UNIVERSITI TEKNOLOGI MARA

DYNAMIC USER-DEFINED ACCESS CONTROL POLICIES via PROGRAMMING LANGUAGE

SUZANA BINTI AHMAD

Thesis submitted in fulfillment
of the requirements for the degree of
Doctor of Philosophy

Faculty of Computer and Mathematical Sciences

January 2018

CONFIRMATION BY PANEL OF EXAMINERS

I certify that a panel of examiners has met on 20th July 2017 to conduct the final examination of Suzana Binti Ahmad on her Doctor of Philosophy thesis entitled "Dynamic User-Defined Access Control Policies via Programming Language" in accordance with Universiti Teknologi MARA Act 1976 (Akta 173). The Panel of Examiners recommends that the student be awarded the relevant degree. The panel was as follows:

Maheran Mohamed Jaafar,PhD
Associate Professor
Faculty of Computer and Mathematical Sciences
Universiti Teknologi MARA
(Chairman)

Rosmawati Nordin,PhD
Associate Professor
Faculty of Computer and Mathematical Sciences
Universiti Teknologi MARA
(Internal Examiner)

Abdul Samad Ismail, PhD
Professor
Faculty of Computing
Universiti Teknologi MALAYSIA
(External Examiner)

Ngoc Thanh Nguyen, PhD
Professor
Wroclaw University of Technology, Poland
(External Examiner)

PROF SR DR HJ ABDUL HADI HJ NAWAWI
Dean
Institute of Graduates Studies
Universiti Teknologi MARA
Date: 22 January 2018

AUTHOR'S DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work, unless otherwise indicated or acknowledged as referenced work. This topic has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic rules and regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student	:	Suzana binti Ahmad
Student I.D. No.	:	2010798845
Programme	:	Doctor of Philosophy - CS990
Faculty	:	Computer and Mathematical Sciences
Thesis Title	:	Dynamic User-Defined Access Control Policies via Programming Language
Signature of Student	:	.....
Date	:	January 2018

ABSTRACT

Allowing data sharing activities to the right users can be determined by concerned access control through assisting every attempt made by a user, to access a resource in an application system. The interests of authorized the users, who are protected by access control, can provide a safe, secure and accessible working environment. Implementation of access control involves three important issues, which include policies, models and mechanisms. The appointed administrator has the authorization to manage the access of data sharing under every possible circumstance by specifying the model of access control as high-level requirements for policy mechanisms. Commonly, most application systems rely on an administrator to manage access control policies which may lead to conflicts between users and the administrators empowerment. Such conflicts exist due to lack of involvement from end-users in handling the access control. Another issue raised, is those of unrevised services, which occur frequently due to massive and complex policy details that need to be handled by the administrator. Additionally, most programming languages and programming environments do not naturally support implementing policy for access control. Nevertheless, the policy needs to be coded as part of the system development for managing access control. Furthermore, access control policies are high-level features, which require high cost maintenance. This thesis examines the control mechanisms in data sharing activities among collaborative users. The results of the research undertaken offers a model that allows data owners to provision access control policies in collaborative data sharing environments via a specific programming language. The model supports dynamic owner-centered empowerment of data access control policy that allows data owners to have control of their own data. The policy can change dynamically according to the data owners needs during collaborative sessions. The proposed model also facilitates explicit access control mechanisms for the data owner to secure his or her data. The investigation uses real life observation on an uncontrolled environment of public and private data sharing as a method to identify missing mechanisms for data owners access control empowerment. A banking system is selected to examine the existing access control mechanism by using an abstract scene approach. This is achieved through observation and the examination of both the existing and non-existing mechanisms, in order to accommodate the data sharing process. In addition, this research extends the experiment through a small-scale case study using a controlled variation of the rules for a modified scrabble game to uncover a list of control policy states. Both findings are modeled and prescribed in the form of language constructs to accommodate the solution and testing. Therefore, a set of language constructs are designed and implemented on an existing scripting language JACIE (Java based Authoring language for Collaborative Interactive Environments) that allows rapid prototyping on the result and testing. Major extensions on JACIE are performed to verify the model. This model will significantly accommodate a comprehensive framework of data sharing among different levels of organizations (government and private sectors) in wider perspectives.

TABLE OF CONTENTS