Enhancing Role-Based Access Control Model through Fuzzy Relations

Hassan Takabi Morteza Amini Rasool Jalili
Network Security Center
Computer Engineering Department
Sharif University of Technology
Tehran, Iran.[*]
{takabi@ce., m_amini@ce., jalili@}sharif.edu

Abstract

Role-Based Access Control (RBAC) model is naturally suitable to organizations where users are assigned organizational roles with well-defined privileges. However, due to the large number of users in nowadays online services of organizations and enterprises, assigning users to roles is a tiresome task and maintaining user-role assignment up-to-date is costly and error-prone. Additionally, with the increasing number of users, RBAC may have problems in prohibiting cheat and changing roles of users. In order to categorize information and formulate security policies, human decision making is required which is naturally fuzzy in the real world. This leads using a fuzzy approach to address the issue in order to provide a more practical solution. In this paper, applicability of fuzzy set theory to RBAC has been investigated by identifying access control building blocks which are fuzzy in essence. An existing RBAC model is extended to allow imprecise access control policies, using the concept of trustworthiness which is fuzzy in nature. We call the extended model as Fuzzy RBAC. Applicability of the extended model has been evaluated through some case studies.

1. Introduction

Role-based access control (RBAC) has emerged as a promising alternative to traditional mandatory access control (MAC) and discretionary access control (DAC) models. RBAC is naturally suitable for organizations where users are assigned organizational roles with well-defined access control privileges. In RBAC, roles represent functions within a given organization and access permissions are granted to roles instead of users. Permissions granted to a role, are related to actions or transactions required to achieve the functions of the role. Thus, users can activate a subset of the roles which they are a member and easily acquire all required permissions.

Main advantages of RBAC include simplifying the security management and support for security principles such as least privilege and separation of duty. Also RBAC models have been shown to be policy-neutral, can express a wide range of security policies including the mandatory and discretionary ones, as well as user-defined or organizational specific policies [11].

Because of the above-mentioned benefits as well as the possibility of using RBAC model to an environment with multiple policy domains, RBAC has been extensively investigated and several extensions to it have been proposed [2], [11], [12], [13], [14], [15], [16]. Although this model has reached a relatively good maturity level, there are still many application requirements that cannot be supported by this model and its different variants. Conventional RBAC model was designed with this assumption that security officers manually assign users to roles. However, in recent years, the perspective of information technologies has changed and many organizations and enterprises such as banks, insurance industry and utility companies, provide online services to their very large number of users. For such enterprises, manually assigning users to roles may not be possible. These factors show that manually assigning users to roles is a tiresome task and maintaining user-role assignment up-to-date is costly and error-prone. Also, with the increasing number of users, RBAC has problems in prohibiting cheat and changing roles of users. It seems using a fuzzy approach to addressing the issue, can provide a more practical way of dealing with such a problem.

In this paper, we investigate the applicability of fuzzy set theory into RBAC through identifying the access control building blocks having fuzzy nature. The concept of trust and trustworthiness has been utilized in this aspect. Then, we extend RBAC with fuzzy parameters to allow imprecise

[*] This work is partially supported by Iran Telecommunication Research Center(ITRC) under grant number 500/8478.

0-7695-2876-7/07 $25.00 © 2007 IEEE
DOI 10.1109/IAS.2007.69

access control policies, what we call it ”Fuzzy RBAC”. The applicability of the idea is shown through a real example.

The remainder of this paper is organized as follows. Section 2, discusses related work. In Section 3, we give an informal description of the model and describe our method for applying fuzzy set theory into RBAC model. In section 4, we present a formal definition of the model. Finally section 5 exemplifies proposed model to proof its applicability in the real environment.

2. Related Work

Some researches are targeted to addressing the usefulness of fuzzy theory to security management and applying fuzzy set theory to the access control models. In [1], Kendel uses fuzzy set theory to policy analysis. Hosmer [7] shows that in many security policies, particularly in nontraditional ones such as privacy, need-to-know, integrity and availability, fuzziness is inherent. Furthermore, she investigated the applicability of fuzzy approach to multiple policy systems. Also, in [8], Hosmer reviews basic fuzzy logic concepts, illustrates their usage with examples from computer security, and incorporates fuzzy logic into the Multipolicy Machine architecture. Ovchinnikov in [9], [10], presented an attempt to build a mathematical foundation for modeling secure computer systems in a fuzzy environment. He offers a fuzzy version of the Bell-LaPadula model. Other researchers, Richard A. Alo, *et al.*, have provided a fuzzy access control model in distributed systems. The model provides additional level of security checks based on heuristic information kept about various system components. They present an algorithm for estimating a fuzzy relation between a fuzzy set and its fuzzy attributes and apply it to computing the probability of hostility of a user in the context of the security access control model [3], [4]. Also, in [5], they provided a similar method for threat analysis. The proposed algorithm generates the data from the historical information and its earlier runs using fuzzy relational equations. In [6], Berrached A., *et al.*, presented an algorithm for reinforcing access control based on heuristic information about the user, the data being accessed, and the various system components. The model uses fuzzy set theory to assess the risks involved in granting the requested service based on uncertain/partial information. The research presented in [18], provided a method to improve user-role assignment in RBAC using fuzzy set theory.

3. Basic Fuzzy Concepts and Definitions

To facilitate understanding the model, the terminology and notations of fuzzy set theory are introduced in this section and then some basic fuzzy concepts, are defined.

In what follows, I denotes the unit interval [0,1], $x \wedge y = min\{x, y\}$, and $x \vee y = max\{x, y\}$.

Universe of Discourse

The Universe of Discourse is the range of all possible values for an input to a fuzzy system. Usually showed with U.

Fuzzy Set

A Fuzzy Set is any set that allows its members to have different grades of membership (membership function) in the interval [0,1]. Fuzzy Set A on U is completely defined by its *membership function* $A : U \longrightarrow I$. A fuzzy set usually represented by $A = \sum A(x)/x$ that $A(x)$ is a member of the set and x is its membership degree.

Support

The Support of a fuzzy set A is the crisp set of all points in the Universe of Discourse U such that the membership function of A is non-zero.

A fuzzy set A is a subset of a fuzzy set B ($A \subseteq B$) if and only if $A(x) \leq B(x)$ for all $x \in U$. Basic operations of intersection, union, and complement are defined in terms of membership functions as follows:
$(A \cap B)(x) = A(x) \wedge B(x)$
$(A \cup B)(x) = A(x) \vee B(x)$
$A(x) = 1 - A(x)$
for all $x \in U$

Maximizing set of two fuzzy sets

Let A and B be two fuzzy sets. Maximizing set of A and B is the fuzzy set M that consists all supports from A and B. Membership degree of each support equals the ratio of the support itself to the maximum support of A and B.

Fuzzy Relation R

Assume that **X** and **Y** be two finite sets and **R** a fuzzy relation from **X** into **Y**. Relation **R** is a fuzzy subset of the Cartesian product **X** × **Y**. We show **R** by a matrix with coefficients in the interval [0,1], where for all $x \in X$ and $y \in$ **Y**, *R*[x,y] represents the membership degree of (x,y) in **R**.

Operator α

Assume that A and B be two fuzzy membership functions in **X** and **Y**, respectively. For all $y \in$ **Y**, the α operator defined as:

$[A\alpha R](y) = sup_{x \in X}\{min\{A(x), R(x, y)\}\}$

where **Y** includes a finite set of values that can be assigned to B. Note that $A\alpha R$ is a fuzzy subset of Y.

Indeed, the α operator, also called the *sup-min composition* of fuzzy set A and fuzzy relation R, can be considered as the shadow of the relation R on the fuzzy set A.

Operator β

We define the fuzzy implication operator β on $[0, 1] \times [0, 1]$ as:

$a\beta b = sup\{c \mid 0 \leq c \leq 1, a \wedge c \leq b\}$

Greatest Membership Degree of a fuzzy set

Let A be a fuzzy set. GMD(A), presents the greatest membership degree of A.

4. Fuzzy Role-Based Access Control Model

In order to improve RBAC, first we define trust and trustworthiness concepts, then we introduce user trustworthiness and role's required trustworthiness parameters and describe how to use these parameters to improve user assignment (UA) and role activation in RBAC. Finally, we present an algorithm to compute these two parameters using fuzzy relation equations.

4.1. Trust and Trustworthiness

Trust as a common phenomenon, is a fundamental concept in human behavior. Without trust, a person would not be able to encounter the complexities of the real world. It is due to the fact that trust gives us the capability to reason perceptibly about the events of everyday life. There are a variety of views about trust and trustworthiness and also many ways in determining trust. Also trust is imprecise and indefinite; when it is attempted to express trust or a trust level, there are some vagueness and uncertainty As the nature of trust is complex and fuzzy, we use fuzzy set theory for measurement and prediction of trustworthiness.

We define two parameters related to the concept of trust and trustworthiness. The first parameter is user trustworthiness (UT) which means how much a user in system is reliable and how mush we trust him/her to assign a specific role or roles in RBAC. The second parameter is role's required trustworthiness (RT) which determines the amount of trust is required by a user to play the role in system. In the next two sections, we present a method for computing the two above parameters. After computing a user trustworthiness (UT) and a role's required trustworthiness (RT), user assignment (UA) is performed based on the trust level of the user (UT) in comparison with the required trust level of the role (RT).

4.2. Description of the Model

Assume an organization uses RBAC. We define a set of users $U = \{u_1, u_2, ..., u_n\}$ where u_i identifies a user of the system, and a set of roles $R = \{r_1, r_2, ..., r_m\}$ where r_j represents a role in the organization. The level of trustworthiness of a user (UT) and role's required trustworthiness (RT) can be computed using users attributes and roles permissions, respectively. In linguistic terms, a user can be identified as very trusted, trusted, somewhat trusted, or distrusted. For improving user assignment (UA) relation and role activation in RBAC, we propose the following procedure:

Step 1. Compute the user trustworthiness UT_i for user u_i and the role's required trustworthiness RT_j for role r_j.

Step 2. Construct the maximizing set M of fuzzy sets UT_i and RT_j.

Step 3. Compute $(UT_i \wedge M)$ and $(RT_j \wedge M)$.

Step 4.

- In user assignment(UA) relation, user u_i can be assigned to role r_j, if and only if $GMD(UT_i \wedge M) \geq GMD(RT_j \wedge M)$.
- In role activation, user u_i can activate role r_j, if and only if $GMD(UT_i \wedge M) \geq GMD(RT_j \wedge M)$.

4.3. Computing user trustworthiness

In this section, we present our algorithm using fuzzy equations to estimate the value of user trustworthiness (UT). It is obvious that the value of UT is dependent on the attributes of the user. The key challenge in the measurement and prediction of trustworthiness is that, what attributes affect the value of trustworthiness. Note that the list of attributes of a user is dependent on the specific requirements and circumstances of each system, and will be different from one system to another. The attributes that we use in this paper as sample, are the most important attributes gathered from trust computation and trust modeling literature.

Note that some attributes of the user are dynamic (e.g. users age, environment, ...), whereas others are static. Thus, to compute user trustworthiness, we can use only static attributes or both static and dynamic attributes. The user trustworthiness that computed using only static attributes used in user-role assignment and the user trustworthiness computed using both static and dynamic attribute used in role activation.

Assume that Y includes a finite set of values that can be assigned to a user trustworthiness (UT). For example, $Y = \{0, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1\}$. X represents the set of attributes that effect UT. For example, we can define X to consist of the following attributes:

- Behavioral history
- Psychological predisposition
- Personal characteristic
- Capability: the user's intelligence, skills, knowledge and experience[17].

- Willingness: the volition of a user to act or be ready to act, honestly, truthfully, reliably[17].
- Predictability
- Reputation: perception that an agent creates through past actions about its intentions and norms[17].

We assume that the value of these attributes are assigned by an expert in system and this value is a number between 0 and 1. Note that $A\alpha R$ is a fuzzy subset of Y. In addition, since our definition of the α operator is based on sup-min composition, $[A\alpha R](y)$ represents the strongest support to the belief that UT equals y. Therefore, we conclude that, for all $y \in Y$, $UT(y) = [A\alpha R](y)$; or more briefly:

$$UT = A\alpha R \tag{1}$$

According to equation (1), having a given fuzzy relation R and a set of attributes A for a user, we can compute the trustworthiness (UT) for that user. Reversely, having a given value of user trustworthiness (UT) and a set of attributes A for a user, we can solve equation (1) and compute the relation R. Equation (1) may have more than one solution; i.e. more than one relation may satisfy the equation for a given pair of A and UT. Thus, the maximal fuzzy relation that satisfies equation (1) is given as[3]:

$$\widehat{R} = A\beta UT \tag{2}$$

Equation (2) provides the strongest association between A and UT that satisfies equation (1). In addition to, note that fuzzy relation $widehatR$ can interpreted as a set of fuzzy inference rules between A and UT.

4.3.1 Training phase: Maximal Fuzzy Relation Estimation

In previous section, we established an equation for computing the value of trustworthiness (UT) for a user with a set of attributes A (equation (1)), given a fuzzy relation R between A and UT. Equation(2) gives the maximal fuzzy relation between a pair of A and UT that satisfies equation (1). In order to find a fuzzy relation R that can be used to compute the trustworthiness for any user given his/her set of attributes A, we need to establish a correspondence between certain sets of attributes and certain values of UT. We train the system for estimating the relation R. The estimation problem can be formulated as follows:

Assume that we have a set of pairs of fuzzy sets $(A_1, UT_1), (A_2, UT_2), .., (A_n, UT_n)$, we want to estimate relation R such that for all k=1,2,,n the relation R satisfied in equations:

$$A_k \alpha R = UT_k \tag{3}$$

Indeed, the mentioned set of pairs can be viewed as a training set based upon which R is estimated. Assuming the training set is well designed, given the user's set of attributes A, the estimated relation can be used to compute the trustworthiness UT for any user. As discussed in the previous section, each equation in the system of equations (3) may have more than one solution with the maximal solution given by equation (2). Let R_k be the set of relations that satisfy the k^{th} equation of the system:
$R_k = \{R \mid A_k \alpha R = UT_k\}$
Note that if $\bigcap_{k=1}^{n} R_k = \phi$, then the system of equations has no solution.
However, if $\bigcap_{k=1}^{n} R_k \neq \phi$ it can be shown[3] that the maximal relation that satisfies the system of equations can be computed by intersecting all the fuzzy maximal relations that satisfy the individual equations; i.e.:

$$\widehat{R} = \bigcap_{k=1}^{n} \widehat{R}_k \tag{4}$$

where, $\widehat{R}_k = A_k \beta UT_k$
From a practical point of view, there is no simple way to verify condition (4). We therefore take the following three-step approach to estimating relation R:
1) Solve each equation of system (3) individually, using equation (2) to find the maximal relation $\widehat{R}_k = A_k \beta UT_k$.
2) Compute $\widehat{R} = \bigcap_{k=1}^{n} \widehat{R}_k$
3) Verify that $\widehat{R}$ as computed in step 2 satisfies each equation in system (3). If it does not satisfy each equation then it is not a solution; otherwise, $\widehat{R}$ is the maximal relation that can be established between the user attributes and the user trustworthiness.

4.4. Computing role's required trustworthiness

Similar to previous section, we can estimate the role's required trustworthiness RT. However, here the set of attributes A, is indeed role's permissions. In RBAC each role has a set of permissions that identified by permission assignment(PA) relation. We show this set by $Perm = \{perm_1, perm_2, ..., perm_n\}$. For computing the role's required trustworthiness (RT), in equation (1) set A replaced with set Perm. Indeed, the elements of set A are role's permissions and we have:

$$RT = A\alpha R \tag{5}$$

Other equations and steps are similar to computing UT.

5. Application Example

In order to illustrate applicability of the proposed model, access control model of a university is given as an example. The model components are defined as follows:
$ROLES = \{FullProfessor, AssociateProfessor, AssistantProfessor, Lecturer, Senior, Junior, Sophomore, Freshman\}$
$USERS = \{Alice, Bob, Cathy, Dina, Eva\}$
To exemplify the presented algorithm, we define X, Y as follows:
$Y = \{0, 0.2, 0.4, 0.6, 0.8, 1\}$
X=$\{$Behavioral history, Psychological predisposition, Personal characteristic, Capability, Willingness, Predictability, Reputation$\}$
A and UT are fuzzy membership functions in X and Y, respectively. Assume the following small training set consists of two pairs of fuzzy sets (for users Alice and Bob):
$A_1 = [0.9, 0.1, 0.1, 0.9, 0.2, 0.2, 0.9]$
$UT_1 = [0.9, 0.7, 0.3, 0.2, 0.1, 0.1]$
$A_2 = [0.1, 0.9, 0.9, 0.1, 0.9.0.9, 0.1]$
$UT_2 = [0.1, 0.1, 0.4, 0.5, 0.9, 0.9]$
Using equation (2), we have:

$$\widehat{R}_1 = \begin{pmatrix} 0.9 & 0.1 & 0.1 & 0.9 & 0.2 & 0.2 & 0.9 \end{pmatrix} \beta \begin{pmatrix} 0.9 \\ 0.7 \\ 0.3 \\ 0.2 \\ 0.1 \\ 0.1 \end{pmatrix} = \begin{pmatrix} 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \\ 1 & 1 & 1 & 1 & 0.1 & 0.1 \\ 1 & 1 & 1 & 1 & 0.1 & 0.1 \\ 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \end{pmatrix}$$

Analogously, we have:

$$\widehat{R}_2 = \begin{pmatrix} 0.1 & 0.9 & 0.9 & 0.1 & 0.9 & 0.9 & 0.1 \end{pmatrix} \beta \begin{pmatrix} 0.1 \\ 0.1 \\ 0.4 \\ 0.5 \\ 0.9 \\ 0.9 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

, and
Using equation (4), we have:

$$\widehat{R} = \bigcap_{k=1}^{2} \widehat{R}_k = \begin{pmatrix} 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 0.1 & 0.1 \\ 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \end{pmatrix}$$

Now, we verify that following equations are satisfied with $\widehat{R}$:
$A_1 \alpha \widehat{R} = UT_1, \; A_2 \alpha \widehat{R} = UT_2$
We have:

$$\begin{aligned} A_1 \alpha \widehat{R} &= sup(min(\\ & \begin{pmatrix} 0.9 & 0.1 & 0.1 & 0.9 & 0.2 & 0.2 & 0.9 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 0.1 & 0.1 \\ 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \end{pmatrix})) \\ &= \begin{pmatrix} 0.9 \\ 0.7 \\ 0.3 \\ 0.2 \\ 0.1 \\ 0.1 \end{pmatrix} = UT_1 \end{aligned}$$

and

$$\begin{aligned} A_2 \alpha \widehat{R} &= sup(min(\\ & \begin{pmatrix} 0.1 & 0.9 & 0.9 & 0.1 & 0.9 & 0.9 & 0.1 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 1 & 1 \\ 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 0.1 & 0.1 \\ 0.1 & 0.1 & 0.4 & 0.5 & 0.1 & 0.1 \\ 1 & 0.7 & 0.3 & 0.2 & 0.1 & 0.1 \end{pmatrix})) \\ &= \begin{pmatrix} 0.1 \\ 0.1 \\ 0.4 \\ 0.5 \\ 0.9 \\ 0.9 \end{pmatrix} = UT_2 \end{aligned}$$

We computed the maximal fuzzy relation R which satisfies the given training set. Now, having the values of user's attributes, we can compute his/her trustworthiness level.

6. Conclusion

In this paper, we applied fuzzy relations into the RBAC model. The proposed model extended RBAC with fuzzy parameters to allow imprecise access control policies using the concept of trust and trustworthiness, which is fuzzy in nature. The applicability of the model was illustrated using a sample application. In comparison to RBAC, our model is more pragmatic, and can provide imprecise access control policies. Enhancements to the model can be considered as future work. We are currently working on investigating applicability of fuzzy relation equations to model separation of duty policies.

References

[1] Kandel, *Fuzzy Statistics and Policy Analysis*, Fuzzy Sets: Theory and Applications to Policy Analysis and Information Systems, ed. By P. Wang and S. Chang, Plenum Press, New York, 1980.

[2] ANSI. American National Standard for Information Technology- *Role Based Access Control*, ANSI INCITS 359-2004, February 2004.

[3] R. Alo, A. Berrached, A. De Korvin, and M. Beheshti, *Using Fuzzy Relation Equations for Adaptive Access Control in Distributed Systems*, In proceedings of the International Conference In Advances In Infrastructure For e-Business And Education On The Internet. L'Aquila, Rome, Italy, pp. 176-184, 2000.

[4] A. Berrached, M. Beheshti, A. De Korvin, and R. Alo, *An Access Control Model Based On Fuzzy Set Theory*, In proceedings of the 8th International Conference on Information Processing and Management Of Uncertainty In Knowledge Based Systems. Madrid, Spain, pp. 890-895, 2000.

[5] A. Berrached, M. Beheshti, A. De Korvin, and R. Alo, *Applying Fuzzy Relation Equations to Threat Analysis*, In proceedings of the 35th Annual Hawaii International Conference on System Sciences, pp. 684-688, 2002.

[6] A. Berrached and A. De Korvin, "Reinforcing Access Control Using Fuzzy Relation Equations," In proceedings of The 2006 International Conference on Security and Management, 2006.

[7] H. Hosmer, *Security is fuzzy!: applying the fuzzy logic paradigm to the multipolicy paradigm*, In proceedings of the New Security Paradigms Workshop, pp. 175-184, 1993.

[8] H. Hosmer, *Using Fuzzy Logic to Represent Security Policies in the Multipolicy Paradigm*, ACM Special Interest Group on Security, Audit, and Control (SIGSAC) Review,Vol. 10, No. 4, pp. 12-21, 1992.

[9] S. Ovchinnikov, *Fuzzy Sets and Secure Computer Systems*, In proceedings of the New Security Paradigms Workshop, Little Compton, Rhode Island, United States, pp. 54-62, 1994.

[10] S. Ovchinnikov, *Modeling security systems in a fuzzy environment*, In proceedings of the IPMU Information Processing and Management Of Uncertainty In Knowledge Based Systems, Granada, Spain, pp. 617-622, 1996.

[11] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, *Role Based Access Control Models*, IEEE Computer, Vol. 29, No. 2, pp. 38-47, 1996.

[12] D. F. Ferraiolo, R. Sandhu, S.Gavrila, D.R. Kuhn, and R. Chandramouli, *Proposed NIST Standard for role based access control*, ACM Transactions on Information and system securiy, Vol. 4, No. 3, pp. 224-274, 2001.

[13] E. Bertino, P. A. Bonatti, and E. Ferrari, *TRBAC: A Temporal Role-based Access Control Model*, ACM Transactions on Information and System Security, Vol. 4, No. 3, pp. 191-233, 2001.

[14] M. J. Moyer, and M. Ahamad, *Generalized Role-Based Access Control*, In proceedings of the 21st International Conference on Distributed Computing Systems, Mesa, USA, pp. 391-398, 2001.

[15] M. A. Al-Kahtani, and R. Sandhu, *Rule-Based RBAC with Negative Authorization*, In Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04) , pp. 405-415, 2004.

[16] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, *A Generalized Temporal Role-Based Access Control Model*, IEEE Transactions on Knowledge and Data Engineering, Vol. 17, No. 1, pp. 4-23, 2005

[17] E. J. Chang, F. K. Hussain, and T. S. Dillon, *Fuzzy Nature of Trust and Dynamic Trust Modelling in Service Oriented Environments*, In Proceedings of the 2005 workshop on Secure web services, pp. 75-83, 2005.

[18] H. Takabi, M. Amini, and R. Jalili, *Trust-Based User-Role Assignment in Role-Based Access Control*, In Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 2007), 2007.