Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Analysis of Existing Privacy-Aware Access Control for E-Commerce Application

Dr. Norjihan Abdul Ghani[1], Harihodin Selamat[2] and Zailani Mohamed Sidek[3]

1

Received: 7 April 2012 Accepted: 30 April 2012 Published: 15 May 2012

Abstract

Due to the growing use of the internet, more and more critical processes are running over the web such as e-commerce. Internet allows commerce and business between parties who are physically distant and do not know each other doing the transaction. For the effective operation of the web application and e-commerce applications, security is a key issue. Various aspects of security are relevant to e-commerce such as database security. The availability of e-commerce, user transactions are no longer bound to traditional office-centered environment, but it can be started virtually anywhere at any time. It was moving from closed environment to open environment. In this paper, we clearly define the privacy-aware access control requirements. We also investigated few existing access control in the context of this requirements. We build an assessment criteria in our comparison based on the requirements defined which we finally used it later as a guidelines to design an access control for e-commerce application.

Index terms— access control, data privacy, e-commerce.

particular person is stored in approximately 1000 different databases [4].

However, the only support provided by database systems where much sensitive structured data reside is the mechanism for access control [7].

A basic idea of access control system is to authorize a user to access only a subset of the data. But, the traditional access control systems having more limitation since in e-commerce we need more reliable and appropriate access control system. The main contribution of this paper is to highlight the main requirements of privacy-aware access control for ecommerce environment.

The rest of the paper is organized as follows. Section 2 discusses the related works in this area. Section 3 discovers basic requirements for the privacyaware access control in e-commerce application. In section 4, we reviewed several access control model which tailored to the basic requirements that have been identified. Then, we make a comparison study between the existing access controls based on the existing models in Section 5. Section 6 concludes the paper.

We will discuss about previous work in the area of privacy preservation in the categories of extending the basic access control model for privacy preservation in ecommerce application. In the previous years, there are a lots of researches have been done in protecting the personal data. The purpose of the researches is to provide an access control system which tailored to privacy aware. In order to address the shortcomings of traditional access control which is lack support for privacy-related, the concept of Hippocratic Database been introduced in [1]. In this concept, the notion of purpose plays a major role in access control models. Motivated by this concept, many researchers used the concept of purpose in introducing the privacy-aware access control [16] , [5] and [6].

Entities are able to choose flexibly what of their data should be accessed to whom, for what purposes and in what circumstances. This concept was not satisfies with the idea that the entities of the data should have more control over the release of their information. The idea of entities having control on access to their data when it stored in e-form has been viewed as an (inalienable) right [2]. We also investigated other important factors in

e-commerce application such as the heterogeneity of users. User credential has been widely used to support the heterogeneity if users in ecommerce. Various types of credentials are being used by existing applications such as identity credential [10] , [15] and standard credential [11]. The differences of this paper is where we introduce the main requirements of privacy access control which it highlighted three basic requirements; purpose, individual control and the use of credential.

Due to the growing use of internet, more and more critical processes are run over the web such as egovernment or e-commerce applications. While current information technology enables people to carry out their business virtually at any time in any place, it also provides the capability to store various types of information the users reveal during their activities. The Federal Trade commission has shown that 97 percent of websites were collecting at least one type of identifying information such as name, e-mail address, or postal address of customers. The current database technology makes it possible to collect and store a massive amount of person-specific data.

An important requirement of any information management system is to protect data and resources against unauthorized disclosure (secrecy) and authorized or improper modification (integrity), while at the same time ensuring the availability to legitimate users (no denials-of-services). Data protection is ensured by different components of a database management system (DBMS). In particular, an access control mechanism ensures data confidentiality [3]. The advance of database technology has also significantly increased privacy concerns. Enforcing protection therefore requires that every access to a system and its resources be controlled and that all and only authorized accesses can take place. This process goes under access control.

This situation was lead to the awareness of privacy-aware access control. Many privacy policy access control models have been proposed in order to protect the privacy of consumers. In [6], the authors pointed out that privacy protection cannot be easily achieved by traditional access control models as it focuses on which user is performing which action on which data object. Agrawal in [1] introduces Hippocratic Database, but it was applied at implementation side. This section, we will discuss the requirements for privacy-aware access control model in database system: a) Flexible User Specification Mechanism Based On User Credentials

Most web-based applications are characterized by a user population which is far more heterogeneous and dynamic than user population typical of conventional information systems. Traditional access control which based on user identity is not relevant anymore when dealing with large numbers of users in open or distributed environment. There is thus the need for using other properties of subjects (e.g., age, nationality, job position) besides login in the specification and enforcement of access control. In an open and distributed environment data access is required by anyone spontaneously, centralized access control methodologies based on identity verification are not suitable. The credential based access control is found to be more appropriate in such environment [11]. b) Supporting Open Environment Government, large companies, and many other organizations are required to offer access to information contained within their information systems to a multitude of users. Users can be internal or external, and typically access the data from their clients connected to a network, refers to open environment. This scenario set the requirements that cannot be easily support with traditional authorization and access control solutions [12].

1 c) Purpose Based Data Privacy Protection

Privacy-aware access control deals with privacy specification and private data management systems. In privacy-aware access control models, the notion of purpose plays a central role as the purpose is the basic concepts around which privacy protection is built. The notion of appears in all privacy codes and legislations such as Data Quality Principle in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

2 d) Data Subject Involvement

Privacy preservation is an important requirement whenever personal data is collected, stored and disclosed. One of the main challenges is to share the information while complying with the data-owner privacy preferences.

There are however, a number of applications that require individual entities to be able to choose flexibly what of their data should be accessible to whom, for what purpose, and in what circumstances [2]. The idea of this owner controlled access control arise when data subjects should have more control over the release of their information to selected recipients and having more control when accessing their information when released it. F ebruary model. In this section, we will briefly discuss several modern access control model which tailored to privacyaware in e-commerce scenario. a) AC #1 : Self-Managed Access Control Self-managed access control (SMAC) is also known as abstract meta-model access control. The idea of this access control arise when data subjects should have more control over the release of their information to selected recipients and having more control when accessing their information when released it [2]. SMAC focus on providing data subjects to define the access controls on their data in order to ensure its confidentiality and so that the data may be used for the data subject's personal advantage.

SMAC policies provide data subjects so that they can provide the purposes for their data. Another feature of SMAC is that policies on access to personal data are facilitated in a distributed as well as a dynamic context. SMAC allow data subjects to choose freely what sources of information are to be used to determine authorized access to their data. Data subjects may revise a data controller's policy on the release of their personal data or the data subject may define its policy on the release of this data. This access control model separates the data

and policy and there is no annotation of data with purpose. It allows for dynamic policies on private data access to be effected autonomously and our logic language allows for executable specifications of access control policies. The limitations of this access control are it not considers obligations, audit policies, and hierarchies of objects or of purposes [2]. Assumptions have been made that data is stored and transmitted securely and that sound methods of authentication of data subjects, controllers and recipients are fully employed.

3 b) AC #2 Purpose-Based Access Control

Privacy preservation of individuals is a challenging problem in the data-mining environment. Enterprises collect customer's personal identification information along with other attributes during any kinds of marketing systems. It is a natural expectation that the enterprise will use this information for various purposes, this leads to concern that the personal data may be misused. These types of access control permits that the particular data element can be conditionally or unconditionally accessed only for the specific purposes with certain conditions. P3P introduced by World Wide Web Consortium defines purpose as "the reason(s) for data collection and use" and specifies a set of purposes.

Since privacy policies are concerned with the purposes that data object is used for rather than the actions that users perform on the data object, traditional access control models cannot easily achieve privacy protection, and the notion of purpose should play a major role in access control model to protect privacy.

Today, the concept of purpose is used as the basis of access control policy [5]. c) AC #3 : Privacy-Aware Role-Based Access Control Privacy-aware Role Based Access Control (P-RBAC) system is based on three requirements as following; the access must be both secure and privacy preserving, the access must be allowed to individuals from different organizations; the access could be confined based on meta information of the system. The idea behind access control is when we need to share sensitive information in a large distributed and heterogeneous environment. In P-RBAC, access permissions are assigned to roles and users obtain such permissions by being assigned to rules.

The distinctive feature of Core P-RBAC lies in the complex structure of privacy permissions, which reflects the highly structured ways of expressing privacy rules to represent the essences of OECD principles. Hence, aside from the data and the action to be performed on it, privacy permission explicitly states the intended purpose of the action along with the conditions under which the permission can be granted and the obligations that are to be finally performed. The notion of data profile is a key in our approach in that it records all information about data that are relevant for privacy enforcement. A data profile is organized as a record storing attributes, that is, properties about a data item or a set of data items.

4 d) AC #4 : Cryptography-Based Access Control

Cryptography access control is a new access control paradigm designed for information systems. It defines an implicit access control mechanism which relies absolutely on cryptography to ensure the data confidentiality and integrity. The basic idea of this access control is to provide a unique key for each resource type so that all users belonging to a class are assigned the key of that class [13]. Cryptography based access control mechanism is designed to operate in an open environment, where establishing the identity of the client suggests no information about the likely behavior of the client and, thus, is unrelated to the secure operation of the server.

5 e) AC #5 : Credential-Based Access Control

Traditional access control approaches are based on identity based authentication where it is assumed that the users are known to provide generally through a process of registration. In an open system environment where data is accessed by anyone anytime, centralized access control is not suitable [11].

User credentials are used to define access control policy and anyone who posses desired credentials is granted access to shared data source. The main advantage of credential-based access control is that it does not require central control and allows users to specify their own trust specification. It has been observed that various kinds of credentials are being used by existing applications and different credentials are found suitable in different environment such as identity credential, attribute credentials and standard credential. CBAC systems are based on authorization. Users do not need to specifically identify themselves, only their authority over a resource. Credentials enable departing from traditional authentication means avoiding the needs for users to remember logins and passwords, at the same time increasing the difficulty for adversaries of impersonating users and improperly acquire access priviledge.

Comparisons in Table **??** highlight several issues in the current access control. Assessment criteria have been derived from the access control in database system requirements discussed previously. The following summarize the criteria used to characterize the access control models as follows : a) Permission Decision Permission decision is a structure of the authorization in an access control model. Basic tuple of access control is ?subject, object, operation? paradigm was used in a traditional access control. A typical features of this criteria is that a way how the permissions decisions are represented as approvals of access to an object in specific access mode.

6 b) Policy Specification

Access control models are based on the specification and representation of policies that govern a database access system. The model should support the ways of specifying the access control policies and syntaxes, rules of languages that allows extension and modification in a simple and transparent manner. This helps to ensure the scalability of the model.

7 c) Authorization-Based

Authorization-based criteria define the way how the authorization is executed. In this case we examine Today, more people rely on online or web services in their daily life transactions such as buying groceries, renew driving license, even though checking their health. This may lead to increasing amount of PI disclosing via internet. The more data being disclose, the more owner lose his/her own privacy. This is because people will lose their control towards the PI once disclosing it. Data privacy is growing concern among businesses and other organizations in a variety sectors. A first important class of techniques deals with privacy preservation when data are to be released to third parties. In this case, data once are released are no longer under the control of the organizations owning them are made. to the -organization's data?. This access control focus on providing data subjects with means for defining access controls on their data, to help to ensure its confidentiality and so that the data may be used for the data subject's personal advantage.

Most of the current access control system focus on privacy-aware access control. But, due to the changes of consumer's perception of e-commerce, we have paid more attention in developing an access control which support open environment. Other than that, the notion of purpose is important in developing the access control model for privacy protection. This paper highlighted three basic requirements in proposing the access control system for e-commerce; purpose, individual control and the use of credential. This paper will give a better understanding and will be used as our future research in extending the current access control to a new one which it will be built based on those requirements. Our future research are trying to develop a privacy-aware access control system for e-commerce which applying all the requirements needed. [1] [2] [3]

Figure 1:

[1] © 2012 Global Journals Inc. (US) Global Journal of Computer Science and Technology Volume XII Issue IV Version I

[2] © 2012 Global Journals Inc. (US)

[3] © 2012 Global Journals Inc. (US) F ebruary

.

	Characteristics	AC #1	AC #2	AC #3	AC #4	AC #5
1	Policy specification	Identification-based Logic program	Object Data, Role, Purpose, Access	Roles, data, actions, Purpose,	Unique key	Credential
2	Authorization-based	Identity	Purpose	Role	Key	Identity/ attribute
3	Support Data Privacy (purpose)	N	Y	Y	Y	Y
4	Supporting environment	Open	Open	Open	Open	Open/ Close
5	Data Subject Involvement	Y	N	N	NA	N

the authorization rely on identity-based or other factors. Emerging trends in web-based applications and database technology where a large amount of data stored in a database, traditional access control which it refers to identity-based is not suitable anymore.
d) Support Data Privacy

Figure 2: Table . 2

.1 This page is intentionally left blank

[Agrawal et al. ()] , R Agrawal , J Kiernan , R Srikant . 2002a.

[Yang et al. ()] , N Yang , H Barringer , N Zhang . 2008.

[Chauduri et al. ()] , S Chauduri , R Kaushik , R Ramamurthy . 2011.

[Nirmal and Ruchi ()] 'Access Control Methodology For Sharing Of Open And Domain Confined Data Using Standard Credentials'. D Nirmal , V Ruchi . *International Journal on Computer Science and Engineering* 2009. 2009. 1 (3) p. .

[Samarati ()] 'Access control: Policies, models, and mechanisms'. V Samarati . *FOSAD'00: International School on Foundations of Security Analysis and Design*, 2001.

[Johnston et al. ()] *Authorization and Attribute Certificates for widely Distributed Access Control?*, William Johnston , Srilekha Mudumbai , Mary Thompson . 1998. IEEE WETICE.

[Bertino and Sandhu ()] E Bertino , R Sandhu . *Database Security -Concepts, Approaches, and Challenges. IEEE Transactions on Dependable and Secure Computing*, 2005. 2.

[Wasim and Al-Hamdani ()] 'Cryptography based access control in healthcare web systems'. A Wasim , Al-Hamdani . *Information Security Curriculum Development Conference*, 2010. 2010. p. .

[Database Access Control Privacy: Is there a Commom Ground? 5 th Biennial Conference on Innovative Data Systems Research] *Database Access Control & Privacy: Is there a Commom Ground? 5 th Biennial Conference on Innovative Data Systems Research. (CIDR '11)*,

[Hippocratic Database] *Hippocratic Database*, (Paper presented at the 28th)

[International Conference on Very Large Data Bases] *International Conference on Very Large Data Bases*, (Hong Kong, China)

[Lefevre et al. ()] 'Limiting Disclosure in Hippocratic Databases'. K Lefevre , R Agrawal , V Ercegovac , R Ramakrishnan . *Paper presented at the 30th international Conference on Very*, 2004.

[Barker ()] 'Personalizing access control by generalizing access control'. S Barker . *Proceeding of the 15th ACM symposium on Access control models and technologies*, (eeding of the 15th ACM symposium on Access control models and technologies) 2010. p. .

[Westin ()] *Privacy and Freedom*, A Westin . 1967. New York: Atheneum.

[Large Data Bases et al. ()] 'Privacy-aware role based access control'. Large Data Bases , Canada Toronto , Q Ni , A Trombetta , E Bertino , J Lobo . *Proceedings of the 12th ACM symposium on Access control models and technologies*, (the 12th ACM symposium on Access control models and technologies) 2007. p. .

[Byun and Li ()] 'Purpose based access control for privacy protection in relational database systems'. J.-W Byun , N Li . *The International Journal on Very Large Data Bases* 2008. 17 (4) p. .

[Byun et al. ()] 'Purpose based access control of complex data for privacy protection'. J Byun , E Bertino , N Li . *Symposium on Access Control Model and Technologies*, 2005. SACMAT.

[Brands ()] *Rethinking Public Key Infrastructures and Digital Certificates : Building in Privacy*, S A Brands . 2000. Cambridge, Massachusetts. (Document Number)

[Thompson and Essiari (2003)] 'Srilekha Madumbai, -Certificate-based Authorization policy in a PKI Environment?'. Mary R Thompson , Abdellilah Essiari . *ACM Transactions on Information and System Security (TISSEC)* November 2003. 6 (4) p. .