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