IJCTA, 9(6), 2016, pp. 2851-2859
© International Science Press

ISSN: 0974-5572

Access Control Management in Collaborative Environment: A Review

S. Rajeshwari* and A. Chandrasekar**

ABSTRACT

The growth of information technology has opened the gate for users of different organizations to work together and share information between them. Even the users of organizations access the same resource from different geographic locations and share the same resource to work in a collaborative nature. The problem of working in collaborative nature is providing security, integrity, privacy preservation, public auditing and more. The security measure describes how the data in collaborative environment has been accessed in secure manner, trust factor represents how the users are evaluated for their trust in accessing the shared data. Privacy preservation is the factor of maintaining the privacy information of different users or organizations from large number of users in collaborative environment. The paper also considers and discuss about how the public auditing is enforced which represents the trustworthy of information the user visit. To provide the above mentioned measures there are number of approaches described in various situations. This paper performs a detailed review in this area of collaborative working and security management and access control policies.

Keywords: ABE, KP-ABE, HIBE, HCRBAC

1. INTRODUCTION

The growth of information technology has opened the gate for the organization to perform their different task without difficulty even though the units of organizations are distributed. The distributed computing has been emerged in the last decade, still the developments are not enough to fulfill the requirements of users. As the technology grows, the organization has started sharing information to reduce the maintenance cost and storage cost. While sharing information between them there are many issues has been raised which affects the security and integrity of the information. To provide such security to the information stored there is a huge requirement of access restriction systems.

By providing security control and access control for the information stored, the data can be shared between the organizations. The organization may maintain different information which are personal to the users of the organization. The organization has the responsibility to safeguard the user secret information. For example, an marketing organization which maintains the trace of purchase of their users. If a user "A", has purchased many products in particular some drugs or special medicines, then the information about the person who purchased the special medicine has to be secured and not to be exposed to any of the organization or to an individual.

Not only the personal information, but also the organization may maintain various other information which has to be secured. In some cases, the purchase patterns and the history of purchase performed by number of global user can be used to perform market analysis, in this case, the organizations shares the information about the purchase history by sharing them with the others. But the individual information

* Research Scholar, Saveetha School of Engineering, Saveetha university, *Email: rajisampath411@gmail.com*

** Professor, Dept of CSE, St. Joseph's College of Engineering, *Email: drchandrucse@gmail.com*

has to be hidden or sanitized. The process of sanitization can be performed in many ways from the attribute level.

The sanitized information can be published or the original information can be shared but the users of the organization could be restricted in different levels. For example, in an marketing organization, the manager could look at the list of access and purchase performed in any day but will be restricted from accessing the user information. Where as the top level users will be allowed to access the user information and so on. This kind of access restriction could be named as profile oriented and similarly the user can be restricted based on the trust, where the trust of any user can be computed in many forms. While applying all these in a collaborative environment the information belong to the specific user or organization can be accessed or shared by many peoples. Whatever the modification performed by any of the user would be reflected on the original copy of the information. Now a day the organizations follow this kind of working principle to reduce the cost of resource and they share the same copy of the resource. Even in the collaborative working environment, the user can be restricted in many ways, by using the attribute based restriction, the user can only view certain attributes which are allowed for him but not all. Similarly, the trust based methods computes trust of any user according to certain factors and only if the user clears the trust check then the user will be allowed to access the data. In case of Profile orient access restriction schemes the environment maintains different user profiles based on the user profile the user will be restricted in accessing certain information. Similarly to secure the data from unauthorized access there are number of access control methods are available.

2. LITERATURE SURVEY

There are number of approaches has been discussed for the problem of access control in collaborative environment, this sections performs a detailed review on various methods

2.1. Generic Access Control Methods:

The access control methods in collaborative environment can be performed in generic access control methods based on key based approaches which may be of security keys. In this domain the attribute based encryption methods are generally being used and different authors have proposed different methods. Attributes have been oppressed to built a secret key for encrypting information and have been utilised as an access rules to monitor users' access. The access policy can be categorized as either key-policy or ciphertext-policy. The key-policy is the access structure on the user's private key, and the ciphertext-policy is the access structure on the ciphertext. And the access structure can also be categorized as either monotonic or non-monotonic one. Using ABE schemes can have the advantages: (1) to reduce the communication overhead of the Internet, and (2) to provide a fine-grained access control [26].

Sahai and Waters described an attribute-based encryption (ABE) model [26] in 2005, and this article proposed the initial idea of the attribute-based encryption scheme. The ABE approach utilisedan user's identification as properties, and a collection of properties were used to encrypt and decrypt information. The ABE model can event the problem that information owner required to use every certified user's secret key to encrypt information.

In 2006, Goyal proposed an key-policy attribute-based (KP-ABE) scheme. This scheme uses a set of attributes to describe the encrypted data and builds a access policy in user's private key. If attributes of the encrypted data can satisfy the access structure in user's private key D, an user can obtain the message through decrypt algorithm.

In 2007, Bethencourt et al. proposed a ciphertext rule attribute-based method, and the entry policy in the encrypted information. The access regulation method of this model is similar to the key policy attribute-based encryption. In key policy attribute-based encryption, the access rule is in user's private key, but the access policy is switched to the encrypted data in ciphertext policy attribute-based encryption. And a set of descriptive attributes are associated with the user's private key, and the access policy is built in the encrypted data.

In 2011, Wang et al. proposed a hierarchical attribute-based encryption scheme composed of a hierarchical identity-based encryption scheme (HIBE) and a ciphertext-policy attribute-based encryption scheme. This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. Moreover, it used disjunctive normal form (DNF) to express the access control policy, and the same domain authority in this scheme administered all attributes in one conjunctive clause. There are five roles in this scheme: the cloud storage service, data owner, the root authority, the domain authority, and data users. The role of cloud storage service is that let a data owner can store data and share data with users. The role of data owner is encrypting data and sharing data with users. The role of the root authority is generating system parameters and domain keys, to distribute them. The role of domain authority is managing the domain authority at next level and all users in its domain, to delegate keys for them. Besides, it can distribute secret keys for users. And users can use their secret keys to decrypt the encrypted data and obtain the message.

2.2. Context Aware Method:

Context aware access control methods verify the user access to the context of data. Based on the verification results the user will be allowed to access the data in the collaborative environment.

HCRBAC–An Access Control System for Collaborative Context-Aware HealthCare Services in Mauritius [1], presents Healthcare Context-Aware Role-Based Access Control) a data access system for the Mauritian healthcare service, where information access within a healthcare organisation is initiated and controlled through the use of circumstance-awareness, while remote entry to data is performed in a secure manner. A fraction of different available access regulation schemes are first examined and a comparative analysis study of these is done. A collection of the different approaches is then used to offer efficient control of the data access model and permitting any healthcare organisation to view up data access to other related organisations, without negotiating confidentiality and integrity of information.

The authors in [30] present a methodology for secure Ad-hoc collaboration, based on the Typed Usage Control (TUCON). It allows capturing the dynamic aspects of collaboration, including both temporal and spatial attributes of objects. The authors argue that their policy scheme allows information flow control beyond organizational boundaries and the autonomy of individual collaborative teams. But like in any other previous models, attributes are only assigned to objects and trust is not taken into account.

2.3. Role-Based Access control (RBAC) Methods:

The role based methods are about restricting the users of collaborative environment according to their role in the environment. Based on the role of user, the user will be allowed to access the requested information. If the role of user has rights to access the data then he will be allowed to access.

(Sandhu et al. 1996) grants access acceptance to data based on authority or roles. End users are made group members of exact roles. The use of roles helps the characterization of access rights as end users roles varies and this compares the idea of positions and authorities in an institution. Promoted or transferred staff members would be allocated new authority and thus automatically inherit new entry rights. RBAC developed from the combination of access rights to end user set, but it goes beyond the roles of groups in that various roles can be established as being bilaterally exclusive and roles can take on bequest. Through the support of constraints (eg. permissions or assignment relations) RBAC enables the enforcement of many different access control policies and thus achieves flexibility (Ramaswamy and Sandhu, 1998). Static and dynamic separations of duties are two of the most common types of RBAC constraints (Sandhu et al. 1996).

Designing Dynamic Access Control rules for Web-based Collective models [35], defines a designing language, called X-Policy, for web-based collective models with changing access control policies. The entry to resources in these models depends on the condition of the system and its composition. The X-Policy language designs systems as a group of actions. These events can model system executions which are operated by users. The X-Policy language permits us to specify operational permissions on each event using complex access situation which can depend on information values, other acceptance, and agent authority. We explain that X-Policy is expressive enough to design collective conference authority systems.

2.4. Proximity Based Access Control Methods:

The proximity based approaches are about restricting the users of collaborative environment according to the proximity value computed for any user.

(Ardagna et al., 2006) is a enhancement of the most common Location-based Access Control (LBAC), which is itself a special case of CBAC, where the circumstance is location. In PBAC, access regulation is based on the reachability of the end user to specific assets to determine access controls. PBAC models consider the subsequent factors: the condition of the physical workspace to identify reachability regions, the 3-D accuracy of the placement system (using Active Badge, RFID, etc) used and the access controls to offer to users within a reachability region (Gupta et al., 2006). Each asset is assigned an access regulation list which is a table holding possible roles known as resource-roles and associating controls.

These controls are based on the end users' group roles (group roles are allocated based on a particular domain a user works) and the system data context (Gupta et al., 2006).

2.5. Trust Based Access Control:

The trust based access control is the method which restricts the access to any resource according to the trust computed on any user. The trust verification is performed using various parameters and there are number of trust based methods are presented.

Trust-based access control for collaborative systems [33], claims that the Traditional access control solutions are inherently inadequate for collaborative systems because they are effective only in situations where the system knows in advance which users are going to access the resources and what are their access rights so that they can be predefined by the developers or security administrators, but in collaborative systems the number of users as well as their usage on resources is not static. Targeting collaborative systems, a fine grained, flexible, persistent trust-based model for protecting the access and usage of digital resources is defined in this paper using radial basis function neural network (RBFNN). RBFNN classifies the users requesting the resources as trustworthy and non-trustworthy based on their attributes. RBFNN is used for classification because of its ability to generalize well for even unseen data and non-iterative method employed in its training. A proof of concept implementation backed by extensive set of tests on the real data collected for one such collaborative systems, i.e. Enabling Grids for E-Science grid demonstrated that the design is sound for collaborative systems where access of resources are provided to large and unknown users with their variant set of requirements.

In order to exclude these malicious peers, peers try to compute their own opinion about the others. This metric should be used in order to determine if a transaction will be performed or not metrics can have different natures, but are often measured by a single value (number, percentage, Boolean) as a combination of several measures. For example, the proposed metric in [40] combines a long-term behavior evaluation (reputation) and a short term one (risk). The reputation is based on a transitive exchange of opinions of a peer about another one. This reputation evolves slowly in the distributed network. On the contrary, the risk is a real-time evaluation of a good or bad behavior of a peer answering a protocol request. This evaluation is useful for detecting a sudden change in the peer's behavior. PET [40] is particularly interesting because it is the first attempt to combine in the trustmetric both reputation and risk. Other works, such as [38], build a trustmetric based on reputation and multiple other factors, such as the number of transactions and the credibility of feedbacks.

2.6. Task Based Access Control Methods

The task based methods restricts the user according to the specific task whether the particular process has the authorization to access the resource.

(Thomas and Sandhu 1993, Thomas and Sandhu 1997) is a dynamic access control method in which access privilege are not allowed to subjects but rather to works in steps related to the advancement of the work. This is advisable for automated processes where the events of tasks cross computer limitation, departmental scope and even organizational scope. In common a task may span different activities that span different network and data set. A work may thus consist of different subtasks that required to be individually or collectively certified. Also, entry to a given entity may be allowed only after a fraction of previous work has been done. (Kang et al. 2001) considers TBAC to be particularly advisable for distributed computing and changing information processing events such as workflow authority and agent-based distributed activity. In the TBAC system, permissions are analysed-in and checked-out in a just-in-time manner, based on events or tasks.

In [43], the authors introduce Secure Flow, which imposes workflow authorization constraints on tasks. It uses an Authorization Template, which is an n-tuple specifying privileges to be granted to a subject of a given role on an object of a given type during a specified time interval. The permissions are activated based on tasks. The authors of [47] propose a role-based specification model for collaboration systems based on requirements of dynamic security policies, with dynamic role management, and especially separation of duties constraints.

2.7. Team Based Access Control Methods:

The team based methods are working to restrict the user according to their team and for different teams there are different access protocols defined.

(Thomas 1997) is an technique of applying role based access regulation in collective scenarios where an task is best achieved through well formed teams. (Altaiby and Chen 2004) explains a team-based access control progress model called TMAC04, designed on RBAC. The TMAC04 method efficiently defines teamwork in the current world. It permits certain users to associate a team based on their available roles in an institution within constrained contexts and new acceptance to perform the needed work. By distinguishing permission assignment from context-based, run-time permission activation, TMAC can be considered an active model of access control. As such, it is able to provide just-in-time permissions and support to a higher degree the principle of least privilege in comparison to passive security models (Georgiadis et al. 2001).

TMAC, [36] that addresses the problem of deploying a role based access control policy in a collaboration environment. This work is also linked to the Task-Based Authorization Control (TBAC) [19] that was proposed to highlight the collaboration between users: new privileges are given to user B when user A has realized a task. This idea is also present in the TMAC model but it is not central as there is no sequences of tasks that validate other tasks. Other similar models of policies have been developed after the first paper about TMAC. For example, in [20, 21, 4], the authors describe a model, OrBAC (Organization based AC), that introduces the notion of organization. Subjects are seen as roles, operations as activities, and objects as views. Each organization has its own policy, as in TMAC teams, and the notion of context is exploited to take into account the dynamicity of the organization policy. All the methods of access restriction protocol has their own merits and demerits which has to be considered while selecting the restriction method.

3. ACCESS RESTRICTION IN COLLABORATIVE SYSTEMS

The access control methods in collaborative environment have greater importance and there are number of access control methods have been described earlier. In any collaborative environment to achieve greater performance and throughput the access restriction has to be implemented in more efficient manner which has to be selected according to the problem notified. Also the solution has to be more optimal and should be more strategic for the kind of environment and application.

The Figure 1, shows the block diagram and various methods of access control in collaborative systems.

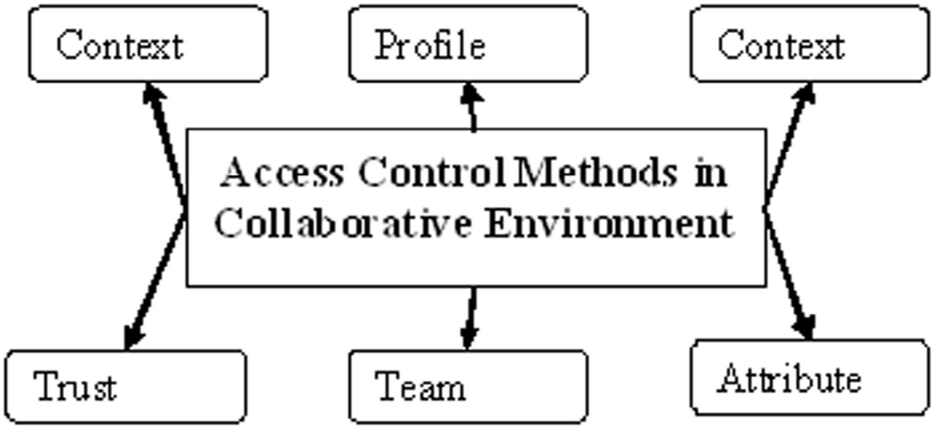

Figure 1: Block Diagram of Access Control methods

4. COMPARATIVE STUDY

This section analyze and describes the above access control approaches with correspond to different benchmark that have been studied relevant to the Mauritian healthcare system, as given below.

- Fraction of Contexts: Large fraction of contexts allow for admirable granularity of ingress control but also offer higher intricacy. A healthcare system generally has to furnish for various situations and also has a large fraction of context data. The appropriate balance between complexity and granularity is a conclusive factor.
- Dynamicity: The healthcare situation is constantly uncertaining; therefore dynamicity is an critical feature for any access control approach to be used in such an situation.
- Platform and Application Domains: This benchmark is used to regulate the correctness of each access control approach to application domains and situation where it is implemented. Suitability for healthcare services can eventually be deduced.
- Flexibility and Adaptability: This benchmark is used to analyze the capability of the access control approach to acclimate to differing environments. A healthcare system commonly attestant a huge fraction of varying unforeseen events. Therefore the access control mechanism used should be malleable and adaptable.
- Centralized/Distributed Management: The objective of this work is to ultimately allow data gathering, storage and usage in the various healthcare organisation of Mauritius and electronic exchange of such information. Therefore it is important to have distributed management of access control.
- Scalability: A healthcare system annoyed the limit of a single healthcare organisation and even that of the healthcare assistance as a whole. Thus, the fraction of conditional users of such a model is likely to be erratic. Consequently, scalability of the access control approach is a important factor.

- Support for user mobility: Offering for user movement in the access control will change in an improved system that allows high-preference users, such as doctors, to monitor patient data from various places in a healthcare organisation, from various organisation and even from their existing place.
- Security Services provided: The security features provided is another vital factor of an access control approach in healthcare environment where highly delicate information is maintained and hence access control information should not be negotiated at any cost.
- Reliability: In a distributed computerized system with a huge fraction of sectors, the failure of one or more sectors at any instance is inexorable. In a healthcare environment which required to be always present, the access control mechanism should be eminently reliable in spite of failures of sectors.
- Performance: However hefty an access control approach may be, user acceptability depends eminently on the feedback time of the model. With the huge volume of information in a healthcare environment, certain care has to be taken to assure the appropriate relation between the performance and the other characters of the access control models.
- Authentication Scheme Used: Since the categories of users accessing data in a healthcare environment is eminently varied, a wide range of authentication schemes required to be examined in order to offer the exact type of entry. Moreover, various authentication schemes may be needed for different entry levels. The following sections below reveal the analysis of the different entry control schemes with relation to the above benchmark. (i) Fraction of contexts RBAC makes use of subject/user data as the only circumstantial information. DRBAC scheme additionally utilizes multiple circumstantial information to examine the context of various subjects/ users. Context limitations are used before assigning response to the subject/user. In CBAC access conditions are allocated dynamically when the circumstance (for example, area, period, role, authentication trust range, category of data used) varies (DuraiPandian et al., 2006). As CBAC, the PBAC model is eminently dependent on the circumstance of the environment to monitor dynamic variations. The circumstance information is combined into three types: user context (for example, the area of the user (reachability), and user's abilities), resource context (for example, ability of the available resource, and existing load on the resource) and system context (for example, fraction of users in reachability of a resource at a given instance (Gupta et al., 2006). TMAC also makes use of different circumstance information, such as periods, shift, and area, can be considered in shaping access control rules.

The TBAC assumes the time of access, the usage fraction and the executing work in addition to the subjects, objects and access policies in traditional access control scheme (Thomas, 1997). (ii) Dynamicity The RBAC system is mostly unchangeable as users are allocated to specific responsibilities and this allocation can only be changed by the system controller. However, in the eminently dynamic and heterogeneous system, the entry privileges of an person depend on its credential, circumstance and existing condition, which are varying. The DRBAC model satisfies these requirements by enhancing dynamicity to role allocations. However, the extent of dynamicity in DRBAC is not exactly defined (Zhang and Parashar, 2003), as this depends on circumstance sensing and processing abilities in the application environments.

The CBAC scheme is also considered as a changing one, since various set of rules are applied when the context varies. It offers dynamic bonding to resources, that is, when the user changes from one domain to another, various sets of policies will be executed before permitting access to the resource (Tripathi et al. 2004).

The Table 1, shows the comparison result on various access restriction protocols and shows the team based access control has greater results.

Table 1
Comparison of access control methods

Technique Name	*Dynamicity*	*Flexibility*	*Centralized/ Distributed*	*Scalability*	*User Mobility*	*Throughput*	*Performance*
RBAC	Static	Low	Centralized	Low	No	High	High
DRBAC	Dynamic	Moderate	Mixed	Moderate	Yes	Moderate	Moderate
TBAC	Dynamic	High	Distributed	High	No	High	–
TMAC	Dynamic	High	Mixed	High	No	High	–

5. CONCLUSION

In this paper, we discussed a detailed review on various methods of access restrictions prescribed by different authors. Each restriction protocols has their own advantages and disadvantages in different factors of access control protocol for collaborative environment. Still the attribute based approaches has more throughput and performance than other methods.

REFERENCES

[1] Oveeyen Mooniana, Sudha Cheerkoot-Jalima, Soulakshmee D. Nagowaha, Kavi Kumar Khedoa, RazviDoomuna, and ZarineCadersaiba, HCRBAC–An Access Control System for Collaborative Context-Aware HealthCare Services in Mauritius, JHIDC, Vol. 2, No. 2, 2008.

[2] Aljareh S. and Rossiter N. “A Task-Based Security Model to Facilitate Collaboration in Trusted Mult-Agency Networks”. SAC 2002,

[3] Madrid, Spain. Ahn G.J., Sandhu R., Kang M. and Park J. “Injecting RBAC to secure a Web-based workflow system”. In Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlin, Germany, 2000.

[4] Alotaiby, F.T. and Chen, J.X. “A Model for Team-based Access Control”. (TMAC 2004). Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC’04), Vol. 2, 450. Alotaiby F.T and Chen J. X. “A Model for Team-based Access Control”. (TMAC 2004), Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC’04) Volume 2, pp. 450, 2004.

[5] Ardagna C.A, Cremonini M., Damiani E., De Capitani di Vimercati S., Samarati P., 2006, “Supporting Location Based Conditions in Access Control Policies”. Proceedings of the ACM Symposium on Information, computer and communications security.

[6] Bardram J.E., Kjær E. R, and Pedersen M. Ø. 2003, “Context Aware User Authentication—Supporting Proximity-Based Login in Pervasive Computing”.

[7] Chou Shih-Chien, Wu Chien-Jung. “An Access Control Model for Workflows Offering Dynamic Features and Interoperability Ability”. International Computer symposium, Dec 15-17 2004, Taipei, Taiwan, pp 1314-1319.

[8] Coulouris G., Dollimore J., Marcus R. “Role and task-based access control in the Perdis groupware platform.” In Proceedings of the 3rd ACM Workshop on Role-Based Access Control. FairFax VA, 115-121.

[9] DuraiPandian, N., Shanmughaneethi, V., Dr.Chellappan, C., 2006. Information Security Architecture-Context Aware Access Control Model for Educational Applications. JCSNS International Journal of Computer Science and Network Security, Vol. 6 No. 12, December 2006

[10] Georgakopoulos, D., Hornick, M. and Sheth, A., 1995. “An Overview of Workflow Management: From Process Modeling to Workflow Automation Infrastructure”. Distributed, and Parallel Databases. Vol. 3, 119-153.

[11] Georgiadis, C.K., Mavridis, I., Pangalos, G. and Thomas, R.K., 2001. “Flexible team-based access control using contexts”. SACMAT 2001, 21-27.

[12] Gupta, S.K.S. Mukheriee, T. Venkatasubramanian, K. Taylor, T.B., 2006, “Proximity Based Access Control in Smart Emergency Departments”. Proceedings of 4th Annual IEEE International Conference

[13] Pereira A.L., Muppavarapu V. and Chung S.M., “Role-Based Access Control for Grid Database Services Using the Community Authorization Service”, IEEE Transactions On Dependable and Secure Computing, Vol. 3, No 2., April June 2006

[14] Ramaswamy, R., Sandhu, R. Role-Based Access Control Features in Commercial Database Management Systems. In Proceedings of 21st NIST-NCSC National Information Systems Security Conference, NISSC’98, 1998

[15] Sandhu R.S., Coyne E.J., Feinstein H.L. and Youman C. E., "Roles-Based Access Control Models" IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.

[16] Thomas R.K., Sandhu R.S., "Towards a task-based paradigm for flexible and adaptable access control in distributed applications" – Proceedings of the 1992-1993 workshop on New Security Paradigms, ACM Press, August 1993.

[17] Thomas R.K., Sandhu R.S., " Task-based authorization control (TBAC): A Family of Models for Active and Enterprise Oriented Authorization Management". Proceedings of the IFIP WG11.3 Workshop on Database Security, Lake Tahoe, California, August 11-13, 1997.

[18] Thomas, R.K. Team-based access control (TMAC): A primitive for applying role-based access controls in collaborative environments, ACM Workshop on Role-Based Access Control 1997: 13-19

[19] Zhang G. and Parashar.M., Dynamic context-aware access control for grid applications. In IEEE Computer Society Press, editor, 4th International Workshop on Grid Computing (Grid 2003), pages 101–108, Phoenix, AZ, USA, November 2003.

[20] Zhang, G. and Parashar M. "Context-aware Dynamic Access Control for Pervasive Applications". Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), San Diego, CA, USA, 2004.

[21] Zhang C., Hu Y. and Zhang G. "Task-Role Based Dual System Access Control Model", International Journal of Computer Science and Network Security (IJCSNS) Vol. 6 No. 7B, July 2006.

[22] Zhang Z., "Scalable Role & Organization-Based Access Control and its Administration", PhD Thesis submitted to the George Mason University, April 2008.

[23] Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang, A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments, International Journal of Network Security, Vol. 15, No. 4, PP. 231-240, July 2013.

[24] Sahai and B. Waters, "Fuzzy identity based encryption," Advances in Cryptology V EUROCRYPT, vol. 3494 of LNCS, pp. 457–473, 2005.

[25] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proceedings of the ICALP, pp. 579–591, 2008

[26] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

[27] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute based encryption with non-monotonic access structures," in Proceedings of the 14th ACM conference on Computer and communications security, pp. 195– 203, 2007.

[28] Sahai and B. Waters, "Fuzzy identity based encryption," Advances in Cryptology EUROCRYPT, vol. 3494 of LNCS, pp. 457–473, 2005.

[29] PunamBedia, HarmeetKaurb&BhavnaGuptaa*, Trust-based access control for collaborative systems, Journal of Experimental & Theoretical Artificial Intelligence, Volume 26, Issue 1, 2014

[30] Z. Liang, W. Shi, PET: a personalized trust model with reputation and risk evaluation for p2p resource sharing, in: Proceedings of the 38th Annual Hawaii International Conference on System Sciences, IEEE, 2005, pp. 201b.

[31] R.K. Thomas, R.S. Shandu, Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management, in: Proc. IFIPWG11.3Workshop on Database Security, Chapman & Hall, 1998, pp. 166–181.

[32] F. Cuppens, A. Miège, Modeling contexts in the Or-BAC model, in: The 19th Annual Computer Security Applications Conference, Las Vegas, Nevada, USA, 2003.

[33] W.-K. Huang, V. Atluri, Secure Flow: a secure web-enabled workflow management system, in: ACMWorkshop on Role-based Access Control, 1999, pp. 83–94.

[34] F. Cuppens, A. Miège, Administration model for Or-BAC, International Journal of Computer Systems Science and Engineering (CSSE) (2004).

[35] G. Mori, F. Paternò, C. Santoro, CTTE: support for developing and analyzing task models for interactive system design, IEEE Transactions on Software Engineering 28 (8) (2002) 797–813.

[36] R. Thomas, R.S. Sandhu, Conceptual foundations for a model of task-based authorizations, in: Proceedings of 7th IEEE Computer Security Foundations Workshop, Franconia, NH, 1994, pp. 66–79.

[37] A.R. Tripathi, T. Ahmed, R. Kumar, Specification of secure distributed collaboration systems, in: Proceedings of the Sixth International Symposium on Autonomous Decentralized Systems, ISADS 2003, IEEE, 2003, pp. 149–156.