International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Token and Session Compatibility in Role Based Access Control with Privileges Management

Shashank Shekhar
Ch. Brahm Prakash Govt. Engineering College
New Delhi, India

Niteshkumar
Ch. Brahm Prakash Govt. Engineering College
New Delhi, India

Abstract **– With the advent growth of organizational expectations, the new ability of security systems is revolutionized to secure confidentiality and integrity of the system interface. The Token security system framework proposed in this paper reduces the gap between Session management and Token. This replica further improves the older models which are not agile enough to handle the granularity of the user roles provided. The model elaborates the flexible Token security system (TSS) with the access authorization to the user interface. The model is divided into six main stages to accommodate the user authentication. Finally, the implementation of TSS becomes safer in the newer architecture.**

Keywords-management; token security; session establishment; RBAC

I. INTRODUCTION

Access is the ability to enter into a computer resource. An access control system enables an authority to control access to areas and resources in a given physical quantity or computer based system. With the rapid growth of information technologies, it is obviously convenient and efficient to provide good security services. Access control is a term for security practice that is supported by security systems and provides a way for security management [16] [17] delivered via the Internet. Security issues are the major issues in the enterprise and e-management .Security requirements reached at the market level, initiating the need for models that can handle the industrial & distributed aspects of information usage. A security model provides a formal presentation of the access control security, policy and its working method. The main aim of information security is to ensure Confidentiality, Integrity and availability of information assets. The information security [17] regulates the confidentiality to prevent the access to or the disclosure of information to unauthorized entities. The Integrity of the security system ensures the information that is available to authorized users. Moreover, the availability provides the ability of authorized users to have access to information resources when they need or request for it. **Access control** the system. A given information technology (IT) infrastructure can implement access control systems in many places and at different levels. The objectives of an access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in system are often described in terms of protecting system resources against inappropriate or undesired user access. A sufficiently finegrained access control mechanism can enable selective sharing of information where in its absence, sharing may beconsidered too risky altogether. The granularity of the access control system requires some of the access control parameters [1][14]which are thebeneficial points of a system based on the access control mechanism. The object can be the pioneer parameter which works as an entity that contains or receive information and provide access to an object potentiallyimplies access to the information it contains. An active entity, the subject is generally in the form of a person, process, or device that causes information to flow among objects (see below) or changes the system state.A list (**Access Control List (ACL))** associated with an object that specifies all the subjects that can access the object, along with their rights to the object. This list maintain the policies and it is the root of all the lists. All the parameters of access control [1]are interrelated with each other to provide maximum security.There is the principle of **Separation of Duty (SOD) [7]** that no user should be given enough privileges to misuse the system. Including a basic parameter which can be helpful , is the **Domain and Type Enforcement,** it explains aboutthe grouping of processes into domains, and objects into types, such that access operations (such as read, write, execute, and create) are restricted from domains to types and between domains. An access control system should maintain the safety of its database by implementing the measures [15]that the access control configuration (e.g., access control mechanism or model) will not result in the leakage of permissions to an unauthorized principal.

II. MECHANISMS &MODELS

The mechanism defines the low level functions that implement the controls imposed by the policy and formally stated in the model. The access control mechanism must work as reference monitor (a trust component intercepting each and every request to the system) [6]. The properties it resembles are the "tamper proof" (states that the properties are not possible to change). The next one is "non bypassable" which states that the security mechanism must mediates all access to the system and its resources. The "security kernel "states that the mechanism should must be confined to the limited part of the system. Security mechanism should be "small" such that it must have size in its limit to be suspectible of rigorous verification methods. The policies defines the (high level) rules according to which access control must be regulated .Access control policies can be grouped into three main classes:

A. DISCRETIONARY ACCESS CONTROL (DAC):

DAC (Discretionary access control) is the least restrictive model. It allows an individual complete control over any objects they own along with the programs associated with those objects. It was developed to implement the access control matrices defined by Lampson in his paper [1] on system protection.

Access control Matrices are usually represented as three dimensional; matrices
where rows are subjects, columns are objects and the mapping of subject and object pairs result in the set of rights the subject had over the object. It allows subjects the discretion to decide access rights on objects they own. DAC access settings are typically stored as either per-object file permission mode (default on UNIX) or as lists. It has two major weakness [1], first it gives the end user complete control to set security level settings for other users which could result in users having higher privileges than they're supposed to be and, secondly, the permissions that the end user has are inherited into other programs they execute which means the end user can execute malware without knowing it & the malware could take advantage of the potentially high level privileges the end user possesses.

B. Mandatory access control (MAC):

MAC is defined as any access control model that enforces security policies independent of user operations. MAC model [1] gives only the owner and custodian management of the access controls. This means the end user has no control over any settings that provide any privileges to anyone. Mandatory access control is usually associated with the 1973 Bell-LaPadula [1] [12] model of multilevel security. The MAC method is primarily developed for purposes where confidentiality is far more important than integrity, Biba's influence was minor on further development of MAC models. Mac systems are difficult and expensive to implement due to the reliance on trusted components and the necessity for applications to be rewritten to adhere to MAC labels and properties [12].

C. Role Based Access Control (RBAC):

RBAC is considered a much more generalized model in compare to both the MAC & DAC, encompassing both the models as special cases providing a policy neutral framework which allows RBAC to be customized on a per-application basis. As the blend of the MAC & DAC models and integrity, RBAC is partially founded on principles showcased by Biba's .

RBAC dynamically assigns the roles to the users based on criteria defined by the manager or system administrator. Role-Based Access Control models are a set of fairly new models [12] first introduced in the ninety's. The RBAC92 model [9] introduces the concept of roles, and RBAC96 [3] refines RBAC92 thanks to the addition of the users notion (different from the subjects one) and a roles hierarchy defined as a partial order. RBAC also stands apart from the more traditional MAC and DAC by granted rights on transactions, not on underlying subjects. These rights are granted to roles, which at first glance appear to be a synonym for DAC groups. The difference lies in that groups consist of a collection of users while roles are a bridge between a collection of users and a collection of the Clark-Wilson model of transaction rights. While RBAC supports data abstraction through transactions, it cannot be used to ensure permissions on sequences of operations need to be controlled .To do this, a less general and more sophisticated access control model must be used.

III. RELATED LITERATURE REVIEW:

Since 1970's several models and comparisons have been proposed for Role Based Access Control Model (RBAC) and implemented to redefine and filter the access control models to ensure the security from the vulnerable and intrusion attacks. In "Assessment of access control systems "[1], V.C. Hu et al. had proposed all mechanisms & access control designs which intends to choose optimal solution. They also implemented the complex issues of security were, to achieve the target. They gave privileges to the user to decide that what is best for them. Although, with the combination of the fast response from materialized view and user access control is a great advantage proposed by R. Bhatti et al. [2] and in his research work "Enabling policy-based access control in BI applications", he provided a middleware enabled policy based architecture that applies the policy of access control to both the base tables and materialized views.

In [3] "Role based access control models" by R.S. Sandhu et al. he implemented an access control system which provided the user groups as the access control unit. Also various family of models were defined consisting four basic concepts including model relationships and essential characteristics. Users, Roles, Permissions and the Constraints had been redefined by describing their permissions and applied on the objects which are single or more. Users own read access to a particular file or generic read access to all files belonging to a particular department. After generating session, the user may activate a subset of the roles belonging to particular session which describes one user to possibly many roles.

In the research methodology i.e. "Design of Algorithm for Environment Based Dynamic Access Control Model for Database Systems " proposed by S. Ahmad and R. Ahmad [4] describing a detailed access control architecture with presentation of Environmental Based Dynamic Access Control Model (EBDACM). Also they implemented the dynamic environment check methodology and redefined the assignment of permissions
to a user of database. In the papers [2] [3] [4] , we have a common type of system in which policy based access control permissions are assigned to a user available in database with the privileges enabled.

A.E. Sayed et al. [5] had put forward the model "DW Access control model" in which the database is given more preference as compared to the user roles. Also data warehouse was assembled and combined the critical data of organization through every available sources and stores them for a long time. The author also implemented enhanced authorization in reference to the permissions discussed in the model [3] to close open security holes in the data warehouse and on-line analytical process by adding flexibility in security roles. They had also enhanced the basic OLAP security norms model to control access rights of the mixture of linked facts and dimensions by assembling much flexible predicates. The author also gave a new idea to avoid missing user's accessibility on the permeable objects.

"Access control: Policies ,Models and Mechanisms" [6] by P. Samarati et al. in which they had implemented the RBAC model which is alternative to the traditional discretionary (DAC) and mandatory access control (MAC) policies, particularly for commercial applications. They also described that it is more important to know what a user's organizational responsibilities are, rather than who the user is. The RBAC policies revised the user's access to the information on behalf of the organizational activities and responsibility that users have in a system. Although, common approaches have been made by [3,7,9,11] in which some of the methods introduced delivers the same concepts . P. Samarati et al. had pointed out the security requirements that may be needed to be taken into consideration.

V.S. Subrahmanian et al., in his paper "A logical Language for Expressing Authorizations" [8], he enforced an extended single access control policy which was able to support various access control policies defined earlier. Also a logical language was used with different approaches to conflict resolutions i.e. a positive and a negative authorization for the same access, for the specification of authorizations over which the described model

can be based. The logical language allows users to specify, together with the authorizations and policies resembling to which access control decisions are to be made. The major advantage of their approach was that it could be used to specify different access control policies that can all coexist in the same system and can be enforced by the same security server.

A Chinese wall security policy was introduced by T.H. Tsai et al. in their paper [10] "A practical Chinese wall security model in cloud computing" which forbid to deploy and run the participators VMs on the same physical drive to achieve the isolation. They also introduced Chinese Wall Central Management System (CWCMS) which is a mechanism in an internal-built cloud and it can manage the VMs and enforce the Chinese wall security policy in the cloud.

The paper [12] " A formal comparison of the Bell &LaPadula and RBAC models" by L. Habib et al. addresses the problem of comparing access control models mainly Bell and LaPadula (BLP) and the Role-Based access control model (RBAC). Authors also described the comparisons required for the models which share the same set of requests provided and it was desirable to relax this constraint. Their work was the first step to consider the notion and the idea of weak simulation of implementation when declaring a preorder over access control models.

H.C. Li et al experimentally proved in their research work,"Deriving and using Data Access Control Information to determine whether to permit derivations of Data Elements"[13] a system for deriving data access control information to recognize whether to permit requested derivation of data elements. Data access control information is initialized for each of a plurality of data elements and it comprises of user access list indicating at least one data element that subjected to a derivation operation with the associated data element. Also the request is received from one user to generalize the first data element and the second data element to a derivation process. Overall, the processed data access control information allows the user to perform the requested operations of the data elements and described that the users which were not included in the user access list are capable of individually accessing the data elements and the data access control information prevented user's not indicated in the user access list.

IV. METHODOLOGY PROPOSED:

The incarnation of the methodology relate to the field of the token database management and more preferably, to the role based access control utilizing the role privileges and token profiles generated. Since the users connected with the network have to login the various services which are available on the network. The single sign on is a configuration which allows the managers/admin to generate a unique password system so that the users can log in once using that unique password and can be authenticated against all network resources and workstations.

One of the obstruction to establish a secure network configuration, is to make sure that whether the user access is free from the network and system attacks or vulnerable to the various attacks. However, the method introduces an improved technique to overcome these attacks using a Session and Token management module. Now a days, Digital signatures are used widely in the field of e-networking. Administrator have the full access to all the fields which are functioning on the database. Thus, the token security system (TSS) involves all the aspects which can restrict the security attacks and the vulnerabilities which results to provide a better configuration system to the user.

Our proposed Model consists of Six main modules which are as follows:

1. User
2. Administrator
3. User Profile Manager
4. Token Management
5. Session Management
6. Database

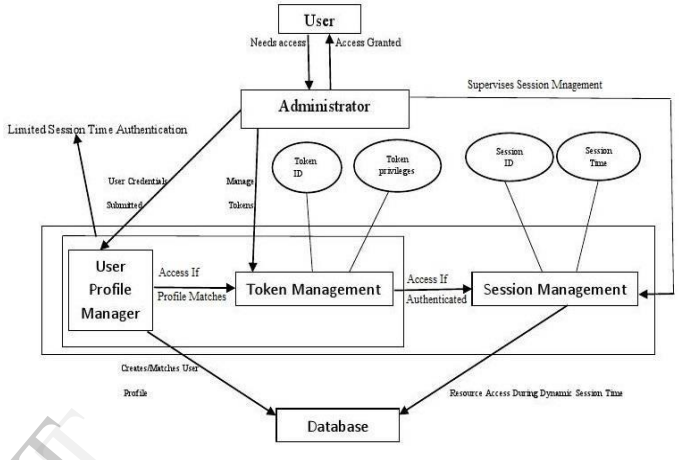

Fig 1. RBAC using Token management and session management

In our proposed model above, starting from the **User Module**, the user will request for the access to the **Administrator** module Fig [1]. But before providing the access to the user, the administrator will make the user go through the authentication process. Further, the administrator will allow internal permission to the **User Profile Manager** module to match the user role credentials from the given database. If the user role matches, then the user will be allowed to move on to the next module i.e. Token Management module. But,however if the user role doesn't get matched or the user doesn't want to enter the credentials, then there will have choice for the user to create their profile and to redirect themselves to initial module. Now if the new user wants to access the system then the user can create profile using User Profile Manager module. After the user profile is created, the access will be redirected to the User Profile Manager module to pre-authenticate the user according to the credentials provided by him. The user can now select the object privileges for accessing the resources of database. A Static Session time module will be generated for the final authentication process for the user while moving on to the process of retrieving Token as per **Token Management System (TMS)** module**.** If in the given session time, the user authenticates himself according to the applied privileges, then the user will be directed to the **Session Management Module**, otherwise the process will be redirected to the initial point. Being linked to the Session Management module the user will be redirected to access the resources from the **Database** but the type of access will depend on the objects privileges.

Working of Token management system and Session management together:

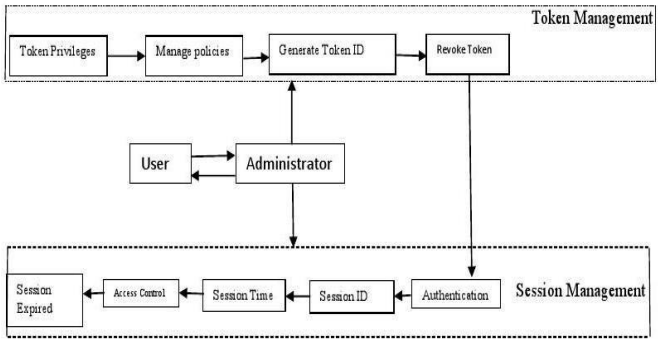

Fig.2 Working of Token and Session Management modules

In medieval time of the process the internal modules of Token and Session Management modules will be invoked. The pioneer need to reach this operation by the user to authenticate in the applied static session time shown in fig [1]. If the previous modules are completed by the user then next operation will be invoked. In the **Token management system (TMS)** module, the user data will be searched and verified according to his privileges, will it be Objects privilege or System's privilege depending on authentication User type. According to the user privilege the Token policies will be generated. Now the process will prepare a **Dynamic Token ID** for the user. After the Token ID is prepared, User will **Invoke Token** and user will provide the invoked Token ID to the session manager. If the invoked Token ID is granted the permission for the session then the process of **Authentication** will be completed and the session manager will revoke Token. In **Revoke Token module**, The Session manager will destroy the dynamic Token Id so that it can't be used in the future for the intrusion attacks)**.** For the generated session operation, the session manager will prepare a Dynamic **Session ID** for the operating user with the generation of the bounded Static/Limited **Session Time.** For access to the resources in the database, The user will provide the generated Session id to the resource access manager (i.e. Session Manager) to view the resources according to the user's object privileges. When the Static Session time expires with the **Session Finalization** then the user will be redirected to the initial module and appropriate actions will be monitored by the **Token Security**

System (TSS).

V. CONCLUSION& FUTURE WORK:

Different methods are proposed in this paper to provide maximum security to an organization for the Role based access control system against the threats andintrusion attacks. With the implementation of this security model based on RBAC, an organization can restrict the attackers to bypass the security. Our proposed model of the RBAC system with compatibility of Token security system module and Session Management module, maintaining the policies and privileges, makes the model hard to bypass. Since, the model operates on the dynamic arrangements of ID's (Token ID'S and Session ID's) in the static session time for the user, therefore it will be difficult for attackers to retrieve the dynamic ID's for intrusion attacks. Thus, this approach will provide a greater and strongest Role Based Access Control Model to an organization to implement which include the compatibility of Token Security System (TSS) and Session management system. The future work includes the implementation of a Role Based Access Control algorithm to provide safer & secure userconfigurational system.

VI. REFERENCES:

[1] V.C. Hu, D.F. Ferraiolo, D.R. Kuhn, "Assessment of access control systems ",NIST Report 7316,September 2006

[2] R. Bhatti, D.Gao , W.S. li, "Enabling policy-based access control in BI applications ",Data and knowledge Engineering ,2008

[3] R.S. Sandhu ,E.J. Coyne ,H.L. Feinstein ,C.E. Youman ," Role Based access control models ",IEEE Computer , Volume 29 Issue-2,1996

[4] S. Ahmad and R. Ahmad' " Design of Algorithm for Environment Based Dynamic Access Control Model For Database Systems ", International Journals of Computer Applications(IJCA)(0975-8887), Volume 21 No-10, May 2011

[5] A.E. Sayed , A.E. Bastawissy, I.E. Imam, "DW Access control model ", International journals of computer science and Network Security ,Volume 10 No-10, October 2010

[6] P. Samarati and S.D.C. Vimercati ," Access control:Policies ,Models and Mechanisms",Page 41-45,2001

[7] G. Ahn and R. Sandhu ," The RSL99 Language for Role Based Separation Of Duty Constraints ",Pages 43-54,Fairfax , VA, USA, October 1999

[8] S.Jajodia , P. Samarati and V.S. Subrahmanian ,"A logical Language for Expressing Authorizations",1997

[9] D. Ferraiolo and R. Kuhn ," Role Based Access Control ", In Proc of 15th NIST- National computer security conference , Pages 554-563,Baltimore, October 1992

[10] D.F.C. Brewer and M.J. Nash," The Chinese Wall Security Policy"' In Proc. Symp. On Security and Privacy , Page 215-228, 1989

[11] S. Osborn , R.Sandhu and Q. Munawer," Configuring Role Based Access Control to Enforce Mandatory and Discretionary Control Policies", ACM Transactions on Information and System security , 3(2): 85-106,2000

[12] L. Habib , M. Jaume and C. Morisset , " A formal comparison of the Bell &LaPadula and RBAC models",HTTS Funded by the Macao Science and Tech. Development Fund,2008

[13] G. Ahn and R. sanhdu ,"Role-based authorization constraints specification". ACMTrans. Inf.Syst. Sec. 3, 4 (Nov.), 2000

[14] J. joshi , A. Ghafoor , W.G. Arefand E.H. Spafford,"Digital government security infrastructure design challenges". IEEE Comput. 33, 2, Feb. 66–72,2001

[15] D.R. Kuhn, Role based access control on MLS systems without kernel changes. In Proceedings of the ACM Workshop on Role Based Access Control (Oct. 22–23), 25–32,1998

[16] A. Stoughton, " Access flow: A protection model which integrates access control and information Flow". Proc. of the IEEE Symposium on Security and Privacy, pages 9–18, Oakland,CA, 1981.