Chapter 1 Introduction

1.1. General

Nowadays, in order to research, marketing or provide better service, a numbers of enterprises would collect customers' relevance data, such as personal information, service experience, and desired functions. However, since the occurrences of deceptive crime and personal information disclosure happened frequently, privacy protection has been paid much attention by consumers, companies, researchers, and legislators. Victims not only receive annoying advertisements and reluctant marketing tricks, but also face to the threat of life and property [1] [2].

In accordance to that storing sensitive information creates fear of privacy violation and a danger that the information could be misused for many online consumers. Also, potential lawsuits brought up by consumers and recently enacted privacy legislations require organizations to pay closer attention to the management of private data [3] [4] [5] [6].

As individuals are more concern about their privacy, they are becoming more reluctant to carry out their businesses and transactions online, and many organizations are losing a considerable amount of potential profits. Therefore without a clear compromise between individuals and enterprises, data quality and data privacy cannot be achieved and many organizations are seriously thinking about privacy issues of consumers. By demonstrating good privacy practices, many businesses are now trying to build up solid trust to customers, thereby attracting more customers [7] [8].

To raise privacy-aware consciousness, data providers should take notice of the private level of delivered data and ensure the transmission security, content confidentiality and supplementary measures like contracts establishment. If the mechanism for privacy protection is defective, we should prefer rejecting to provide sensitive data to indiscriminately exposing private information, which may result in facing the threat of life and property. Fortunately, businesses gradually have built up customer dependence by practicing privacy protection mechanism, consequently, they avoid losing potential profits and attract more customers as much as possible [9] [10].

Recent research efforts have been developed many different types of database access control models for privacy protection. Access control models ensure that only authorized users are given access to certain data or resources necessary to perform their respective tasks, while preventing access to resources that are not relevant to the user. The access control decision is enforced by a mechanism implementing regulations established by a security policy.

There are core elements of any access control model; Identification, Authentication and Authorization. Identification is the activity of the subject supplying information to identify itself to an authentication service. Authentication is the process of ensuring that the identity in use is being used by the right person. Authorization is the process of determining the set of action allowed for the identified subject. It is based on some type of predefined criteria, which is enforced through access control policies. Access control policies ensure a high degree of protection in a way; they prevent any illegal flow of information [11] [12].

The remainder of this chapter is organized as the following. In section 1.2, a brief description of the related work and the need for a new model is presented. In section 1.3, the organization of the thesis is outlined.

1.2. Motivation and Scope of Work

Privacy protection of individuals is a challenging problem due to the rapid advances in database systems and information technology. The fact that the customer information can be collected and used leads to the fear that the personal data can be misused.

As privacy becomes a major concern for both consumers and enterprises, many research efforts have been developed toward privacy protecting technology. As enterprise has to develop a secure privacy access control model that ensure accessing the customer data while at the same time assuring privacy, the Wide Web Consortium (W3C) has proposed the Platform for Privacy Preference Project (P3P). This platform allows websites to encode their privacy practice policy in a standard format, but it does not provide any mechanism to ensure that this policy is fulfilled and the collected information will not misused [13].

Another contribution to privacy protection technology is the Conditional Purpose Based Access Control model (CPBAC), which allows users to use some data for certain purpose with conditions. More information from data providers can be extracted while at the same time assuring privacy that maximizes the usability of consumers' data. The main disadvantage of this model is that it has a static permission assignment by means that the permission assignment process is not automated and does not change by the progression of a task, permissions will in most cases manually be "turned on" too early or too late and will probably remain "on" long after the tasks have terminated. Another drawback is that there is no scope for the permission inheritance in the role hierarchy; the parent role inherits total permissions from the child roles, which leads to vulnerabilities in the system, as the data may be misused [14].

Recently, Flexible Policy Based Access Control Model for Workflow Management Systems (PBFW) presented an approach to enforce privacy policy in a workflow environments, by means it has authorization policies to support dynamic separation of duty to prevent illegal data access [15].

Another great contribution to the privacy protection access control models is the Access Control Model Based on Multi-Role and Task (MD-TRBAC) [16]. This model address some distinct problems in the CPBAC model [14]. MD-TRBAC introduced permission inheritance scope; the parent role only inherits the required permissions or inherits no permissions.

PBFW model and MD-TRBAC model meet the workflow and enterprise's needs, both have automated permissions assignment and the notion of a life-cycle. But both lead to information loss because users are not allowed to get more information conditionally. The main concern is to preserve privacy of individuals as well as extracting more information and have an automated solution to meet the workflow environment requirements, which is presented in the proposed model. The related work taxonomy is illustrated in Figure 1-1.

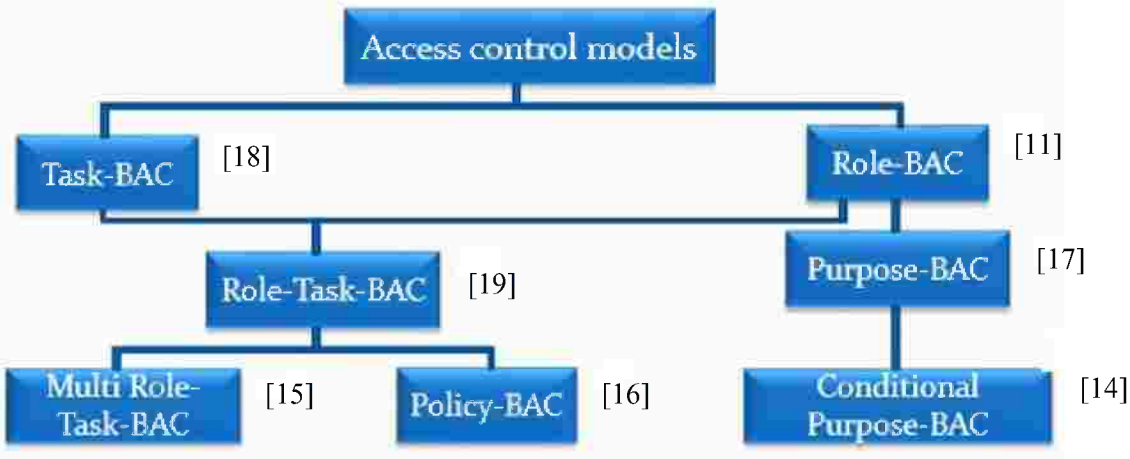

Figure 1-1 Related work hierarchy

.

The aim of this thesis is to combine the advantages of the most powerful access control model the **CPBAC** model with the advantage features of the PBFW model and MD-TRBAC model**.** The proposed model will have a reliable data management by using the conditional access purpose concept. In addition achieving scalability and meeting the workflow environment requirements. The scope of this thesis, is to implement and study in detail the previously mentioned features. A case study will be presented as a proof of concept to simulate the implementation process and evaluate the proposed model.

1.3. Organization of Thesis

The remaining of the thesis is organized as below.

In chapter 2, existing database access control models are surveyed and discussed in details. The need to extend such models and its functionality to add some dynamic characteristics and reduce the complexity of the access policy is established.

In chapter 3, a proposed database access control model is introduced.

In chapter 4, the obtained results and a comparison to the related work are discussed through a case study.

Finally, in chapter 5, conclusions and possible future work are discussed.