Privacy Protection Data Access Control

Min-Yu Chen[1], Chou-Chen Yang[1], and Min-Shiang Hwang[2]
(Corresponding author: Min-Shiang Hwang)
Department of Management Information Systems, National Chung Hsing University[1]
250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.
Department of Computer Science and Information Engineering, Asia University[2]
500 Liufeng Road, Wufeng, Taichung, Taiwan 402, R.O.C.
(Email: mshwang@asia.edu.tw)
(Invited Paper)

Abstract

For some purposes, such as benefits, requirement-fitted services and management, enterprises regularly ask customers, employees, and business partner to provide relevance data including sensitive personal information. However, transparent information bring the infringement of privacy and threats of living security to the data providers. Recently, enterprises have suffered from the loss of potential customers and benefits because of the rise of privacy protection consciousness. Therefore, this article researches in the solutions of data privacy protection in enterprises, and classifies into three categories, "*Role-based*", "*Purpose-based*", and "*Extension*". Furthermore, we define three criterions which should be achieved when an enterprise wants to implement a data access system with privacy protection mechanism. We hope it is helpful for enterprises to strengthen privacy protection depending on their own characteristics and requirements.

Keywords: Access control, privacy protection, purpose-based access control, role-based access control

1 Introduction

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 [5, 12]. Therefore, the enterprises, government and data providers need to raise privacy-aware consciousness. 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 [6].

In this paper, we classify the schemes in the domain of privacy protection access control to "*Role-based*", "*Purpose-based*", and "*Extension*". Traditional access models include mandatory access control (MAC), discretionary access control (DAC), and Non-discretionary access control. Role-based access control (RBAC) [23] is either a NIST standard [10] or an alternative measure of both MAC and DAC to directly aid function-based and job-based access control.

The RBAC model as Figure 1 consists of four entities: User, Role, Permission and Session.

User: User is a human being related to the entire internal and external enterprise system. All users, such as employees, customers, and business partners, have their own position and duty in an enterprise.

Role: Role is a named job title or job function which defines an authority level. If an user has been assigned and authorized a role (User Assignment; UA), he/she can exercise a permission to access specific data. The relations between users and roles are many-to-many, in other word, an user can belong to many roles, and a roles can assigned to many users. Figure 1 shows a special model in the framework, Role hierarchy (RH). Hierarchies are means for structuring the relations between roles to reflect an organization's lines of job function, class, and responsibility. For example, the relation through a superintendent, a primary-care physician, and a health-care provider in a hospital is a hierarchy structure. The senior-most role is that of superintendent, and a health-care provider is junior

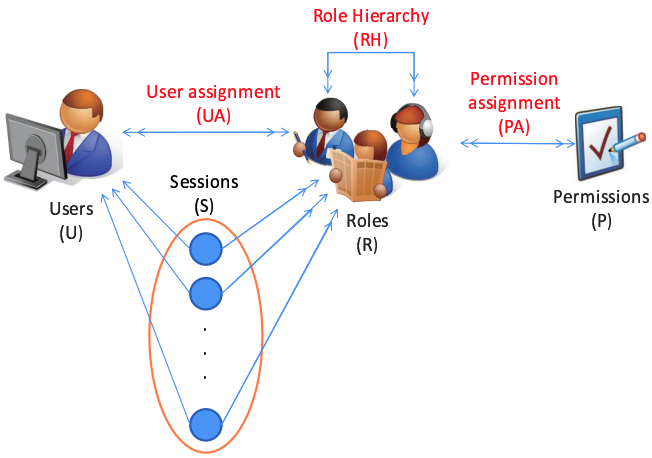

Figure 1: The conceptual models of an original role-based access control

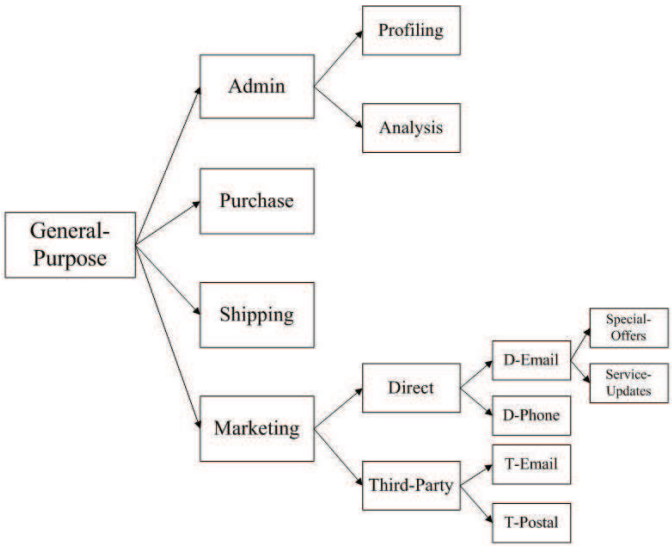

Figure 2: Purpose tree

to a primary-care physician. It means a superintendent could inherit all permissions from primary-care physician and health-care provider because of transitive inheritance.

Permission: A permission can be the terms authorization, access right, and privilege in the literature. Permissions confer on their holder the ability to perform an action such as read, write, and execute in the system. After assigned specific permissions (Permission assignment; PA), a role has rights to do operations designated in permissions to data. Based on many-to-many relation, A role can hold many permissions, and the same permission can be appointed to many permissions. If the data provider want to protect his/her sensitive privacy data, he/she could edit permissions for restricting rights or specific conditions to access data he/she own. For instance, a data provider, Bob can set a permission like "only the salesman can read Bob's personal information for marketing at 9 to 17 o'clock. In this example, Bob sets four restrictions on his personal information, including access operation "read", role assignment "salesman", specific purpose "marketing" ,and time period "9 to 17 o'clock". By this way to protect privacy of data providers, they could rely on their intention to adjusting permissions flexibly.

Session: Users can activate a subset of the roles simultaneously for establishing sessions. A user invoke the roles they belong to enable to accomplish tasks in a session.

RBAC is a wildly used approach to restricting system access to authorized users in computer system security. The permissions which perform certain operations of resources are assigned to specific roles. It means that RBAC regulates users' access based on rights and authorization of their roles. One of the reasons why we adopt RABC to protect privacy is its authorization management mechanism. RBAC is designed to meet the need of relieving the authorization management and immediately offering access control policies [21]. Therefore, more and more companies adopt the RBAC model for access and authority control using many commercial products (e.g. ORACLE database system, ORACLE IDM, IBM Tivoli IDM, and Sun IDM) and support services (e.g. Role Engineering and Role Mining) [18]. The permission is assigned by a data provider, and only authentic users playing the authorized role could access data. Because of the security policies of the organization and ability of privacy protection by using purpose restrictions, many researches combine these two fields to achieve the objective of privacy protection.

Another alterative for privacy protection in enterprises is the concept of purpose used as the basic element for data access control [1, 2, 7, 15, 16, 22, 27]. A data provider is able to make specific policies containing privacy-aware regulations with which must be complied as assigned data is accessed. Policy for preserving privacy might include purpose (e.g. marketing), condition (e.g. specific time period), retention (e.g. retaining time), and obligation (e.g. mail notification). The World Wide Web Consortium (W3C) developed the Platform for Privacy Preferences Project (P3P), a protocol which defines the purpose as "the reason(s) for data collection and use", and declared a set of purposes including current, admin, develop, contact, telemarketing [26].

In order to be convenient and applicable to business environments, a hierarchical purpose structure is created for representing relationships of purposes [8, 14, 17, 18]. Therefore, a set of purposes is organized in a tree structure referred to as Purpose Tree (See Figure 2), where each node and each edge represent a purpose and a hierarchical relation between two purposes. For instance,

assuming that p_i, p_j connected to each other is a subclass set of Purpose Tree, if $p_i > p_j$, we would say p_i is an ancestor of p_j, or p_j is a descendent of p_i, just like the relation between "Admin" and "Profiling" in Figure 2.

We define three criterions which should be achieved after consulting [4] when an enterprise wants to implement a data access system with privacy protection mechanism.

Flexibility: Because of individual factors, different persons have their own requirements for privacy protection. We consider that whether the methods we survey could provide a flexible mechanism for users to set their policies through their own requirement or not.

Data quality: Although privacy protection is an important issue for users, we are unwilling to see that enterprises could not collect enough information for researches or provide better services because of privacy protection policies. We consider that the methods we survey could either retain the data quality or protect a data provider's privacy.

Simplicity: The great majority of data providers are common people, but not program developers. The policy construction should be simple and easy to use, so that normal users can edit their own privacy policy for access control.

Next, we briefly introduce three directions of implementing data access control "*Role-based*", "*Purpose-based*", and "*Extension*". In Section 3, we utilize three criterions to put across features of each category. And then, we bring up future research issues in Section 4. Conclusions are in Section 5.

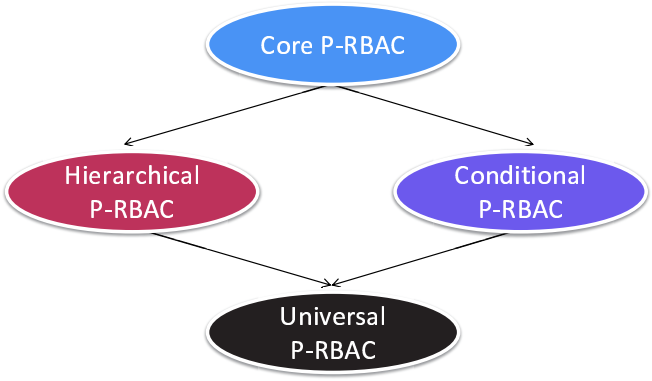

Figure 3: The family of conceptual P-RBAC models

2 Privacy Protection Data Access Control

2.1 Role-based Data Access Control

In [11, 18, 20] implement the notion of role-based access control for preserving private information by properly structured restriction. In [11], the confidentiality of personal identifiable information and protected health information is important for patients. The author presents a framework of RBAC with privacy-based extensions in e-Healthcare services. In [20], in order to practice in controlling access to sensitive data, such as electronic health record, the authors develop a Situation-Based Access Control (SitBAC) model. It not only protecting patients' privacy but also regulate the concerning data access used by employees. The above mechanisms devote to protect users' privacy in a particular environment by constructing an privacy-aware system using the concept of integration of the model of role-based access control.

In [18], the authors propose a comprehensive framework applying a family of privacy-aware role-based access control (P-RBAC) as Figure 3 to enforce access control to data containing personal or sensitive privacy information. A family of role-based access control models is the key feature that extends classical RBAC on taking into account purposes and obligations.

There is four models in the family: core, hierarchical, conditional, and universal P-RBAC.

Core P-RBAC models includes five basic elements: Users, Roles, Objects, Operations, and Permissions as via 4. Core P-RBAC is based on Core RBAC [10] without the session component. Hierarchical P-RBAC models and Conditional P-RBAC models extend Core P-RBAC with advantages of additional components to be appropriate for various requirements of different enterprises. In [11], the entity "User" refers to persons who may use the e-Healthcare service system including doctors, patients, administrators, and insurance companies, etc., and "Role" is the job title or job function of an user. "Object" refers to attributes (e.g., salary, age, and department etc.) related to users or something essential (e.g. e-mail) in processes of data access control. After defining entities above in advance, if an user is about to do "Operation"(e.g., read/write) on privacy data such as protected health information, the "Permission" set up by data owners define restrictions such as specific role, object, condition, and obligation, etc..

Hierarchical P-RBAC models contain Role Hierarchical (RH), Object Hierarchical (OH), and Purpose Hierarchical (PH). We survey some papers of hierarchical applications, such as [9] defined clearly about the role relationships, abuse inheritance, and security principles. The authors of [8, 14] use the concept of hierarchical purpose to protect the privacy of users. The concept of a hierarchical structure is an order relation between two different individuals. For instance, given two roles $R_1 \in R_2$, if a policy defines the data access authority to R_1, R_2 could inherit this permission to get the data access authority because of a higher role level than R_1.

Conditional P-RBAC models [19] provide permission assignment sets and complex Boolean expressions. Conditional P-RBAC models support not only new context variable types like string and integer, but also logical operators like negation and disjunction.

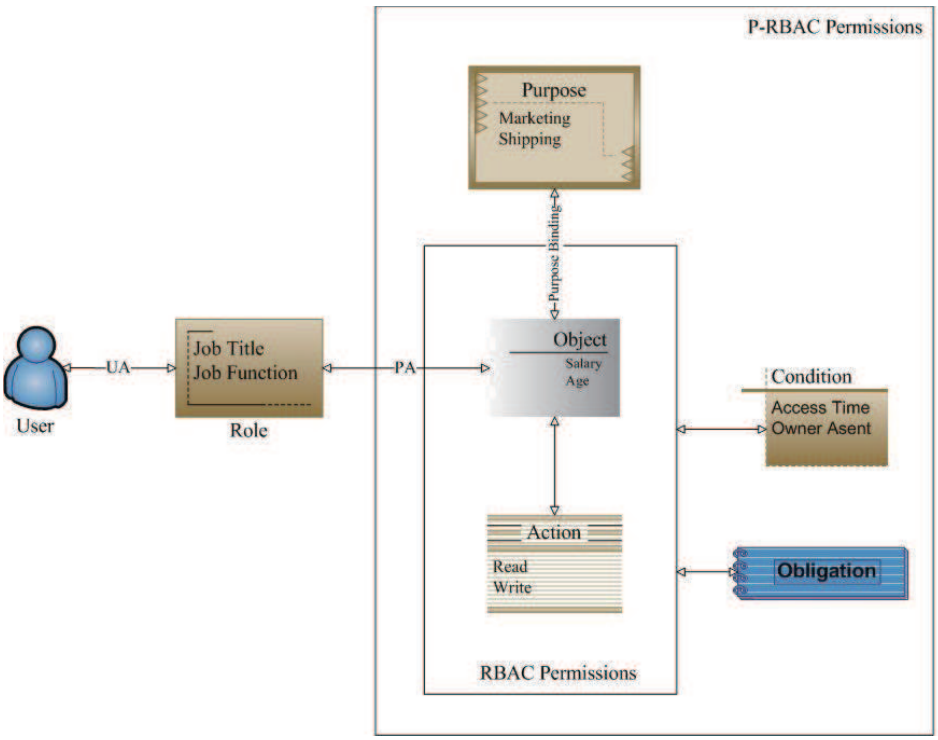

Figure 4: Core P-RBAC model

Universal P-RBAC combines the character of either Hierarchical P-RBAC or Conditional P-RBAC, and provides additional three features, negative permissions, flow control for obligation execution, and permission combination principles.

In conclusion, after historical development, researchers combine role-based access control with privacy protection mechanism to construct the family of four models for supporting demands components strongly.

2.2 Purpose-based Data Access Control

In [7, 13, 14, 24, 25] propose mechanisms for privacy preserving access control based on variety of purposes. In order to protect the privacy of individuals, a number of work has showed that the notion of purpose used for specifying privacy policies. In access management systems, purpose is considered as the reason to collect or to access private data. Data providers can preserve their own private or sensitive information by restricting the intended purpose of data access. By this way, data providers immediately avoid the threat of data abuse on unwilling purposes. For instance, Bob could prohibit receiving marketing advertisement from salesman from denying the right to access his address for marketing purpose.

In the recent paper [14] presents a method of defining a conditional purpose as the intention of data accesses or usage under certain conditions. The authors utilize the purpose definition which describes the intentions for data access and data collection from [8]. An intended purpose is composed of the following three components:

Allowable Intended Purpose (AIP) indicates that the data provider allows accessing the data for a specific purpose without any restriction.

Conditional Intended Purpose (CIP) indicates that the data provider allows accessing the data for a specific purpose with some conditions such as hiding personal privacy information.

Prohibited Intended Purpose (PIP) indicates that the data provider absolutely disallows accessing the data for a specific purpose.

The three components (AIP, CIP and PIP) are set as the intended purpose by the data provider. Access purpose must comply with the intended purpose for authorization of data access. Combining the advantages of RBAC [23], it achieves the compliance computation between intended purpose and access purpose. Moreover, it provides more possible options for privacy protection and maximizing the usability of data.

For instance, in Table 1, Group 1, Group 2 and Group 3 have their own authorization setting for data access. Group 1 gives consent for all general purpose, Group 2 conditionally gives consent for purchasing, and Group 3 doesn't give consent for marketing.

Table 1: Predetermined intended purposes

	Group 1	Group 2	Group 3
Name	$\langle\{G\},\{0\},\{0\}\rangle$	$\langle\{G\},\{P\},\{0\}\rangle$	$\langle\{G\},\{0\},\{M\}\rangle$
Address	$\langle\{G\},\{0\},\{0\}\rangle$	$\langle\{G\},\{P\},\{0\}\rangle$	$\langle\{G\},\{0\},\{M\}\rangle$
Phone	$\langle\{G\},\{0\},\{0\}\rangle$	$\langle\{G\},\{P\},\{0\}\rangle$	$\langle\{G\},\{0\},\{M\}\rangle$
Age	$\langle\{G\},\{0\},\{0\}\rangle$	$\langle\{G\},\{P\},\{0\}\rangle$	$\langle\{G\},\{0\},\{M\}\rangle$
Income	$\langle\{G\},\{0\},\{0\}\rangle$	$\langle\{G\},\{P\},\{0\}\rangle$	$\langle\{G\},\{0\},\{M\}\rangle$

G=General purpose, T=Third-Party, 0=No restriction

After it defines the authorization of data access, the term "conditions" means that data could be used in some restrictions (e.g. specific period) or in scope expansion. For instance, Table 2 shows conditional records and intended purposes of a data provider John.

Table 2: Conditional records and intended purposes

	Name	Age	Address	Income
AIP	John	35	100,West St.,FY. Taichung	10,000
CIP	J	30-40	FY. Taichung	5,0000-15,0000
PIP	*	*	*	*

$*$ means unallowable data access

2.3 Extension Mechanisms

In this category, there are different methods from the mechanism on the basic of the role-based and the purpose-based data access control. The papers, [3, 8, 22], direct toward the improvement of efficiency and efficacy on incorporating privacy protection into database systems. Although the notion of purposes has been utilized wildly and long, it is a complicated issue about the management of attributes and users purposes. For simplification, individual user is assigned to map roles, and permissions including access purpose are granted to roles. In order to support dynamic changes in purpose, attributes with hierarchy inheritance features are distribute to roles. For instance, at the begin, the salesman is assigned an attribute of task as "D-Email" or "D-Phone" because of Purpose Tree 2 which includes "D-Email" and "D-Phone". If Purpose Tree need to add a new task as a subtree of Direct marketing "D-Meet" and change some salesman's task to "D-Meet", the management of attributes and users purposes would be complicated because of the hierarchical structure of role and purpose.

In [8], the authors propose the model which makes the intended purpose of data usage associated with the data element. A key feature of the model is that multiple purposes are allowed to be associated with each data element, as well as prohibitive intended purposes. They use the context of relational databases and propose four different labelling schemes for the issue whose purposes can be associated with the unit of data, namely the granularity of data labelling. Assuming that R is the set of roles, P is the set of purposes, IP is all of the intended purpose by definition ($ip \in IP$, l is a column having IP for its domain), and A_i is an attribute of R.

Relation-based is a pair $\langle R, ip\rangle$. Each ip governs the access to every data element in instances of R (See Table 3 and Table 5).

Attribute-based is a set $\langle A_i, ip_i\rangle$ Each ip_i governs the access to each data element A_i in any instance of R (See Table 4 and Table 5).

Tuple-based is a relation scheme Rtl(A_1, A_2, ..., A_n, l), such that $R = \prod_{A_1,...A_n}(Rtl)$. The l_j governs the access to each instance of R (See Table 6).

Element-based is a relation scheme Rel(A_1, l_1, A_2, l_2, ..., A_n, l_n), such that $R = \prod_{A_1,...A_n}(Rel)$. The l_i governs the access to data element A_i in each instance of R (See Table 7).

Table 3: Access-Log table

Client IP	Date	Time	URL
120.23.54.9	11/01/2012	17:45:11	/index.html
111.45.31.1	12/02/2011	13:11:55	/login.html
123.221.34.89	02/01/2013	18:18:8	/app.html

Table 4: Order table

Order ID	Product	Date	Status
101	P465	07/11/2012	Shipping
102	P788	08/12/2012	Packaged
103	P222	11/11/2012	Ordered

Table 5: Privacy-Policy table

Table Name	Column Name	IP
Order	Order ID	$\langle\{A,P,S\},0\rangle$
Order	Product	$\langle\{P\},\{M\}\rangle$
Order	Date	$\langle\{A,P,S\},0\rangle$
Order	Status	$\langle\{A,P\},0\rangle$
Access-Log	ALL	$\langle\{A,P\},0\rangle$

Table 6: Address table

Customer ID	Street	City	State	Addr_IP
1001	32 Oval Dr.	Taichung	Taiwan	$\langle\{G\},\{A,M\}\rangle$
1002	44 State Rd.	Taipei	Taiwan	$\langle\{G\},0\rangle$
1003	199 First Ave.	Boston	CA	$\langle\{G\},\{T\}\rangle$

Table 7: Customer table

Customer ID	C_ID_IP	Name	Name_IP
1001	$\langle\{G\},0\rangle$	Becky	$\langle\{G\},\{M\}\rangle$
1002	$\langle\{G\},0\rangle$	Allen	$\langle\{G\},\{0\}\rangle$
1003	$\langle\{G\},0\rangle$	Jim	$\langle\{G\},\{T\}\rangle$

In this category, researchers improve the efficiency and efficacy on incorporating privacy protection into database systems. The authors of [8] proposed an efficient method for settling access purposes and presented four labelling schemes providing a different granularity.

3 Comparison

In this paper, we define three directions of the way of preserving privacy, role-based, purpose-based, and extension data access control. There are both positive and negative effects in these three direction. Therefore, we synthesize three criterions of privacy protection data management system implementation.

In this paper, we classify the data privacy protection schemes into three categories, "Role-based", "Purpose-based", and "Extension". Role-based schemes have developed for a long time, so their capability, expansibility, and development degree are integral. Purpose-based schemes utilize the notion of purpose limitation, they are clear and easy to understand for customers, employees, and correlative data providers. Extension schemes direct toward the improvement of efficiency and efficacy on incorporating privacy protection. After researching on these three domains of schemes, there are three significant and major factors we synthesize on constructing an data access control system for preserving privacy of data providers. Finally, The comparison of these three factors with above classifications are shown in Table 8.

Flexibility:
Qun et al. [18] provide either conditions or obligations for users to edit own policies, and they propose some condition language for additional options like "OwnerConsent", "OwnerAge", and "CurrentTime". A data provider can track privacy data by defining obligations such as requesting who should send E-mail to the data provider when accessing the specific data. Because of condition language and obligations, Qun et al. make their method flexible.

Data Quality: Because of conditions and obligations, Qun et al. [18] let users not only allow or prohibit data access but choose to set obligations if data is not private but sensitive enough for a data provider. They make data quality good for data collection.
Besides allowance and prohibition, Enamul et al. [14] provide another option, conditional intended purposes, so data providers can dim privacy data (e.g. personal information) from an exact number to a broad range. It is acceptable for users to protect their privacy data, and it slightly makes data quality up.

Simplicity: Qun et al. [18] propose a family of conceptual models composed of four function models, core, hierarchical, conditional, and universal P-RBAC. Each model is responsible for specific useful functions, and users have to set the policies including appointing the desire demands. Thanks for an easy-to-use tool provided by Qun et al., users can edit policies in natural language. By compiling natural language, it automatically transfers a sentence to a policy in XACML format, so it is simple for users except some additional conditional variable needed to memorize. Similar to Enamul et al.'s method, Ji-Won et al. [8] need users to complete configurations of allowable and prohibitive intended purpose. Ji-Won et al. focus on the effective manner to store data with intended purpose indicated in Section 2, so it is the simplest of three methods we survey.

4 Future Research

In this article, we introduce the recent development of privacy-aware data access control, in order to be suitable for enterprise applications and users' requirement, researchers proposing a specific scheme such as additional condition and obligation support, conditional data presentation, and efficacy promotion in a relational database system. However, there are several issues worth researching and developing in the future as followings.

Data Security: No matter how secure a system is, it must exist some security loopholes or weakness which might be attacked or invading in the system. We should establish a data protection mechanism for sensitive and private data such as encryption. For another situation, a user belonging the role can do definite operations to specific data if the role have particular permissions, but if users need to store data in files for particular situations like a travel on business, the portability of data might be a secret worry.

Table 8: Comparison table

	Role-based as [18]	Purpose-based as [14]	Extension as [8]
Flexibility	**Flexible** (+) Condition language (+) Obligations	**Inflexible** (-) Fixed purpose (-) Unchangeable relation	**Inflexible** (-) Fixed purpose (-) Unchangeable relation
Data quality	**Good** (+) Condition (+) Obligations	**Normal** (+) Conditional intended purposes	**Bad** (-) Simple allowance and prohibition
Simplicity	**Normal** (-) Four function models (+) Easy-to-use tool (+) Natural language	**Normal** (+) Purpose setting (+) Substitution range (-) Lengthy process	**Simple** (+) Purpose setting (+) Effective

Deception: Most schemes of privacy-aware access control are based on the user of trust; therefore, purposes in access control policy are used by data requesters oneself. If data requesters lie for illegal objectives, it could be difficult to detect and dangerous for user privacy data. It needs an entire mechanism to ensure that data requesters certainly utilize data for specific purposes they assign. Nevertheless, even a perfect mechanism has been constructed, and it cannot entirely stand against the malicious attack from adversaries. Therefore, we can adopt passive detection instead of active limitation. For instance, recording each private data access for tracking, it would be described later.

Infringement Detection: Like every protection system such as IDS, IPS, and firewall, etc., if we apply an infringement detection to a privacy protection in data access, it could strengthen the trust of data providers. Generally, a detection system includes four steps. At first, it collects all related data records, and we could follow it as an example to collect all data access records including a privacy infringement behavior. Second, it should define characteristics which can represent the features of infringement caution like times of data access, user login record, and error occurrence. Third, it analyzes statistics for a possible malicious behavior such as massive data access, irregular authorization, and periodical error, etc.. Finally, it configures the setting of thresholds to warn system administrators, related employees, and even data providers.

5 Conclusion

In this article, we are conscious of privacy aware, and there are various methods proposed by many researchers. We introduce three directions with representative papers and analyze them by three criterions which could represent the important features of privacy protection in a data access control scheme. These three categories have their respective features and advantages for improving completeness of privacy protection in data access control.

Since the new electronic age has come, the electronic storage documents have replaced the paper records in the way to convey and store information. However, unsheltered transparent information bring the infringement of data providers' privacy. By the privacy-aware trend, researchers have developed in-depth and wide schemes for preserving privacy of information. We roughly classify the data access control schemes for privacy protection into three categories, "Role-based", "Purpose-based" and "Extension". On implementing an data access control system for preserving privacy of data providers, we define three factors, "flexibility", "data quality", and "simplicity" to make the comparison of factors with above three classifications. Through this article, we hope it is helpful for researchers, enterprises, and customers to understand the importance of privacy protection and strengthen privacy protection depending on their own characteristics and requirements.

References

[1] R. Agrawal, P. Bird, T. Grandison, J. Kiernan, S. Logan, and Y. Xu, "Extending relational database systems to automatically enforce privacy policies," in *21st International Conference on Data Engineering*, pp. 1013–1022, Tokyo, 2005.

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Hippocratic databases," in *28th International Conference on Very Large Databases*, pp. 143–154, Hong Kong, 2002.

[3] S. S. Al-Fedaghi, "Beyond purpose-based privacy access control," in *ADC'07 Proceedings of the Eighteenth Conference on Australasian Database*, vol. 63, pp. 23–32, 2007.

[4] C. A. Ardagna, M. Cremonini, S. De, Capitani Vimercati, and P. Samarati, "A privacy-aware access control system," *Journal of Computer Security - 20th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec'06)*, vol. 16, no. 4, pp. 369–397, September 2008.

[5] B. S. Babu and N. Jayashree and P. Venkataram, "Performance analysis of Steiner tree-based decentralization mechanism (STDM) for privacy protection in wireless sensor networks," *International Journal of Network Security*, vol. 15, no. 5, pp. 321–330, 2013.

[6] S. Barker and P. J. Stuckey, "Flexible access control policy specification with constraint logic programming," *ACM Transactions on Information and System Security*, vol. 6, no. 4, pp. 501–546, 2003.

[7] J. W. Byun, E. Bertino, and N. Li, "Purpose based access control of complex data for privacy protection," in *10th ACM Symposium on Access Control Model and Technologies*, pp. 102–110, Stockholm, 2005.

[8] J. W. Byun and N. Li, "Purpose based access control for privacy protection in relational database systems," *Information Systems Frontiers*, vol. 17, no. 4, pp. 603–619, 2008.

[9] W. Cai, R. Huang, X. Hou, G. Wei, S. Xiao, and Y. Chen, "Atom-role-based access control model," *IEICE Transactions on Information and Systems*, vol. E95.D, no. 7, pp. 1908–1917, 2012.

[10] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed standard for role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 224–274, 2001.

[11] P. C. K. Hung, "Towards a privacy access control model for e-healthcare services," in *Third Annual Conference on Privacy, Security and Trust*, Oct. 2005.

[12] W. S. Juang and J. L. Wu, "Efficient user authentication and key agreement with user privacy protection," *International Journal of Network Security*, vol. 7, no. 1, pp. 120–129, 2008.

[13] E. Kabir, H. Wang, and E. Bertino, "A conditional purpose-based access control model with dynamic roles," *Expert Systems with Applications*, vol. 38, pp. 1482–1489, March 2011.

[14] E. Kabir, H. Wang, and E. Bertino, "A role-involved purpose-based access control model," *Information Systems Frontiers*, vol. 14, no. 3, p. 809, 2012.

[15] K. Lefevre, R. Agrawal, V. Ercegovac, R. Ramakrishnan, Y. Xu, and D. DeWitt, "Disclosure in hippocratic databases," in *30th International Conference on Very Large Databases*, Toronto, pp. 108–119, 2004.

[16] C. T. Li, M. S. Hwang, Y. P. Chu, "Further improvement on a novel privacy preserving authentication and access control scheme for pervasive computing environments," *Computer Communications*, vol. 31, no. 18, pp. 4255-4258, Dec. 2008.

[17] J. W. Lo, M. S. Hwang, C. H. Liu, "An efficient key assignment scheme for access control in a large leaf class hierarchy," *Information Sciences*, vol. 181, no. 4, pp. 917-925, Feb. 2011.

[18] Q. Ni, E. Bertino, J. Lobo, C. Brodie, C. Karat, J. Karat, and A. Trombetta, "Privacy-aware role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 3, July 2010.

[19] Q. Ni, D. Lin, E. Bertino, and J. Lobo, "Conditional privacy-aware role-based access control," in *Proceedings of the European Symposium on Research in Computer Security*, Springer-Verlag, Berlin, pp. 72–89, 2007.

[20] M. Peleg, D. Beimel, D. Dorib, and Y. Denekamp, "Situation-based access control: Privacy management via modeling of patient data access scenarios," *Journal of Biomedical Informatics*, vol. 41, pp. 1028–1040, Dec. 2008.

[21] H. C. Peng, J. Gu, and X. Ye, "Dynamic purpose-based access control," in *Parallel and Distributed Processing with Applications, 2008. ISPA '08. International Symposium on*, pp. 695–700, 10-12 Dec. 2008.

[22] C. S. Powers, P. Ashley, and M. Schunter, "Privacy promises, access control, and privacy management," in *3rd International Symposium on Electronic Commerce*, North Carolina, pp. 13–21, 2002.

[23] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer archive*, vol. 29, no. 2, pp. 38–47, 1996.

[24] L. Sun and H. Wang, "A purpose based usage access control model for e-healthcare services," in *International Conference on Data and Knowledge Engineering (ICDKE 2011)*, pp. 41–46, Sept. 2011.

[25] L. Sun and H. Wang, "A purpose-based access control in native xml databases," *Concurrency and Computation: Practice and Experience*, vol. 24, pp. 1154–1166, July 2012.

[26] World Wide Web Consortium (W3C). "Platform for privacy preferences (p3p)", Technical Report (http://www.w3.org/P3P).

[27] N. Yang, H. Barringer, and N. Zhang, "A purpose-based access control model.," in *3rd International Symposium on Information Assurance and Security*, Manchester, pp. 143–148, 2007.

Min-Yu Chen was born in Taichung County, Taiwan, in 1989. He received the B.M. degree from National Chiayi University (NCYU), Chiayi, in 2011 in management information systems. He is currently pursuing the M.S. degree with the Department of Management Information Systems from National Chung Hshing University (NCHU), Taichung. His research interests include electronic commerce, access control, information security, and point-to-point system of mobile technology.

Chou-Chen Yang received his B.S. in Industrial Education from the National Kaohsiung Normal University, in 1980, and his M.S. in Electronic Technology from the Pittsburg State University, in 1986, and his Ph.D. in Computer Science from the University of North Texas, in 1994. From 1994 to 2004, Dr. Yang was an associate

professor in the Department of Computer Science and Information Engineering, Chaoyang University of Technology. Currently, he is a professor in the Department of Management Information Systems, National Chung Hshing University. His research interests include network security, mobile computing, and distributed system.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. He was a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He obtained 1997, 1998, 1999, 2000, and 2001 Outstanding Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 170+ articles.