Telecare, volume 11, pp. 23-25.*

H. L. Sollins(2008). HIPAA privacy guides for providers and patients,Geriatric Nursing.

ISO(2005).Electronic Health Record—Definition, Scope and Context. International Organization for Standardization 2005.

J. B. D. Joshi, W. G. Aref, A. Ghafoor, and E. H(2001), Spafford. Security models forweb-based applications. Communication of the ACM, 44(2):38–44.

L. Zhang, G. Ahn, and B.-T. Chu (2001). A Rule-based framework for role based delegation, In Proceedings of the 6th ACM symposium on Access control models and technologies Chantilly, Virginia, USA.

L. Kagal, C. Hanson, D.Weitzner(2008). Using dependency tracking to provide explanations for policy management, *in IEEE Policy*.

M. Evered and S. Bögeholz(2004). A case study in access control requirements for a health information system. Proceedings of the 2nd Australasian information security workshop (AISW2004), Dunedin.

NJBM Zaizi (2007). A Study Of Security And Privacy Issues In Hospital Record Management System.

Rui Zhang and Ling Liu.(2010).Security Models and Requirements for Healthcare Application. *Information Technology and Applications in Biomedicine (ITAB), 2010 10th IEEE International Conference on , vol., no., pp.1-4, 3-5 Nov. 2010 Clouds.*

R. S. Sandhu and P. Samarati.(1994). Access control: Principles and practice. IEEECommunications Magazine, 32(9):40–48, 1994.

R. Studer, V. R. Benjamins, and D. Fensel(1998).Knowledge engineering: principles and methods. ***D**ata Knowl.Eng., vol. 25, no. 1–2, pp. 161–197, 1998.*

R. Dieng-Kuntz, D. Minier, M. Ruzicka, F. Corby, O. Corby, and L.Alamarguy.(2006). Building and using a medical ontology for knowledge management and cooperative work in a health care network.*Comput. Biol. Med.,vol. 36, no. 7–8, pp. 871–892.*

T. Strang and C. Linnhoff-Popien,(2004), Context modeling survey. InProc. Workshop Adv. Context Model., Reason. Manage. (UbiComp 2004),Nottingham, England, 2004.

T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, et al, ROWLBAC (2008). Representing Role Based Access Controlin OWL, *Proc 13th Symposium on Access controls Models and Technologies* (2008) 73-82.

V. Hu, D. Ferraiolo, and D. R. Kuhn.(2006). Assessment of access control systems. Technical Report NISTIR-7316, National Institute of Standards and Technology.

Valls, K. Gibert, D. S´ancheza, and M. Bateta(2010). Using ontologies for structuring organizational knowledge in Home Care assistance,” *Int. J. Med. Inform., vol. 79, no. 5, pp. 370–387, 2010.*

X. H.Wang, D. Q. Zhang, T. Gu, H.K. Pung, and H. K.(2004), “Ontology based context modeling and reasoning using OWL,” in Proc. 2nd IEEE Conf.PervasiveComput. Commun. Workshops, 2004, pp. 18–22.