International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.153-172
http://dx.doi.org/10.14257/ijsia.2016.10.12.13

Role Performance 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*
[2]*Faculty of Information Management, Universiti Teknologi MARA, Malaysia*
mohdrafiz@sarawak.uitm.edu.my, izura@upm.edu.my, mohdizuan@upm.edu.my, fazlida@upm.edu.my, hamidah.ibrahim@upm.edu.my

Abstract

Preserving privacy is a challenge and requires the management of access control, which may be based on role, purpose or trust. There are many recent advances of access control models have been developed to avoid unauthorized users access to the privacy. However, there are still issues that impede the development of effective access control. The issue highlight in this paper is inappropriate access and use of sensitive attributes by authorized users. Therefore, it is critical to design an efficient access control model based on trust to protect sensitive attributes from untrusted user. In this paper, we propose a new access control model based on trust called role performance trust-based access control to permit trusted user access to sensitive attributes. Subsequently, we also propose a comprehensive policy to permit user access sensitive attributes based on two trust metrics namely user experience and behaviour. To evaluate the trustworthiness of authorized user, we propose a quantification method to measure those metrics. Based on the results, role performance trust-based access control may significantly permit or prohibit access to personal information, especially sensitive attributes by authorized users. This model is capable to solve the issue of authorized user without trust to access sensitive attributes.

Keywords: *Privacy protection, Role performance, Sensitive attributes, Trust, Trust-based access control.*

1. Introduction

Companies or owners are required to allow access to the privacy or personal information contained within the information systems to a multitude of users or staffs. Users can access the privacy at any location. Privacy is becoming one of the very important issues in data management. Privacy is divided into three attributes, namely: de-identified, quasi identifier and sensitive. De-identified is defined as a key attribute. This attribute should be removed as it is the obvious identifying records, for instance name, address and social security number. In contrast, quasi identifier is a non-key attribute. However, this attribute needs to be anonymized before it can be released. The example of quasi identifier attributes is; race, age, and zip code [10]. Finally, sensitive is a classified data which the identity belongs to the customer, for example; disease and income. People are now more conscious about how their privacy being secured and protected by the organization. This awareness has been getting more highlights when sharing and collecting of information become seamless and prevalent by the omnipresence of internet connection. The

* Corresponding Author

ISSN: 1738-9976 IJSIA

administrator may allow users to access the privacy, but the information system should be equipped with the mechanisms to permit specified users to access it. Based on the US healthcare industry legislated the Health Insurance Portability and Accountability Act (HIPAA) in 1996, the minimum requirements of reasonable access for privacy and security is really necessitated. As a solution, most of the works have been focusing on access control in which the access authorization to a source is selectively permitted. Access control is assigned to limit access of personal information by preventing unauthorized access to the resources of the system. Users are permitted to access personal information if it is authorized by the policy [1, 2, 3, 4, 5, 6, 7, 8].

The issue discussed in this paper is sensitive attributes privacy disclosure. In anonymization, the data (de-identified and quasi identifier attributes) needs to be anonymized to avoid adversary infer the customer's sensitive information especially sensitive attributes [9]. In this case, sensitive attributes need to be secured to avoid malicious user disclose the information. Based on literature, existing access control models based on purpose focus on protecting personal information from unauthorized users [25, 26, 27]. However, protecting sensitive attributes should be taken into critical consideration. The weaknesses of the access control models based on purpose are each levels of authorized users have been permitted to access sensitive attributes and the user trust is mutable. It may cause sensitive attributes to be disclosed to untrusted user, i.e. Authorized user which may not be trusted. Therefore, a new model needs to be considered to avoid the inappropriate access and use of sensitive attributes.

This paper addresses the issue of protecting sensitive attributes from inappropriate access that can cause privacy disclosure. A new access control model based on trust called Role Performance Trust-Based Access Control (RPTBAC) is proposed to permit trusted user access to sensitive attributes. In order to deal with the dynamic nature of trust, a new scheme is designed to engage with the continuous process of updating and measuring user behaviour in an organization. This involves a comprehensive policy for user to permit access to sensitive attributes based on their level of seniority and behaviour called "role performance". The user role performance rp will be quantified to identify either they are permitted or denied access to sensitive attributes. This policy is devised from the combination of existing access control policies based on trust and other resources to determine the criteria as a higher level of trust. Two types of user properties have taken into consideration in this policy to allow the trust relationship between a user and the system namely; experience and recommendations. In this proposed system, authorized user without trust are able to access personal information, but authorized user with higher level of trust are granted to access personal information with sensitive attributes. In summary, the main contributions of this paper are as follows:

1. Propose a new access control model called role performance trust-based access control model (RPTBAC) to protect sensitive attributes.

2. Present a comprehensive policy for user to permit access to sensitive attributes based on user experience and behaviour.

3. Propose a quantification method of rp to deal with the dynamic nature of trust.

The rest of this paper is organized as follows: A comprehensive policy to permit access to the sensitive attributes is introduced in Section 2. In Section 3, the RPTBAC mechanism is explained while the components of the user access decision is presented in Section 4. The results and discussion are presented in Section 5 while the related works is discussed in Section 6. Finally, the paper ends with a conclusion and suggestions for future work.

2. A Comprehensive Policy

The proposed policy uses two types of properties. The properties are; experience, and recommendations. These properties allow the trust relationship between a user and the system.

Experience is assigned to measure the seniority of user, whilst recommendations is assigned to measure the user behaviour. The experience is based on the previous activities that had occurred in the past within a certain period of time, which involve in their substantive service and that the administrator has a recollection about. Recommendations are provided by trusted third-parties who have knowledge about a user with respect to their behaviour.

2.1. Properties

Each role in the organization requires certain properties of a user. In this research, the properties allow access to sensitive attributes based on the information provided by the administrator and it is based on the calculation of experience and recommendations. The explanation of both properties is as follows:

a. Experience

Based on previous work, users of the senior role can perform the same set of duties as its junior role. However, a user who is assigned as a senior role is typically considered more trustworthy as compared to a user who is assigned as a junior role [11]. In RPTBAC, the seniority of the user can be applied to identify the activeness of the user by quantifying their experience or activities perform during their substantive service. If the user thinks they have performed enough activities and can achieve the minimum requirement set by the administrator, they can apply online in the system to allow the organization to decide based on the calculation of activities whether they are eligible or not to change their role status from junior to senior. The experience of the user can be set in the role status attribute in the user personal details and in this case, there are two levels of user seniority: junior (less trust) and senior (highly trust).

However, a user who is assigned as senior role is not necessarily considered to have a higher level of trust. For example, if a user has been assigned as a senior, but proven to perform negative activities, therefore in this case, a user is restricted to access sensitive attributes. This means that, having a seniority does not mean having a higher level of trust. A higher level of trust refers to the user who is assigned as a senior role with a trusted behaviour. To identify the user that is senior with a trusted behaviour, this model assigns recommendations to identify the behaviour of a user.

b. Recommendations

In general, the truster does not know much about the trustee. The truster needs to assign recommendations to evaluate the trust of the trustee. A recommendation could be one or more recommender that claim to know more about the trustee with respect to the particular roles [11]. In RPTBAC, recommendations are assigned by the administrator to evaluate a user behaviour. A user behaviour categories illustrated in Figure 1 [13] are applied in this research to specify the user's level of trust by quantifying all the categories. Recommendations are assigned to quantify the user behaviour and the result is supplied in the role trust attribute at the user personal details. In previous work, three levels of trust has been presented: disbelief, belief and uncertainty [11]. In this case, three levels of user behaviour has proposed: mistrust (junior), trust (senior) and uncertainty (senior performing negative behaviours). If the user's

rp is junior, the system will automatically assign as mistrust and they are not allowed to access sensitive attributes. Similar to the user's rp is senior and uncertainty, they are also restricted to access sensitive attributes. However, if the user's rp is senior-with-trust, they are permitted to access sensitive attributes. Figure 2 shows in detail the influence of seniority and behaviour level to authorize access of customer personal information or with sensitive attributes.

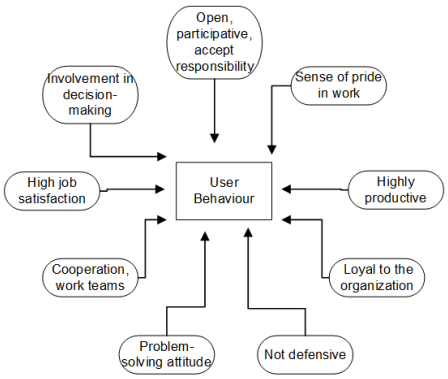

Figure 1. Seniority and behaviour level to authorize access of information

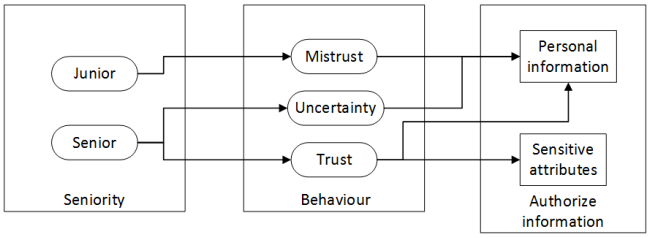

Figure 2. Seniority and behaviour level to authorize access of information

In access control mechanism, both contexts in this model play important roles to determine the trustworthiness of a user. The role status (seniority) and role trust (behaviour) attributes are identified as the role performance rp. Multiple levels of rp can be associated with the user. A user's rp needs to be identified in authorization phase. For example, if a user Alice's rp is a senior-with-trust, then she is granted to access sensitive attributes. Otherwise, she is denied access it.

In previous work, truster evaluates trustee in some context which refer to the role the user is assigned to. To specify between a user and a role, a user's trust value is evaluated based on user role context rc, for example the trust relationship is represented between truster A, and trustee B, on some rc, as a triple, $(A^{b^{rc}}_{B}, A^{d^{rc}}_{B}, A^{u^{rc}}_{B})$, A's belief on B about the latter's trustworthiness, A's disbelief on B, and A's uncertainty on B. Each of these components has a value between [0, 1] and the sum of these components is 1 [11]. In RPTBAC, those three measures are assigned as, $(A^{t^{rp}}_{B}, A^{m^{rp}}_{B}, A^{u^{rp}}_{B})$, where A's trust on B if the system authorize the role performance of B is a senior-with-trust. A's mistrust on B if the role performance is a junior-with-mistrust and A's uncertainty on B if the role performance is a senior-with-uncertainty. The rp of senior-with-trust is permitted to access sensitive attributes. Hence, the rp of junior-with-mistrust and senior-with-uncertainty are restricted to access sensitive attributes.

2.2. Quantifying 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. Based on Toahchoodee [11], the experiences of the user are stored in the User Role History (URH) database. Therefore, in RPTBAC, URH database is assigned to store a user's experience and it will be calculated automatically by using weighing evidence. This notion is adapted from the work of Gollmann [14] where Figure 3 shows the calculation of a user's experience in a weighing evidence.

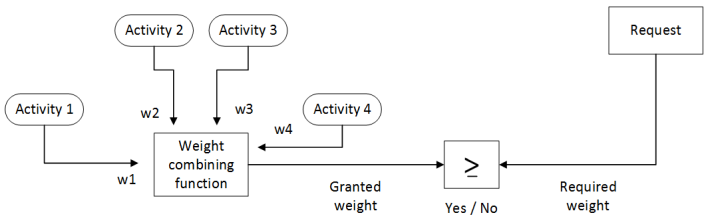

Figure 3. Calculation of a trustee's experiences

2.2.1. 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. i and j represent the activities. The total sum of m is calculated $(m_i + \cdots + m_j)$. Then, sum of w 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 equation 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 [15], Alice's overall score is 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 RPTBAC, calculation of the 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.

2.3. Quantifying Recommendation

Recommendations are assigned to evaluate a user behaviour. A user behaviour needs to be quantified to specify the user level of trust. The quantification involves specifying either the user is trusted or mistrusted. Uncertainty refers to the user that previously senior-with-trust. However, due to they perform negative activities, the administrator will change manually from trust to uncertainty. The examples of negative activities are: committing the fraud, ignorance of obligation, dishonest behaviour, etc. Before specifying the user level of trust, recommendations require to supply the user's scores in the user evaluation form (EF) as illustrated in Table 2. Then, the scores will be calculated.

Table 2. 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	

Let b denote the total amount of each behaviour category and c is the total number of behaviour categories. i and k represent the scores. The sum of b is $(b_i + \cdots + b_k)$. 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 equation 2.

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

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. [16, 15], the level of a user trusted behaviour for the overall score is illustrated as in Table 3. For example, assume a user Carol obtains the overall score 0.7. Based on Table 3, 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.

Table 3. 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

2.4. Computing Trustworthiness

To determine either the user is allowed or prohibited access to sensitive attributes, experience and recommendations is considered to be calculated. The minimum required weight for both calculations is set by the administrator. If the user attains a minimum required weight for the experience and recommendations, they are permitted to access sensitive attributes. There is a suggestion to merge experience and recommendations to accurately obtain the user's trust value, which is assigned in the field [0,1] [12]. In RPTBAC, both entities are merged to obtain user's rp value by calculating the user experience to identify the user's seniority, and recommendations to identify the user's behaviour.

In this model, if the computation of experience attains the minimum required weight but the calculation of recommendations does not achieve minimum requirement or vice versa, the user is not assigned the rp senior-with-trust. Therefore, both attributes should achieve a minimum requirement set by the administrator to permit access to sensitive attributes.

3. Access Control Mechanism

In access control model, the access control mechanism is the most important to either permit or prohibit access to personal information. In this paper, access control model focuses on protecting sensitive attributes based on trust. Figure 4 shows the RPTBAC mechanism and the explanations are as follows:

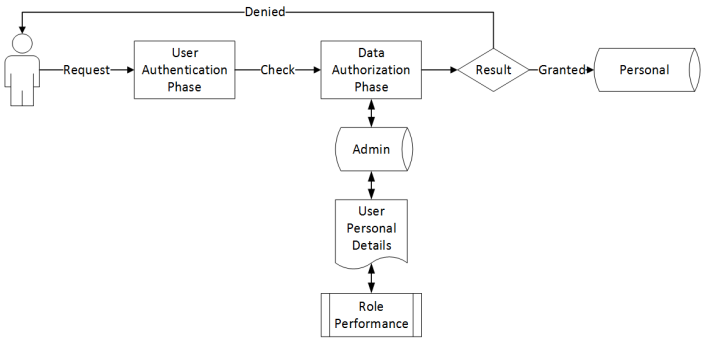

Figure 4. RPTBAC Mechanism

1. User: User in this model refers to the staff. User is requested to access privacy in the system. First, the user needs to supply user identification and password.
2. User authentication phase: This is the first stage in access control mechanism. In this stage, the system authenticates the user identification and

password. If the user supplies 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's role status is senior and role trust is a trust, they are permitted 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 4) include the user information and the necessary attributes that are assigned for user authorization.

Table 4. 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
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 access to sensitive attributes. It is assigned 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. The 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 in the personal database.

4. User Access Decision

To permit access to sensitive attributes, the administrator needs to clarify the components to decide which user is allowed to access personal information or with sensitive attributes. Four components or parameters are identified to access sensitive attributes. Figure 5 shows the flow of user access decision.

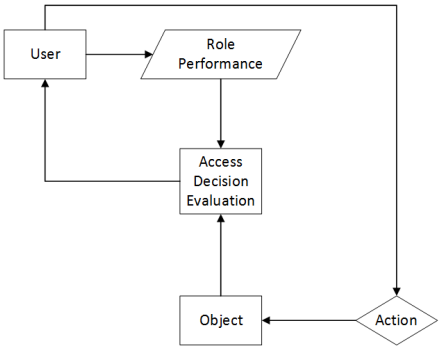

Figure 5. User access decision

The user's identification, password and rp are evaluated in the access decision evaluation. Next, the system reacts by providing an object based on user's rp and action set in the system. Object refers to the personal information with sensitive attributes. Action means right to execute on the privacy and the administrator is responsible to set it. In this model, the user may perform the action of reading privilege [17] or select operation (to retrieve data) [18].

5. Results and Discussion

In this section, the results are discussed in subsection 5.1. Next, the query modification is explained in subsection 5.2 and finally, test and validation of this model is presented in subsection 5.3.

5.1. Results

In this subsection, 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 $u \in U$, $rp \in RP$, $a \in A$, $o \in O$. 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:

<Staff, Junior Mistrust, Select, Income>

The parameter above is the example of the user junior-with-mistrust to access personal information without sensitive attribute. For example, based on the parameters above, the result of user Danny (Table 5) can access Bob Parker's personal information is shown in Table 6:

Table 5. 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 performance
Role Trust:	Mistrust	

Table 6. The result appear for junior-with-mistrust or senior-with-uncertainty

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

In Table 6, Bob's income which is sensitive attribute does not appear in the result due to Danny's rp (Table 5) does not achieve a higher level of trust. Therefore, he is not allowed to access sensitive attribute. In contrast, the parameter for a user to access personal information with sensitive attribute are as follows:

<Staff, Senior Trust, Select, Income>

This parameter is owned by the user with a higher level of rp to access sensitive attribute. The result has appeared as in Table 7:

Table 7. The result appear for Senior-with-trust

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

Table 7, Bob's income appears in the result as Caren's rp (Table 4) has attained a higher level of trust to access sensitive attribute.

Based on the comparison of the results above, trust plays an important role in accessing customer sensitive attributes. In this model, trust refers to role performance rp that is assigned to identify the identity of the user in the organization. Access control is assigned to authenticate rp and authorize user access to customer sensitive attributes based on trust. RPTBAC may significantly permit or prohibit authorized user access to personal information, but authorized users with higher levels of rp are permitted to access sensitive attributes.

5.2. RPTBAC Query Modification Algorithm

Access control mechanisms must ensure that query results contain only the personal information that is allowed to be accessed by the user. In RPBAC, the mechanism ensures the authorized user with a higher level of trust is permitted to access sensitive attributes. This expectation is achieved in this section by using a query modification. The query modification must be complied with all conditions before accessing to the privacy is granted. Our query modification algorithm is outlined in Figure 6.

1 Input : Username and password
// Verify in the user authentication (UA) phase
2 If failed, ACCESS DENIED
3 Else
4 ACCESS GRANTED

User Authentication

// Verify in the data authorization (DA) phase
User u Role Performance rp
6 If u (rp) = False then
//Go to the next step (9)
7 Else if
8 If u (rp) = True then
// Go to the next step (13)

Administrator *A* trust value to user B either to permit access to the personal information (PI) or with sensitive attributes (PISA)
9 If $(A^{t^{rp}}_{B}, A^{m^{rp}}_{B}, A^{u^{rp}}_{B})$ = (0, 1, 0) then
10 DA = Access to the PI
11 Else if $(A^{t^{rp}}_{B}, A^{m^{rp}}_{B}, A^{u^{rp}}_{B})$ = (0, 0, 1) then
12 DA = Access to the PI
13 Else $(A^{t^{rp}}_{B}, A^{m^{rp}}_{B}, A^{u^{rp}}_{B})$ = (1, 0, 0)
14 DA = Access to the PISA
//Return the query result
Output: PI or PISA

Data Authorization

Figure 6. RPTBAC Query Modification Algorithm

The RPBAC query modification algorithm is implemented in two levels: user authentication and data authorization. The decision will be made whether the authorized user is either permitted or prohibited access to sensitive attributes. In the user authentication (UA) phase, the system will verify the user identification and password. First, the user will supply the user identification and password (Line 1). The user will be verified either they are granted (Line 4) or denied (Line 2) access to the system. Assume the user is granted access to the system, then the system will check the user's rp in the data authorization (DA) phase.

In the DA phase, if the u (rp) is false (Line 6) or a junior-with-mistrust $A^{m^{rp}}_{B}$ (Line 9) or a senior-with-uncertainty $A^{u^{rp}}_{B}$ (Line 11), the user is allowed to access the personal information, but not permitted to access sensitive attributes. However, if the u (rp) is true (Line 8) or a senior-with-trust $A^{t^{rp}}_{B}$ (Line 13), the user is permitted to access sensitive attributes.

Based on the query modification algorithm, it shows that the notion of using the rp as a user trust metric has successfully specified a trusted authorized user to access sensitive attributes. RP efficiently differentiated a user with and without a higher level of trust based on the quantification of seniority and behaviour. Finally, by using rp, it shows that the model proposed is effectively working either to permit or restrict user access to sensitive attributes.

5.3. Tests and Validation on RPTBAC Mechanism Implementation

To specify the validity of the proposed model, test by using the prototype is required to validate the three components of the access control system which consist of access control models, policies and mechanism. A scenario simulating a bank

information system called ABC Bank Information System is developed as a prototype in this research. This prototype is developed by using Adobe Dreamweaver CS6 and WampServer which comprises of three applications: Apache2, PHP and MySQL database. The quantification of user experience and behaviour to specify the user's trustworthiness is developed by using Microsoft Visual Studio. The scenario is explained as follows.

ABC Bank Information System is a system to access the privacy of the customer. All authorized staffs are permitted to access the customer's personal information in this system. However, to access the customer's sensitive attributes, authorized staffs need to achieve a higher level of trust. The quantification of a user's experience and behaviour is required to identify the user's trustworthiness. In this system, all authorized staffs are permitted to view or retrieve the personal information, but authorized users with a higher level of trust are authorized to view or retrieve sensitive attributes.

In this system, three case studies are required to specify the user's trustworthiness based on the policy. Case Study 1 is the situation where the staff Danny wants to access the customer's privacy, but he has not achieved a higher level of trust (Figure 7). Next, Case Study 2 is the situation where the staff Caren has achieved a higher level of trust (Figure 7) and she would like to access the customer's privacy. Finally, Case Study 3 is the situation where the staff Emmet has achieved a higher level of trust, however, he has proven to perform negative activities (Figure 7) and he wants to access the customer's privacy.

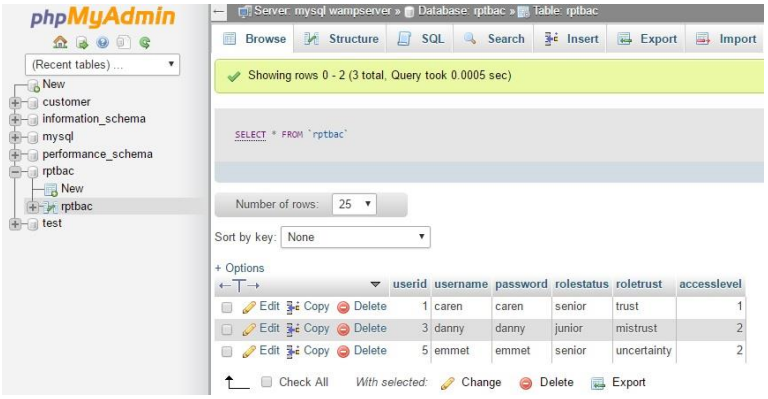

Figure 7. User database

Before explaining in detail the mechanism to allow the user in three case studies to access the privacy, this paper describes how to quantify the user's rp or experience and behaviour. Based on Case Study 1, assume Danny applies to achieve a higher level of trust by quantifying his rp. To attain a higher level of trust, Danny requires to achieve a minimum requirement of rp set by the administrator. If Danny achieves a minimum requirement, he is permitted to access customer's sensitive attributes. If Danny is not achieved a minimum requirement of both rp or one of it, he is not allowed to access it. In this research, an administrator sets the minimum requirement of the total experience and behaviour is 0.4. Based on the quantification of Danny's rp, he has not achieved a higher level of trust (Figure 8 and 9).

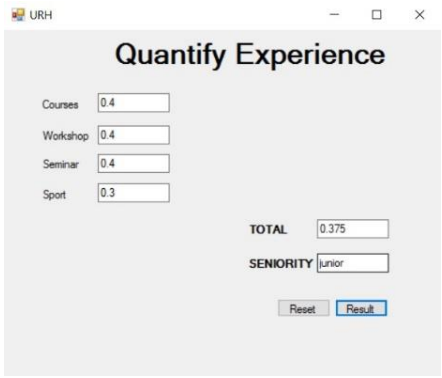

Figure 8. The result of the user does not achieves a higher level of seniority

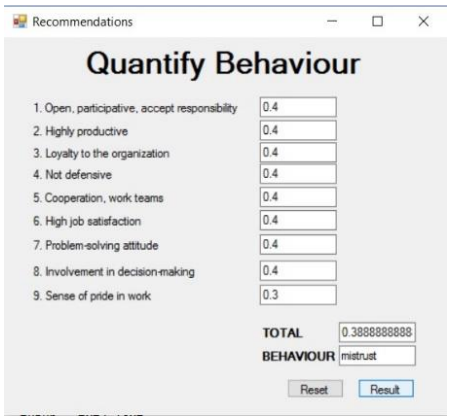

Figure 9. The result of the user does not achieves a higher level of behaviour

In the next situation, assume Caren applies to achieve a higher level of trust. Based on Figure 10 and 11, Caren has achieved a higher level of trust. Therefore, she is permitted to access sensitive attributes.

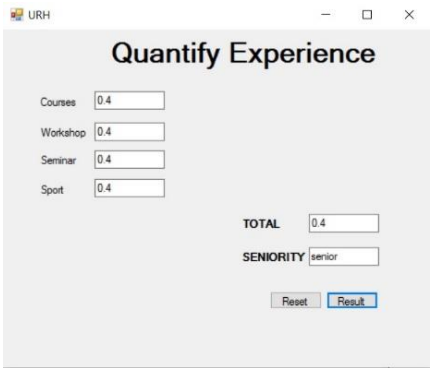

Figure 10. The result of the user achieves a higher level of seniority

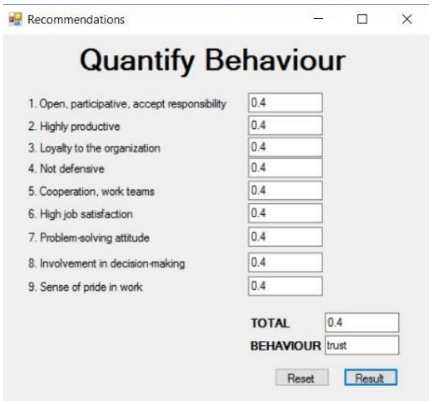

Figure 11. The result of the user achieves a higher level of behaviour

Finally, assume Emmet has achieved a higher level of trust. However, he has proven to perform negative activities. Therefore, his behaviour can be set as uncertainty by the administrator manually and he is not permitted to access sensitive attributes.

Based on the three types of user, all of them have different levels of trust and they have different permissions to access the privacy. Next, the three case studies are discussed.

5.3.1. Case study 1

Case study 1 is the situation where Danny has not achieved a higher level of trust and he wants to access the privacy. In RPTBAC system, the first process is Danny needs to login his username and password.

Based on Table 8, the query of the Case Study 1 is executed. The authentication of the user is started when the user supplies a username and password in the login page. Next, the system examines either the input given by the user is correct or not. Assume Danny supply correct username and password, then the system will proceed to the next stage called data authorization to specify the user's rp. In this case, Danny's rp is: role status = junior and role trust = mistrust. Based on the rp, Danny is permitted to access the customer's personal information without sensitive attribute as shown in Figure 12.

Table 8. Query Processing for Case Study 1

Input	Description	SQL Statement
Username = danny Password = danny	Login the user's information	SELECT username and password FROM user_personal_details WHERE username = 'danny', password = 'danny'
	System check the user's rp	SELECT rolestatus, roletrust FROM user_personal_details WHERE rolestatus = 'junior', roletrust = 'mistrust'
	• Access Compliance Checking	SELECT custid, name, age, address

	• Authorized attributes • Authorized action	FROM customer

custid	name	age	address
1	Bob Parker	40	5 Aug Ave. WA 21000
3	Aice	35	1 April Ave.

Logout

Figure 12. Result of the Case Study 1

5.3.2. Case study 2

Case study 2 is the situation where Caren attains a higher level of trust and he wants to access the privacy. In RPTBAC system, the first process is Caren needs to login her username and password.

Next, Table 9 shows the query of the Case Study 2. In the user authentication phase, assume Caren supplies correct username and password, then the system will proceed to the next stage called data authorization to specify the user's rp. In this case, Caren's rp is: role status = senior and role trust = trust. Based on the rp, Figure 13 shows Caren is permitted to access the customer's sensitive attribute.

Table 9. Query Processing for Case Study 2

Input	Description	SQL Statement
Username = caren Password = caren	Login the user's information	SELECT username and password FROM user_personal_details WHERE username = 'caren', password = 'caren'
	System check the user's rp	SELECT rolestatus, roletrust FROM user_personal_details WHERE rolestatus = 'senior, roletrust = 'trust'
	• Access Compliance Checking • Authorized attributes • Authorized action	SELECT custid, name, age, address, income FROM customer

custid	name	age	address	income
1	Bob Parker	40	5 Aug Ave. WA 21000	10000
3	Aice	35	1 April Ave.	5000

Logout

Figure 13. Result of the Case Study 2

5.3.3. Case study 3

Case study 3 is the situation where Emmet has not achieved a higher level of trust and he wants to access the privacy. First, Emmet login his username and password.

Based on Table 10, the query of the Case Study 3 is executed. First, assume Emmet supplies correct username and password, then the system will proceed to the next stage called data authorization to specify the user's rp. In this case, Emmet's rp is: role status = senior and role trust = uncertainty. Based on the rp, Figure 14 shows Emmet is permitted to access the customer's personal information without sensitive attribute.

Table 10. Query Processing for Case Study 3

Input	Description	SQL Statement
Username = emmet Password = emmet	Login the user's information	SELECT username and password FROM user_personal_details WHERE username = 'emmet', password = 'emmet'
	System check the user's rp	SELECT username, rolestatus, roletrust FROM user_personal_details WHERE rolestatus = 'senior', roletrust = 'uncertainty'
	• Access Compliance Checking • Authorized attributes • Authorized action	SELECT custid, name, age, address FROM customer

custid	name	age	address
1	Bob Parker	40	5 Aug Ave. WA 21000
3	Aice	35	1 April Ave.

Logout

Figure 14. Result of the Case Study 3

6. 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 [19]. The main focus of RPTBAC 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) [20]. A higher level of delegation task is assigned to the delegate if they have a higher trust level. In RPTBAC, the system has to check a user's 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) is 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 user authorizations may be revoked [21]. The same concept is proposed in RPTBAC 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 [12, 22]. The history or experience of the user is stored in the User Role History (URH) [11]. In RPTBAC, 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 [23].

Generally, trust can be changed from time to time. This change may revoke user from ongoing access. It can be revoked manually or automatically, depending on the trust evaluation concept set by the administrator [11, 24]. In RPTBAC, 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.

7. 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's seniority and behaviour, the system will calculate seniority by using a user's experience and behaviour is evaluated by recommendations. Subsequently, our new trust-based access control model called role performance trust-based access control (RPTBAC) is designed to permit all authorized users to access personal information. However, authorized users with a higher level of trust are permitted to access sensitive attributes. These contributions show the issue of authorized user without trust to access sensitive attributes will be solved. The result shows RPTBAC are able to permit or prohibit authorized users access to personal information, but authorized users with higher levels of rp are permitted to access sensitive attributes.

Among the future work planned includes a prototype to implement the RPTBAC. 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] C. Bertolissi and M. Fern´andez, "A metamodel of access control for distributed environments: Applications and properties," Information and Computation, (**2014)**.

[2] J. Crampton and J. Sellwood, "Path conditions and principal matching: a new approach to access control," in Proceedings of the 19th ACM symposium on Access control models and technologies. ACM, (**2014)**, pp. 187–198.

[3] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The nist model for role-based access control: towards a unified standard," in ACM workshop on Role-based access control, vol. 2000, (**2000**).
[4] P. C. Hung, "Towards a privacy access control model for e-healthcare services." in PST, (**2005**).
[5] A. Kayes, J. Han, and A. Colman, "A semantic policy framework for context-aware access control applications," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on July, (**2013**), pp. 753–762.
[6] A. Lazouski, F. Martinelli, and P. Mori, "Usage control in computer security: A survey," Computer Science Review, vol. 4, no. 2, (**2010**), pp. 81–99.
[7] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for securing data in clouds," in Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on. IEEE, (**2012**), pp. 556–563.
[8] P. Samarati, "Protecting respondents identities in microdata release," Knowledge and Data Engineering, IEEE Transactions on, vol. 13, no. 6, (**2001**), pp. 1010–1027.
[9] Q. Zhang, N. Koudas, D. Srivastava, and T. Yu, "Aggregate query answering on anonymized tables." in ICDE, vol. 7. Citeseer, (**2007**), pp. 116–125.
[10] L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, **(2002)**, pp. 557-570.
[11] M. Toahchoodee, R. Abdunabi, I. Ray, and I. Ray, "A trust-based access control model for pervasive computing applications," in Data and Applications Security XXIII. Springer, (**2009**), pp. 307–314.
[12] M. Li, H. Wang, and D. Ross, "Trust-based access control for privacy protection in collaborative environment," in e-Business Engineering, 2009. ICEBE'09. IEEE International Conference on. IEEE, (**2009**), pp. 425–430.
[13] J. G. Bruhn, Trust and the Health of Organizations. Springer Science & Business Media, (**2001**).
[14] D. Gollmann, "From access control to trust management, and back–a petition," in Trust Management V. Springer, (**2011**), pp. 1–8.
[15] B. Vidyalakshmi, R. K. Wong, and C.-H. Chi, "Decentralized trust driven access control for mobile content sharing," in Big Data (BigData Congress), 2013 IEEE International Congress on. IEEE, (**2013**), pp. 239–246.
[16] M. Kim, J. Seo, S. Noh, and S. Han, "Identity management-based social trust model for mediating information sharing and privacy enhancement," Security and Communication Networks, vol. 5, no. 8, (**2012**), pp. 887–897.
[17] M. Mirabi, H. Ibrahim, L. Fathi, N. I. Udzir, and A. Mamat, "An access control model for supporting xml document updating," in Networked Digital Technologies. Springer, (**2011**), pp. 37–46.
[18] N. Abdul Ghani, "Credential purpose-based access control for personal data protection in web-based applications," Ph.D. dissertation, Universiti Teknologi Malaysia, Faculty of Computing, (**2013**).
[19] M. Heupel, L. Fischer, D. Kesdogan, M. Bourimi, S. Scerri, F. Hermann, and R. Gim´enez, "Context-aware, trust-based access control for the di. me userware," in New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on. IEEE, (**2012**), pp. 1–6.
[20] M. Li, X. Sun, H. Wang, and Y. Zhang, "Multi-level delegations with trust management in access control systems," Journal of Intelligent Information Systems, vol. 39, no. 3, (**2012**), pp. 611–626.
[21] R. Yang, C. Lin, Y. Jiang, and X. Chu, "Trust based access control in infrastructure-centric environment," in Communications (ICC), 2011 IEEE International Conference on. IEEE, (**2011**), pp. 1–5.
[22] G. Lin, D. Wang, Y. Bie, and M. Lei, "Mtbac: A mutual trust based access control model in cloud computing," Communications, China, vol. 11, no. 4, (**2014),** pp. 154–162.
[23] J. B. Bernabe, G. M. Perez, and A. F. S. Gomez, "Intercloud trust and security decision support system: an ontology-based approach," Journal of Grid Computing, (**2015**), pp. 1–32.
[24] N. Sarrouh, "Formal modeling of trust-based access control in dynamic coalitions," in Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual. IEEE, (**2013**), pp. 224–229.
[25] M. E. Kabir and H. Wang, "Conditional purpose based access control model for privacy protection," ser. ADC '09. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., (2009), pp. 135–142. [Online]. Available: http://dl.acm.org/citation.cfm?id=1862681.1862699
[26] M. E. Kabir, H. Wang, and E. Bertino, "A conditional purpose-based access control model with dynamic roles," Expert Syst. Appl., (2011), pp. 1482–1489.
[27] M. Kabir, H. Wang, and E. Bertino, "A role-involved purpose-based access control model," Information Systems Frontiers, vol. 14, no. 3, (2012) pp. 809–822. [Online]. Available: http://dx.doi.org/10.1007/s10796-011-9305-1

Author

Mohd Rafiz Salji is a postgraduate student at the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). He obtained his Master in Information Management from Universiti Teknologi MARA, Malaysia in October 2007. His field of study is in Security in Computing and his interest is in access control.