HOSTED BY

ELSEVIER

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

ORIGINAL ARTICLE

Role-task conditional-purpose policy model for privacy preserving data publishing

Rana Elgendy, Amr Morad [*], Hicham G. Elmongui, Ayman Khalafallah, Mohamed S. Abougabal

Computer and Systems Engineering, Alexandria University, Alexandria, Egypt

Received 28 February 2017; accepted 27 May 2017

KEYWORDS

Database security;
Access control;
Data publishing;
Anonymization

Abstract Privacy becomes a major concern for both consumers and enterprises; therefore many research efforts have been devoted to the development of privacy preserving technology. The challenge in data privacy is to share the data while assuring the protection of personal information. Data privacy includes assuring protection for both insider ad outsider threats even if the data is published. Access control can help to protect the data from outsider threats. Access control is defined as the process of mediating every request to resources and data maintained by a system and determining whether the request should be granted or denied. This can be enforced by a mechanism implementing regulations established by a security policy. In this paper, we present privacy preserving data publishing model based on integration of CPBAC, MD-TRBAC, PBFW, protection against database administrator technique inspired from oracle vault technique and benefits of anonymization technique to protect data when being published using k-anonymity. The proposed model meets the requirements of workflow and non-workflow system in enterprise environment. It is based on the characteristics of the conditional purposes, conditional roles, tasks, and policies. It guarantees the protection against insider threats such as database administrator. Finally it assures needed protection in case of publishing the data.

1. Introduction

Many enterprises would collect customers' data, such as personal information, financial or medical data in order to provide better service [1]. Since the occurrences of deceptive crimes and sensitive personal information disclosure happened frequently, privacy protection has been taken much attention by companies, consumers, and researchers [1]. Victims may receive annoying advertisements and reluctant marketing tricks in addition to face the threat of life and property [2].

Because of these threats, individuals are becoming frightened of sharing their businesses and transactions online, so organizations are losing large amount of potential profits. Therefore organizations pay attention to the management of private data [2].

[*] Corresponding author.
E-mail addresses: rana_elgendy@yahoo.com (R. Elgendy), amr.morad20@gmail.com (A. Morad), elmongui@alexu.edu.eg (H.G. Elmongui), ayman.khalafallah@alexu.edu.eg (A. Khalafallah), mohmed.abougabal@alexu.edu.eg (M.S. Abougabal).

Peer review under responsibility of Faculty of Engineering, Alexandria University.

http://dx.doi.org/10.1016/j.aej.2017.05.029
1110-0168 © 2017 Faculty of Engineering, Alexandria University. Production and hosting by Elsevier B.V.

A major requirement of any information management system is to protect resources and data against unauthorized disclosure, called secrecy, and unauthorized or improper modifications, called integrity, while at the same time ensuring their availability to the users, means that no denial-of-service occurs. Enforcing such protection requires that every access to a system and its resources have to be under control and only authorized access requests are granted. This process is called access control [3].

Significant research efforts have been done toward achieving the perfect privacy preserving data publishing model. Many different types of database access control models have been developed to protect against outsider threats. Recent research also has been conducted on the privacy protection in the context of both workflow and non-workflow systems. A workflow system is defined as the orchestration of a set of activities involving coordinated execution of multiple tasks done by different processing entities [4]. Workflow systems guarantee the management of the flow of work such that the work is done by the proper person at the right time. This ensures a global integration between all the entities in the business process framework. Workflow systems also support resource allocation and dynamically adapt to workload changes [5].

In this paper, we provide a solution for privacy preservation against insider and outsider threats. This solution assures privacy in case the data are published. Our solution represents integration in some existing privacy preserving models; namely, (1) the CPRBAC access control model [6], (2) the MD-TRBAC access control model [7], (3) the PBFW access control model [8], some concepts from oracle vault technique [9], and (4) k-anonymity [10]. This integration would result in the benefits of these protection techniques. Therefore, the proposed privacy preserving data publishing model would inherit, from CPRBAC [6], the role-based access control and the task-based access control. It would also support workflow systems, as MD-TRBAC [7], and would have access control policies to enhance user privacy, as in PBFW [8]. It guarantees the protection against insider threats by adopting some concepts from oracle vault technique [9]. The model also would guarantee, from k-anonymity [10], that the individuals who are the subjects of the data cannot be re-identified while the data remain practically useful when the data are published. The model meets the particular requirement of the workflow systems such as the notion of a task life cycle, the dynamic access control, the separation of duty principle [11], and active permission assignment. In addition the new model adapts the notion of conditional purpose [6] which provides more reliable data management because more information can be extracted while assuring the user's privacy.

2. Related work

Several works have been done toward privacy protection technology. Enterprises have to develop a secure privacy protection model that ensures accessing the customers' data while at the same time assuring privacy for their sensitive data.

Role-based access control (RBAC) [12] has been widely used in database management systems and operating systems products because of its significant impact on access control systems. Following RBAC, Task-based access control (TBAC) [13] mainly focused on task-oriented perspective; therefore it approaches security modeling and enforcement at the application/enterprise level. A combination between RBAC and TBC, called Task Role-based access control (TRBAC) [14], which inherits the intuitionistic characteristic of RBAC model and the dynamic characteristic of TBAC model, is considered good step toward privacy protection access control models.

Purpose based access control (PBAC) [15] and conditional purpose based access control (CPBAC) [16] are considered a landmark toward privacy protection. The basic concept of both models is purposes. Purposes [15] describe the intentions for data collection and data access. Permissions are assigned on the combination of conditional roles and purposes. Role is defined as a job title or job function within the organization associated with its authority. Roles are organized in a role hierarchy to facilitate the administration tasks [15]. Purposes support both positive and negative privacy policies. In both models, purpose information associated with a given data element specifies the intended use of the data element. An access to a specific data item is allowed if the purposes allowed by privacy policies include or imply the purpose for accessing the data. An intended purpose consists of three components: Allowed Intended Purpose, Conditional Intended Purpose, and Prohibited Intended Purpose [15]. This structure provides greater flexibility to the access control model. Conditional purpose allows users to use some data for certain purpose with conditions [16]. More information from data providers can be extracted while at the same time assuring privacy. This maximizes the usability of consumers' data. The main drawback of the model is that it has a static permission assignment which 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 means that the parent role inherits total permissions from the child roles. This leads to vulnerabilities in the system, as the data may be misused [15,16].

Flexible Policy Based Access Control Model for Workflow Management Systems (PBFWs) [8] presented a great approach for enforcing privacy policy in workflow environments [8]. It has authorization policies to support dynamic separation of duty to prevent illegal data access [11]. The advantages of RBAC [12] and TBAC [13] are adopted; therefore PBFW meets the dynamic and flexible requirements, such as Separation of Duty policy (SoD), and dynamic access control that meets the workflow needs [11]. Separation of duty means that at least two different people are responsible for the completion of a task or set of related tasks [11]. The purpose of this principle is to discourage fraud by spreading the responsibility and authority for an action or task over multiple people, thereby raising the risk involved in committing a fraudulent act [11]. Also the model dynamically manages permissions as authorizations progress to completion [8]. The main drawback of the system is that it does not know the notion of the purposes and conditional purposes, which cause more information loss [8].

One of the remarkable contributions to the privacy protection is the Access Control Model Based on Multi-Role and Task (MD-TRBAC) [7]. This model addresses some distinct problems in the Conditional Purpose Dynamic Role-based