Performance-Aware Trust-Based Access Control for Protecting Sensitive Attributes

Mohd Rafiz Salji[1,2(✉)], Nur Izura Udzir[1], Mohd Izuan Hafez Ninggal[1], Nor Fazlida Mohd. Sani[1], and Hamidah Ibrahim[1]

[1] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Seri Kembangan, Malaysia
mohdrafiz@sarawak.uitm.edu.my
[2] Faculty of Information Management, Universiti Teknologi MARA, Shah Alam, Malaysia

Abstract. The prevailing trend of the seamless digital collection has prompted privacy concern not only among academia but also among the majority. In enforcing the automation of privacy policies and law, access control has been one of the most devoted subjects. Despite the recent advances in access control frameworks and models, there are still issues that impede the development of effective access control. Among them are the lack of assessment's granularity in user authorization, and reliance on identity, role or purpose-based access control schemes. In this paper, we address the problem of protecting sensitive attributes from inappropriate access. We propose an access control mechanism that employs two trust metrics name experience and behavior. We also propose a scheme for quantifying those metrics in an enterprise computing environment. Finally, we show that these metrics are useful in improving the assessment granularity in permitting or prohibiting users to gain access to sensitive attributes.

Keywords: Behavior-aware · Trust-based access control · Sensitive attributes · Privacy protection

1 Introduction

Privacy is increasingly becoming one of the very important issues in data management. People are now more conscious about how their information are being secured and protected by service providers. This awareness has been getting more highlights when sharing and collecting of information become seamless and prevalent by the omni-present of internet connection. In common situation, companies or data keepers are required to allow access to the information reside within the information systems to multitude of users. The administrator may allow the users to access to the information in supporting decision making or analysis activities.

Many efforts have been made in terms of enforcing the automation of privacy policies and law. In providing the solution, most of works have been focusing on access control in which the access authorization to a source is selectively permitted. It

T. Herawan et al. (eds.), *Recent Advances on Soft Computing and Data Mining*, Advances in Intelligent Systems and Computing 549, DOI 10.1007/978-3-319-51281-5_56

is important that every information systems are equipped with an access control mechanism to ensure that access to personal information is in accordance with company policies [3, 5, 8, 9, 11, 16–18]. Despite the recent advances in access control frameworks and models, there are still issues that impede the development of effective access control models such as the lack of assess granularity in authorizing, and reliance on identity, role or purpose-based access control schemes.

One of the many access control mechanisms, Trust-based Access Control (TBAC) is an access control model that is inspired by an important role in human life, which is trust. By this concept, a user that is highly trusted will be granted more accessibility to a source as compared to lower thereof. However, trust is mutable in response to the changings of situations. Therefore, it is paramount important to design an efficient access control model that is able to capture the dynamic nature of user behavior with regards to trustworthiness.

This paper addresses the issue of protecting sensitive attributes from inappropriate access that can causes privacy disclosure. We propose an access control scheme that embraces two trust metrics named experience and behavior with respect to the user. In order to deal with the dynamic nature of trust, we design a scheme that engages with the continuous process of updating and measuring user behavior in an organization. This involves a comprehensive policy that is devised from the combination of existing access control policies and other resources for determining the level of trust. Three factors have taken into consideration to bridge the trust relationship between a user and the system; properties, experience and recommendations. By using the proposed mechanism, the system is able to identify whether an access request to sensitive attributes is permitted or denied. Authorized user with lower level of trust is still granted to access personal information, but user with preferred experience and behavior will be allowed to access to sensitive attributes. In summary, the main contributions of this paper are as follows:

(a) We propose a new access control model based on trust to protect sensitive attributes.
(b) We identify two trust metrics called behavior and experience to be used as decision factor in controlling access to sensitive attributes.
(c) We propose a quantification method to deal with the dynamic nature of trust.

The rest of this paper is organized as follows: Sect. 2 provides the related works. The proposed method is then presented in Sect. 3. We discuss the result in Sect. 4 and finally, Sect. 5 concludes the work.

2 Related Works

Trust-based access control models have been explored in many distributed computing environments.

In previous work, situational trust is defined as the security of a location by using a level of trust, which limits the documents that can be sent to or observed at that location [7]. The main focus of Performance-Aware Trust-Based Access Control for Protecting

Sensitive Attributes (PATBAC) is to secure sensitive attributes by using a level of seniority and behaviour as a trust.

To access high risk resource, the system needs to filter the user with a certain degree of trust. A multi delegation model with trust management has been proposed to permit or prohibit access to the access control system. Three levels of delegated tasks are organized; low (less trust), medium (intermediate trust) and high (highly trust) [12]. A higher level of delegation task is assigned to the delegate if they have a higher trust level. In PATBAC, the system have to check a user role performance *rp* which comprises with the levels of seniority and behaviour. Two levels of user seniority (junior (less trust) or senior (highly trust)) and three levels of user behaviour (mistrust (junior), trust (senior) or uncertainty (senior performing negative behaviours)) are organized. All authorized users are permitted to access personal information but the user with a higher level of *rp* (senior-with-trust) are able to access sensitive attributes.

In access control model with trust management, the user with a higher trust level have more privileges compared to other levels and the user who are unauthorized will be restricted access to the system. Trust into role based access control model (TRBAC) has been proposed where user with good behaviour will be rewarded with the higher level of trust and they are permitted to access more resources, while malicious users' authorizations may be revoked [22]. The same concept is proposed in PATBAC where the user who is assigned as a higher level of *rp* are able to access more resources.

To specify the user's trust value, the system needs to quantify their performance in substantive service. The user performance is calculated by using the history and recommendation [13, 14]. The history or experience of user is stored in the User Role History (URH) [20]. In PATBAC, URH is assigned to store and calculate automatically the user experience or activity in their substantive service. Moreover, Evaluation Form (EF) is assigned to evaluate the user behaviour and it is based on recommender evaluation. URH and EF may represent values in range [0, 1], which are taken directly from system measurements [2].

Generally, trust can be changed from time to time. This change may invoke user from ongoing access. It can be invoked manually or automatically, depending on the trust evaluation concept set by the administrator [19, 20]. In PATBAC, if the user performs negative behaviour, the administrator will change the user role trust attribute manually. It means that even the user role status is senior, if the role trust attribute is changed to uncertainty, the user is not permitted to access sensitive attribute. The user can apply for the role trust as trust after a certain period of time set by the administrator. If the user has attained a certain period of time, they are allowed to request for re-calculation of their behaviour.

3 Performance-Aware Trust-Based Access Control (PATBAC)

In this section, we propose our method. We first present the trust metrics and discuss about its function in building trust relationship between user and the system. We then present our method to quantify those metrics in enterprise computing system.

3.1 Trust Metrics

Each role in the organization requires certain properties of a user. The properties of a user in PATBAC are referring to the user experience and behaviour, and the explanation of those metrics is as follows:

a. **User Experience**

- Refers to the number of the user activities that is performed during their substantive service.
- It is assigned to specify the seniority of a user.
- It can be set at the role status attribute in the user personal details.
- Two levels of user seniority: junior (less trust) and senior (highly trust).

b. **User Behavior**

- Refers to the user attitude shown during their substantive service. The scope of the user behaviour in this model refers to the categories that is introduced by Bruhn [4] in Table 3.
- It is assigned to specify the behaviour of a user.
- Recommendations are assigned to quantify the user behaviour and the result is supplied in the role trust attribute at the user personal details.
- Three levels of user behaviour: mistrust (junior), trust (senior) and uncertainty (senior performing negative behaviours).

Role performance *rp* refers to the trust degree of a user based on the level of seniority and behaviour to access sensitive attributes. If the *rp* of a user is junior, the system will automatically assign as mistrust and s/he is not allowed to access sensitive attributes. Similar to the role *rp* of a user is senior-with-uncertainty, s/he is also restricted to access sensitive attributes. However, if the *rp* of a user is senior-with-trust, s/he is permitted to access sensitive attributes.

3.1.1 Quantification of User Experience

Experience refers to the number of activities calculated by a system regarding a user activity in their substantive service. The activities that is participated by a user for example, seminar, workshop, courses and others that is determined by the organization. Different department performs different activities. The calculation of a user's experience is perform by using weighing evidence [6].

Weighing Evidence

Weighing evidence is a decision process to specify the seniority of a user. The administrator needs to identify how many activities to be set to identify the activeness of a user. Each of these components has a value between [0, 1] and the sum of these components is 1. The minimum required weight should be set by the administrator to identify either a user is granted or denied to be a senior.

Let m denote the total amount of each activity and w is the total number of activities. The total sum of m is calculated $(m_i + \ldots + m_j)$. Then, sum of m is divided by w to obtain the result of a user activities ua. The result is in the range of [0, 1]. The ua is calculated as in Eq. 1.

$$\frac{\sum_{i=1}^{j} i}{w} \in [0, 1] \tag{1}$$

Hence, the administrator a have to decide the minimum required weight of ua. If the result of ua is more than the required weight set by a, user u able to be assigned as senior role.

Assume the minimum required weight set by the administrator is 0.4 and a user Alice's overall score is 0.5. This means that she is permitted to assign as senior role. Based on Table 1 [21], Alice's overall score are in Level 3, i.e. the activeness of Alice is average.

Table 1. Indicator of the user activeness

Value	Meaning	Activeness score
Level 0	Totally inactive	0
Level 1	Inactive	0.1–0.19
Level 2	Minimal	0.2–0.39
Level 3	Average	0.4–0.59
Level 4	Active	0.6–0.79
Level 5	Very active	0.8–1

In PATBAC, calculation of user's experience is not enough to assign a user as trustworthy. A user's behaviour will be evaluated by recommendations to permit access to sensitive attributes.

3.1.2 Quantification of User Behaviour

Recommendations are assigned by the administrator to evaluate a user behaviour. User behaviour is evaluated in the evaluation form (EF) (Table 3). A user behaviour categories is applied in this research to specify the user behaviour [4]. Table 2 has become an indicator to facilitate the recommender to evaluate a user trust behaviour based on categories [21]. The value of each category is between [0, 1] and the sum of these categories is 1. For example, if recommender A evaluates user B on the category of open, participative, accept responsibility, recommender A needs to place a mark in that category. Assume recommender A gives a score to a user B in that category is 0.5, it means that user B is in Level 3, which the score on that category is average. Scores will be placed in the user evaluation form as illustrated in Table 3.

Let b denote the total amount of each behaviour category and c is the total number of behaviour categories. The sum of b is $(b_i + \ldots + b_k)$. Then, total sum of b is divided by c to obtain the result of a user behaviour ub. The result is in the range of [0, 1]. The ub is calculated as in Eq. 2.

Table 2. Indicator of a user trusted behaviour based on categories

Level	Meaning	Trust range
Level 1	Very poor	0–0.19
Level 2	Poor	0.2–0.39
Level 3	Average	0.4–0.59
Level 4	Good	0.6–0.79
Level 5	Very good	0.8–1

Table 3. User behaviour evaluation form

No.	Categories	Mark
1.	Open, participative, accept responsibility	
2.	Highly productive	
3.	Loyalty to the organization	
4.	Not defensive	
5.	Cooperation, work teams	
6.	High job satisfaction	
7.	Problem-solving attitude	
8.	Involvement in decision-making	
9.	Sense of pride in work	
	Total mark	
	Total mark/9	

$$\frac{\sum_{i=1}^{k} i}{c} \in [0, 1] \tag{2}$$

Hence, the administrator *a* have to decide the minimum required weight of *ub*. If the result of *ub* is more than the required weight set by *a*, user *u* can be assigned as trust.

Scores for each category will be added first and divided by a number of categories to obtain an overall score. Combinations from the notions of Kim et al. and Vidyalakshmi et al. [10, 21], the level of a user trusted behaviour for the overall score is illustrated as in Table 4. For example, assume a user Carol obtains the overall score 0.7. Based on Table 4, Carol is in Level 4, which is good. If the minimum requirement set by the administrator is 0.6, she is qualified to be assigned as trust.

3.2 Access Control Mechanism

Figure 1 shows the process of access control model using *rp* as a trust to access sensitive attributes and the explanations are as follows:

1. User: User in this model refers to the staff. User is requested to access privacy in the system. First, user needs to sign in using user identification and password.

Table 4. Levels of a user trusted behaviour for overall score

Value	Meaning	Explanation	Trust range
Level 0	Distrust completely	Untrustworthy	0
Level 1	Ignorance	Cannot decide	0.1–0.19
Level 2	Minimal	Lowest trust	0.2–0.39
Level 3	Average	Mean trustworthiness	0.4–0.59
Level 4	Good	Trusted by major population	0.6–0.79
Level 5	Fully trust	Fully trustworthy	0.8–1

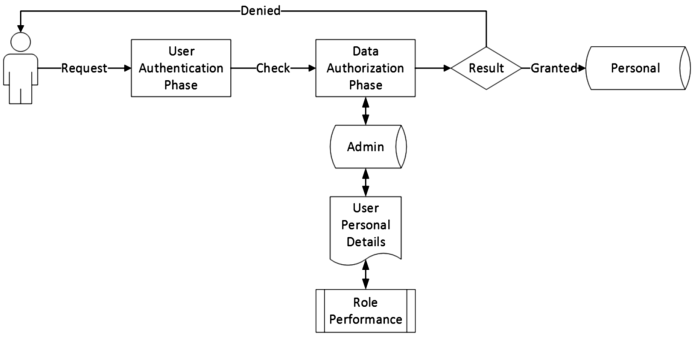

Fig. 1. Role performance trust-based access control

2. User authentication phase: This is the first stage in access control mechanism. In this stage, system authenticates the user identification, and password. If the user supply wrong user identification and password, they are denied further process.
3. Data authorization phase: This is the second stage in access control mechanism. This stage is assigned to identify the user's trust value either allowed or prohibited access to sensitive attributes. If the user role status is senior and role trust is a trust, s/he is prohibited to access sensitive attributes. Otherwise, they are allowed to access personal information without sensitive attributes.
4. Admin database: The authorization of user's *rp* in the user personal details is located in this database.
5. User personal details: User personal details (Table 5) includes the user information and the necessary attributes that are assigned for user authorization.

Table 5. The illustration of user personal details

User Personal Details			
Name:	Caren		
Address:	4 July Ave. WA 11000		
Age:	40		
Email:	Caren@yahoo.com		
Department:	Human Resource		
Role Status:	Senior	Role performance	Updated by the administrator
Role Trust:	Trust		

6. Role performance: Role performance is a role status and role trust attributes which are assigned to identify either user is permitted or prohibited to access sensitive attributes. It is used to identify the trustworthiness of the user.
7. Result: All authorized users are granted access to personal information. Moreover, user as a senior-with-trust can access sensitive attributes. User is denied access to personal information if the administrator may not state any values in their role status and/or role trust attributes.
8. Personal: Personal information is located on the personal database.

4 Results and Discussion

In this section, we discuss on how the user is either permitted or prohibited access to the sensitive attributes. In this model, if user request to access sensitive attributes, the parameter is assigned to identify the trust of the user. Four parameters are identified to permit access to sensitive attributes. The parameter is as follows; $< u, rp, a, o >$ where $u \in U$, $rp \in RP$, $a \in A$, $o \in O$. In PATBAC, action a refers to the user which allow to perform read privilege [15] or *select* operation (to retrieve data) [1]. The parameter stated a user u has a role performance rp with an action a to access object o. For example, if a user is granted to access personal information without sensitive attributes. The parameter is as follows:

$$< \text{Staff}, \text{Junior Mistrust}, \text{Select}, \text{Income} >$$

For example, based on the parameters above, the result of user Danny (Table 6) access to Bob Parker's personal information is shown in Table 7:

Table 6. The illustration of user personal details

User Personal Details	
Name:	Danny
Address:	5 Aug Ave. WA 22000
Age:	38
Email:	Danny@yahoo.com
Department:	Human Resource
Role Status:	Junior
Role Trust:	Mistrust

Role performance

Updated by the administrator

In Table 7, Bob's income which is a sensitive attribute does not appear in the result due to Danny's *rp* does not allow access to sensitive attribute. In contrast, the parameter for a user to access personal information with sensitive attribute are as follows:

$$< \text{Staff}, \text{Senior Trust}, \text{Select}, \text{Income} >$$

Table 7. The result appear for junior-with-mistrust or senior-with-uncertainty

	Name	Age	Address
Result	Bob Parker	40	5 Aug Ave. WA 21000

This parameter is owned by the user with a higher level of *rp* to access sensitive attribute. The result has appeared as in Table 8:

In Table 8, Bob's income appears in the result as Caren's (Table 5) *rp* has attained a higher level of trust to access sensitive attribute.

Table 8. The result appear for senior-with-trust

	Name	Age	Address	Income
Result	Bob Parker	40	5 Aug Ave. WA 21000	10000

5 Conclusion and Future Work

In this paper, we propose a comprehensive policy to permit authorized user access sensitive attributes based on seniority and behaviour. To specify the user seniority and behaviour, the system will calculate seniority by using a user experience, and behaviour is evaluated by recommendations. Subsequently, our new trust-based access control model is designed to permit all authorized users access to personal information. However, authorized users with higher level of trust are permitted to access sensitive attributes. These two contributions show the issue of authorized user without trust to access sensitive attributes will be solved. Result shows PATBAC are able to permit or prohibit authorized users access to sensitive attributes.

Among the future work planned includes a prototype to implement the PATBAC. In addition, the model will be combined with purpose based access control (PBAC) to allow user access personal information with sensitive attributes based on trust and purpose.

Acknowledgments. The authors would like to thank the reviewers for their valuable comments to help improve this article. This work is partly sponsored by the Scholarship Department, Ministry of Education, Malaysia.

References

1. Abdul Ghani, N.: Credential purpose-based access control for personal data protection in web-based applications. Ph.D. thesis, Universiti Teknologi Malaysia, Faculty of Computing (2013)
2. Bernabe, J.B., Perez, G.M., Gomez, A.F.S.: Intercloud trust and security decision support system: an ontology-based approach. J. Grid Comput. 1–32 (2015)
3. Bertolissi, C., Fernandez, M.: A metamodel of access control for distributed environments: Applications and properties. Inf. Comput. **238**, 187–207 (2014)
4. Bruhn, J.G.: Trust and the Health of Organizations. Springer Science & Business Media, New York (2001)

5. Crampton, J., Sellwood, J.: Path conditions and principal matching: a new approach to access control. In: Proceedings of the 19th ACM Symposium on Access Control Models and Technologies, pp. 187–198. ACM (2014)
6. Gollmann, D.: From access control to trust management, and back – a petition. In: Wakeman, I., Gudes, E., Jensen, C.D., Crampton, J. (eds.) IFIPTM 2011. IAICT, vol. 358, pp. 1–8. Springer, Heidelberg (2011). doi:10.1007/978-3-642-22200-9_1
7. Heupel, M., Fischer, L., Kesdogan, D., Bourimi, M., Scerri, S., Hermann, F., Gimenez, R.: Context-aware, trust-based access control for the di.me userware. In: 2012 5th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–6. IEEE (2012)
8. Hung, P.C.: Towards a privacy access control model for e-healthcare services. In: PST (2005)
9. Kayes, A., Han, J., Colman, A.: A semantic policy framework for context-aware access control applications. In: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 753–762 (2013). doi:10.1109/TrustCom.2013.91
10. Kim, M., Seo, J., Noh, S., Han, S.: Identity management-based social trust model for mediating information sharing and privacy enhancement. Secur. Commun. Netw. **5**(8), 887–897 (2012)
11. Lazouski, A., Martinelli, F., Mori, P.: Usage control in computer security: a survey. Comput. Sci. Rev. **4**(2), 81–99 (2010)
12. Li, M., Sun, X., Wang, H., Zhang, Y.: Multi-level delegations with trust management in access control systems. J. Intell. Inf. Syst. **39**(3), 611–626 (2012)
13. Li, M., Wang, H., Ross, D.: Trust-based access control for privacy protection in collaborative environment. In: IEEE International Conference on e-Business Engineering, ICEBE 2009, pp. 425–430. IEEE (2009)
14. Lin, G., Wang, D., Bie, Y., Lei, M.: Mtbac: a mutual trust based access control model in cloud computing. China Commun. **11**(4), 154–162 (2014)
15. Mirabi, M., Ibrahim, H., Mamat, A., Udzir, N.I.: Integrating access control mechanism with EXEL labeling scheme for XML document updating. In: Fong, S. (ed.) NDT 2011. CCIS, vol. 136, pp. 24–36. Springer, Heidelberg (2011). doi:10.1007/978-3-642-22185-9_3
16. Ruj, S., Stojmenovic, M., Nayak, A.: Privacy preserving access control with authentication for securing data in clouds. In: 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp. 556–563. IEEE (2012)
17. Samarati, P.: Protecting respondents identities in microdata release. IEEE Trans. Knowl. Data Eng. **13**(6), 1010–1027 (2001)
18. Sandhu, R., Ferraiolo, D., Kuhn, R.: The NIST model for role-based access control: towards a unified standard. In: ACM Workshop on Role-Based Access Control, vol. 2000 (2000)
19. Sarrouh, N.: Formal modeling of trust-based access control in dynamic coalitions. In: Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual, pp. 224–229. IEEE (2013)
20. Toahchoodee, M., Abdunabi, R., Ray, I., Ray, I.: A trust-based access control model for pervasive computing applications. In: Gudes, E., Vaidya, J. (eds.) DBSec 2009. LNCS, vol. 5645, pp. 307–314. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03007-9_22
21. Vidyalakshmi, B., Wong, R.K., Chi, C.H.: Decentralized trust driven access control for mobile content sharing. In: 2013 IEEE International Congress on Big Data (BigData Congress), pp. 239–246. IEEE (2013)
22. Yang, R., Lin, C., Jiang, Y., Chu, X.: Trust based access control in infrastructure-centric environment. In: 2011 IEEE International Conference on Communications (ICC), pp. 1–5. IEEE (2011)