Journal of Engineering and Applied Sciences 13 (Special Issue 9): 7032-7038, 2018
ISSN: 1816-949X
© Medwell Journals, 2018

Performance and Divisional Trust and Purpose-Based Access Control for Privacy Preservation

[1, 2]Mohd Rafiz Salji, [1]Nur Izura Udzir, [1]Mohd Izuan Hafez Ninggal,
[1]Nor Fazlida Mohd and [1]Sani Hamidah Ibrahim
[1]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia,
Seri Kembangan, Malaysia
[2]Faculty of Information Management, Universiti Teknologi MARA, Shah Alam, Malaysia

Abstract: Privacy has been recognized to be a critical requirement in computing environments. To keep the privacy safe from inappropriate use, one of the most popular methods that can be used is the access control. Currently, many augmentation of access control models has been developed to improve the effectiveness in preserving the privacy. However, there are still issues that need improvements. In current Purpose-Based Access Control (PBAC) Models, all authorized users in the domain are allowed to access the personal information especially sensitive attributes equally. It may cause the risk of privacy disclosure by ‘limited-authorized’ user, i.e., legitimate user but untrusted and unauthorized to access certain personal information with sensitive attributes. In this study a finer-grained access control called performance and divisional trust and purpose-based access control is proposed to prevent limited-authorized user access to the privacy. Based on organizational structure (functional departmentalization) current PBAC Models permit authorized user in the functional level to access the personal information. This model can be set at the next level after the functional level, i.e., the divisional level to access it. Subsequently, a comprehensive policy is proposed to permit user to access sensitive attributes based on two trust metrics namely user experience and behaviour. To evaluate the trustworthiness of the authorized user, a quantification method is proposed to measure those metrics. Based on the results, this model may significantly permit or prohibit access to personal information or with sensitive attributes. Besides, the issue of privacy disclosure by limited-authorized user to access certain privacy is resolved.

Key words: Access control, divisional, purpose, purpose-based access control, privacy, role performance, sensitive attributes, trust

INTRODUCTION

Organization permits authorized users or staffs to access the privacy contained within the information systems and it can be accessible at any time and location. Privacy is divided into three categories, 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. Finally, sensitive is a classified data which the identity belongs to the customer, for example, disease and income. The privacy is permitted to be accessed by the user but the information system should be equipped with access control. Access control is assigned to limit access the privacy by preventing the resources from unauthorized access. Privacy is permitted to be accessed by the user based on access control policy (Bertolissi and Fernandez, 2014; Crampton and Sellwood, 2014; Sandhu *et al*., 2000; Kayes *et al*., 2013; Lazouski *et al*., 2010; Hung, 2005; Ruj *et al*., 2012; Samarati, 2001).

In access control, two most popular models are Trust-Based Access Control (TBAC) and PBAC. TBAC assigns human’s trust to access resources and the user with a higher level of trust will be permitted to access the privacy. Next in PBAC, purpose means for what reason data is collected or used. To permit or deny access to the privacy, the decision in this model considers the factor of purpose.

The weaknesses of current PBAC models are privacy disclosure. Currently, authorized user in the domain who

Corresponding Author: Mohd Rafiz Salji, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Seri Kembangan, Malaysia

are not supposed to access certain privacy is equally permitted to access it. For example, the users in a Human Resource H Department are permitted to access customer's personal information. However, not all users in H supposed to access it, i.e., staff in the training unit in H is assigned to train all staffs in the organization and they are not related to accessing customer's personal information. Therefore, the staff in training unit is not supposed to access it. Besides, they are permitted to access sensitive attributes without any validation of trust. It may cause the inappropriate use of the privacy by 'limited-authorized' user i.e., legitimate users but untrusted and unauthorized to access it.

In this study Performance and Divisional Trust and Purpose-Based Access Control (PDivTPBAC) Model is proposed to permit a specific authorized user with a higher level to access personal information with sensitive attributes. In current PBAC Models, the user's functional purpose fp (the department where they work) needs to be authorized by Access Purpose (AP) to permit access to the privacy (Kabir *et al*., 2011; 2012). AP refers to the user in functional level (based on organizational structure (functional departmentalization)). Besides, current PBAC Models does not consider the user's trustworthiness to access sensitive attributes. In PDivTPBAC, to permit or deny access to personal information or with sensitive attributes, the authorization must consider the user's fp and dp (the unit in the department where they work) to access the personal information and user's rp (the level of seniority and behaviour) to identify their trustworthiness to access sensitive attributes. In order to access the personal information, two methods are introduced to authorize the user's fp and dp. First, the user's fp and dp will be authorized by AP directly. Sec, the user's fp is authorized by AP while dp will be authorized by Divisional Access Purpose (DAP). A responsible person in these two methods is suggested to set the privacy in the divisional level. First, the customer is assigned to set it in the Intended Purpose (IP) while in the sec method, an administrator is assigned to set it in DAP. Moreover, to permit access to sensitive attributes, a comprehensive policy is introduced to authorize the user's trust by using the user's level of seniority and behaviour, called role performance, rp. The quantification method to measure the user's rp is proposed to determine either the user is permitted or denied access to sensitive attributes.

Literature review

Purpose-based access control: In PBAC system, purpose is an essential factor either to permit or deny access to the privacy. Purpose have divided into two types; Intended Purpose (IP) and Access Purpose (AP) (Byun and Li, 2008). In PDivTPBAC, to permit trusted specific authorized user access to the privacy, Divisional Access Purpose (DAP) (Table 1) is proposed as a new type of purpose to authorize user's dp.

Table 1:The illustration of divisional access purpose

Divisional access purpose	
Parameter	Variables
Department:	H
Units:	HRA
Department:	M
Units:	Adv, Dis

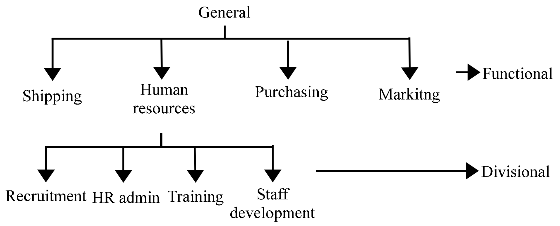

Fig. 1: Purpose tree refers to domains and units

In current PBAC Models, customer is required to set the privacy by using IP to permit authorized user access to their privacy (Byun and Li, 2008; Sun and Wang, 2012; Sun *et al*., 2010). In PDivTPBAC, a responsible person in the two methods is proposed to set the privacy. In the first method, functional and divisional levels (Fig. 1) are set by the customer directly. Next, functional level is set by the customer while divisional level is set by an administrator on behalf of the customer. These two methods have the advantage and disadvant age but both positively releasing the customer's privacy to the target user.

Trust-based access control: To access the privacy, the system requires the most powerful methods to identify the degree of user's trust. Three levels of trust have been proposed in a multi delegation model to permit or prohibit access to the system. The three levels of trust are organized as follows; low (less trust) medium (intermediate trust) and high (highly trust). A user with a higher level of trust is assigned to handle a higher level of delegation task (Li *et al*., 2012). In PDivTPBAC, the user's rp is assigned to identify the user's level of trust which comprises the levels of seniority and behaviour. Two levels of the user's seniority are organized as follows; (junior (less trust) or senior (highly trust)) and three levels of the user's behaviour; (mistrust (junior) trust (senior) or uncertainty (senior performing negative behaviours). The specific authorized user with a higher level of rp (senior-with-trust) are able to access sensitive attributes.

In general, the user's trustworthiness is mutable. The changes to the negative behaviour may revoke user from ongoing access. The administrator has the authority to revoke manually or automatically (Sarrouh, 2013; Toahchoodee *et al*., 2009). In PDivTPBAC, the administrator can change the user's rp manually if the customer proved to perform negative behaviour. It means that the user's behaviour will be changed from trust to uncertainty.

Definition of purpose

Intended Purpose (IP): Customer is assigned to set their privacy to be accessed by the user. They can set their privacy in three options; Allowable Intended Purpose (AIP), Conditional Intended Purpose (CIP) and Prohibited Intended Purpose (PIP).

Allowable Intended Purpose (AIP): Data is permitted to be accessed by the user for certain purposes without any restriction. For example, Bob's income, e.g., 11K.

Conditional Intended Purpose (CIP): Data is allowed to be accessed by the user for certain purposed with certain condition. For instance, Bob's income, e.g., from 11-10-15 K.

Prohibited Intended Purpose (PIP): Data is restricted access by the user for certain purposes. For example, Bob's income, e.g., from 11K to "*".

Access Purpose (AP): The intention of user access to customer's privacy. The privacy was determined by the system.

Departmentalization: One of the key elements in organizational structure and it is the arrangement of individual jobs and activities into logical groups in the organization (Mosweunyane *et al*., 2005; Rehman, 2008; Bianchi, 2000).

Functional departmentalization: The same job or function or skill is grouped together in the organization to form an organized management in the organization (Lunenburg, 2010; Rehman, 2008; Theodore, 2011).

The policy of current PBAC models stated the privacy is allowed, conditionally allowed or restricted access by a third party based on AP (Kabir and Wang, 2009; Kabir *et al*., 2011, 2012). However, in PDivTPBAC, the privacy is allowed, conditionally allowed or restricted access by a trusted specific third party based on AP (first method) or AP and DAP (second method).

MATERIALS AND METHODS

Methods for accessing personal information: Two methods are introduced in the authorization phase. A responsible person is suggested to set the privacy in the divisional level and the explanation is as follows:

Customer:

- Two levels of the privacy are set by the customer (functional and divisional levels) (Fig. 1) directly
- For example, based on Table 2, the customer Bob can set his privacy in income, H (HRA) for AIP
- Advantage
- The privacy is set by the customer itself
- Disadvantage
- Customer unfamiliar with the functions of each unit

Administrator:

- The customer's privacy is set by the administrator at the divisional level by using DAP (Table 1)
- Advantage
- Administrator familiar with all the units
- Disadvantage
- The customer feels not comfortable due to their privacy is set by the administrator

A comprehensive policy for accessing sensitive attributes

Properties: Each role in the organization requires certain properties of a user. In this research, two types of properties are assigned to permit access to sensitive attributes and the explanation is as follows:

Experience:

- Refers to the number of the user's activities that is performed during their substantive service to identify their activeness
- It is assigned to specify the seniority of a user. If the user has achieved the minimum requirement of activeness set by the administrator based on quantification, they are eligible to become a senior
- Two seniority levels; junior (less trust) and senior (highly trust)

Recommendations: Recommendations are assigned by the administrator to evaluate a user's behaviour. User's behaviour refers to the user's attitude shown during their substantive service to identify the trustworthiness of a user. The scope of the user's behaviour in this model refers to the categories that is introduced by Bruhn (2001) in Table 3. Three behaviour levels: mistrust (junior) trust (senior) and uncertainty (senior performing negative behaviours). In this model, the user is permitted to access sensitive attributes if the user' rp is senior-with-trust.

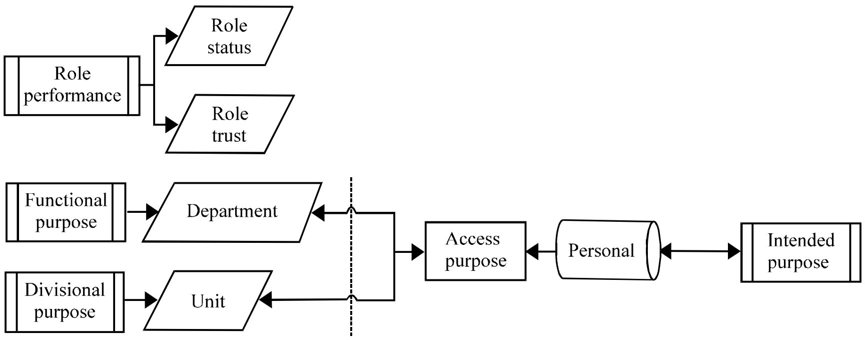

Fig. 2: The illustration of the authorization process (Divisional level set by the customer)

Table.2: Microdata illustrating AIP, CIP and PIP

Name	Age	Address	Income	$Name_{ip}$	Age_{ip}	$Address_{ip}$	$Income_{ip}$
Bob	40	2 May Ave. WA 21000	12K	{{G}, {M{Adv, Dis}}, {P}}	{{G}, {M{Adv, Dis}}, {A,P}}	{{G}, {Ø}, {M,P}}	{{H{HRA}} {A{Sta}}, {M,P}}

G General, A Admin, M Marketing, H Human resource, P Purchasing, Adv. Advertising, Dis. Distribution, HRA HR Admin, Sta. Staffing, Eva. Evaluation, ip Intended Purpose = {AIP, CIP, PIP}

Table. 3: The result appears to comply with AP and DAP

Variable	Name	Age	Address
Result	Bob	40	2 May Ave. WA 21000

Quantifying experience: In PDivTPBAC, a weighing evidence is assigned to quantify the user's experience or activities (Gollmann, 2011). The example of activities organized by companies is as follows; seminar, workshop, courses and others.

Weighing evidence: Weighing evidence can be assigned to quantify and specify the seniority of the user based on their activities. The value of each component is between [0, 1]. Assume the administrator set the minimum required weight is 0.4 and a user Bob's overall score is 0.5. This means that he is permitted to assign as senior role.

Quantifying recommendations: A user's behaviour illustrated by Bruhn (2001) is evaluated by recommendations to specify the user's trustworthiness.

User behaviour evaluation form
Categories:

- Open, participative, accept responsibility
- Highly productive
- Loyalty to the organization
- Not defensive
- Cooperation, work teams
- High job satisfaction
- Problem-solving attitude
- Involvement in decision-making
- Sense of pride in work

Scores for each category will be added first and divided by a number of categories to obtain an overall score. For example, assume a user Bob's overall score is 0.5 and the administrator set the minimum requirement is 0.4. As a result, he is qualified to be assigned as trust.

Access control mechanism: Based on Fig. 2 (first method) the personal information with sensitive attributes can be set by the customer in IP until the divisional level. For example, the customer Bob set his age (Table 2) G for AIP, M (Adv, Dis) for CIP and A and P for PIP. It means that he set his age in two levels, i.e., for CIP, M (functional) and Adv, Dis divisional. If a trusted specific authorized user request to access Bob's privacy, AP will be assigned to communicate with the system.

In Fig. 3 (second method) customer set the privacy only to the functional level. For example, the customer Bob set his age (Table 4) G for AIP, M for CIP and A and P for PIP. To set the privacy in the divisional level, an administrator is assigned on behalf of the customer to set it at the DAP (Table 1). For example, if the user's dp is human resource admin HRA, the system needs to check either HRA is listed or not in DAP. Assume HRA is listed in DAP, therefore, the specific authorized user is permitted to access the personal information. User divisional access purpose database is assigned to store DAP.

If the user's rp is senior-with-trust and fp and dp are in compliance with AP (first method) or AP and DAP (second method) the trusted specific authorized user is permitted to access personal information with sensitive attributes.

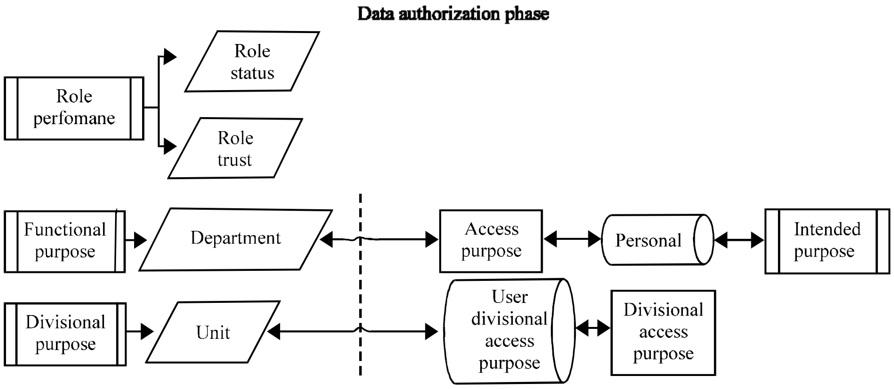

Fig. 3: The illustration of the authorization process (Divisional level set by the administrator)

Table 4: Microdata illustrating AIP, CIP and PIP

Name	Age	Address	Income	Name$_{ip}$	Age$_{ip}$	Address$_{ip}$	Income$_{ip}$
Bob	40	2 May Ave. 21000	12k WA	{{G}, {M}, {P}}	{{G}, {M}, {A,P}}	{{G}, {Ø}, {M,P}}	{{H}, {A}, {M,P}}

G General, A Admin, M Marketing, H Human resource, P Purchasing, ip Intended Purpose = {AIP, CIP, PIP}

RESULTS AND DISCUSSION

To permit or prohibit user access to the personal information or with sensitive attributes, 6 parameters are assigned by the system to identify the user. The parameters are as follows; <u, rp, fp, dp, a, o> where u∈u, rp∈RP, fp∈FP, dp∈Dp, a∈A, o∈O. This model refers action α is to allow user perform read privilege (Mirabi *et al*., 2011) or select operation (to retrieve data) (Ghani, 2013). The parameter states a user u has a Role Performance rp, working at a functional purpose dp in the divisional purpose fp with an action a to access object o.

In parameter 1, Danny is a staff, rp, junior-with-mistrust, work at the Purchasing P, in the unit of Evaluation, the action is set as read privilege or select operation to access the object, privacy. Parameter 1 shows Danny has not achieved a higher level of rp. Meanwhile, Danny's fp and dp is set Purchasing P and Evaluation Eva which does not comply with AP (First method (Table 2)) or AP (Second method (Table 4)) and DAP (Second method (Table 1)). It means that Danny is not allowed to access Bob's privacy.

Next, Emmet's rp is senior-with-uncertainty which has not achieved a higher level of trust. His fp and dp are sets Marketing M and Sales Sal which his fp complies with AP (First and second method (Table 2 and 4)) but dp is not complied with AP (First method (Table 2)) or DAP (Second method (Table 1)). As a result, he is not allowed to access Bob's privacy.

In parameter 3, Flora's rp is senior-with-uncertainty which has not achieved a higher level of trust, meanwhile, her fp and dp are sets H and HRA which complies with AP (Table 2 and 4) and DAP (Table 1). Therefore, she is permitted to access Bob's personal information but denied access to sensitive attribute. Table 4 shows the result of Flora access to Bob's personal information.

Table 5: The result appears to comply with AP and DAP

Variable	Name	Age	Address	Income
Result	Bob	40	2 May Ave. WA 21000	12k

Finally, Caren's rp is senior-with-trust which she has achieved a higher level of trust. Meanwhile, Caren's fp and dp are sets H and HRA which complies with AP (Table 2 and 4) and DAP (Table 1). Therefore, she is permitted to access Bob's personal information with sensitive attribute as shown in Table 5.

CONCLUSION

PdivTPBAC is designed to prevent limited-authorized user access to the privacy. To permit user access to sensitive attributes, role performance rp is assigned to specify the user's trustworthiness. To access personal information, functional purpose fp and divisional purpose dp needs to be complied with AP (first method) or AP and DAP (second method). Two methods are proposed and responsible persons are assigned to set the privacy in functional and divisional level.

IMPLEMENTATIONS

Finally, DAP is proposed to authorize user's dp. As a result, the issue of limited-authorized user to access certain privacy is solved in this model by permitting trusted specific authorized users to access it.

This model able to permit or prohibit user access to personal information or with sensitive attributes. A prototype of PDivTPBAC will be implemented for future work.

REFERENCES

Bertolissi, C. and M. Fernandez, 2014. A metamodel of access control for distributed environments: Applications and properties. Inf. Comput., 238: 187-207.

Bianchi, E.M.P.G., 2000. Internationalization, its impact and implications on organizational structure: The case of oxiteno. Bus. Manage. Rev. Innovation, 1980: 615-627.

Bruhn, J.G., 2001. Trust and the Health of Organizations. Springer, New York, USA., ISBN:0-306-47265-1, Pages:219.

Byun, J.W. and N. Li, 2008. Purpose based access control for privacy protection in relational database systems. VLDB. J., 17: 603-619.

Crampton, J. and J. Sellwood, 2014. Path conditions and principal matching: A new approach to access control. Proceedings of the 19th ACM Symposium on Access Control Models and Technologies, June 25-27, 2014, ACM, New York, USA., ISBN:978-1-4503-2939-2, pp: 187-198.

Ghani, N.A., 2013. Credential purpose-based access control for personal data protection in web-based applications. Ph.D Thesis, University of Technology, Johor Bahru, Malaysia.

Gollmann, D., 2011. From access control to trust management and back-a petition. Proceedings of the 5th IFIP International Conference on Trust Management, June 29-July 1, 2011, Springer, Copenhagen, Denmark, pp: 1-8.

Hung, P.C., 2005. Towards a Privacy Access Control Model for E-Healthcare Services. University of Ontario, Oshawa, Ontario,.

Kabir, M.E. and H. Wang, 2009. Conditional purpose based access control model for privacy protection. Proceedings of the 20th Australasian Conference on Australasian Database, January 01-01, 2009, ACM, Wellington, New Zealand, ISBN: 978-1-920682-73-6, pp: 135-142.

Kabir, M.E., H. Wang and E. Bertino, 2011. A conditional purpose-based access control model with dynamic roles. Expert Syst. Appl., 38: 1482-1489.

Kabir, M.E., H. Wang and E. Bertino, 2012. A role-involved purpose-based access control model. Inf. Syst. Front., 14: 809-822.

Kayes, A.S.M., J. Han and A. Colman, 2013. A semantic policy framework for context-aware access control applications. Proceeding of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), July 16-18, 2013, IEEE, Hawthorn, Australia, ISBN:978-0-7695-5022-0, pp: 753-762.

Lazouski, A., F. Martinelli and P. Mori, 2010. Usage control in computer security: A survey. Comput. Sci. Rev., 4: 81-99.

Li, M., X. Sun, H. Wang and Y. Zhang, 2012. Multi-level delegations with trust management in access control systems. J. Intell. Inf. Syst., 39: 611-626.

Lunenburg, F.C., 2010. The management function of principals. National Forum Educ. Administration Supervision J., 27: 4-10.

Mirabi, M., H. Ibrahim, A. Mamat and N.I. Udzir, 2011. Integrating Access Control Mechanism with EXEL Labeling Scheme for XML Document Updating. In: Networked Digital Technologies, Fong, S. (Ed.). Springer, Berlin, Germany, ISBN:978-3-642-22184-2, pp: 24-36.

Mosweunyane, G., T. Zuva and K.G. Dibetso, 2005. Using VLANS to revolutionalize the organizational structure. Proceedings of the 35th Conference on of SACLA, July 3-6, 2005, University of Botswana, Kasane, Botswana, pp: 69-290.

Rehman, H., 2008. Occupational stress and a functional area of an organization. Int. Rev. Bus. Res. Pap., 4: 163-173.

Ruj, S., M. Stojmenovic and A. Nayak, 2012. Privacy preserving access control with authentication for securing data in clouds. Proceeding of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), May13-16, 2012, IEEE, Ontario, Canada, ISBN:978-1-4673-1395-7, pp: 556-563.

Samarati, P., 2001. Protecting respondents identities in microdata release. Trans. Knowledge Data Eng., 13: 1010-1027.

Sandhu, R., D. Ferraiolo and R. Kuhn, 2000. The NIST model for role-based access control: Towards a unified standard. Proceedings of the ACM workshop on Role-Based Access Control Vol. 2000, July 26-28, 2000, ACM, Berlin, Germany, ISBN:1-58113-259-X, pp: 1-11.

Sarrouh, N., 2013. Formal modeling of trust-based access control in dynamic coalitions. Proceedings of the 2013 IEEE 37th Annual Conference and Workshops on Computer Software and Applications (COMPSACW), July22-26, 2013, IEEE, Japan, ISBN:978-1-4799-2160-7, pp: 224-229.

Sun, L. and H. Wang, 2012. A purpose-based access control in native XML databases. Experience, 24: 1154-1166.

Sun, L., H. Wang, R. Jururajin and S. Sriprakash, 2010. A purpose based access control in XML databases system. Proceeding of the 2010 4th International Conference on Network and System Security (NSS), September 1-3, 2010, IEEE, New York, USA., ISBN:978-1-4244-8484-3, pp: 486-493.

Theodore, J.D., 2011. Organizational size: A key element in the development of private enterprises in the less developed countries: The case of ecuador. Int. Bus. Econ. Res. J. IBER., Vol. 8,

Toahchoodee, M., R. Abdunabi, I. Ray and I. Ray, 2009. A trust-based access control model for pervasive computing applications. Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, July 12-15, 2009, Springer, Montreal, Canada, pp: 307-314.