ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Secure Interoperation Model for Different User Authentication System using Multi Level Security (MLS)

Muthukumaran T

B.E, M.Tech – Assistant Professor, Department of CSE, Dr. Navalar Nedunchezhiyan College of Engineering, Tholudur, Cuddalore(DT), Tamil Nadu, India.

Abstract: Service Oriented Architecture (SOA) is more important concept for secure sharing of information or services accessing among distributed environments. It comes from the idea of Object Oriented Architecture and it also adopted with web service technologies. Sharing the services among two or more different distributed domains or within their subdomains, there is a need for secure interoperation among those systems when they access, sending, and retrieving data services. This is most important and challenging issue nowadays in every distributed environment. For example, consider three different university domains having different characteristics and policies sharing their resources among them in a distributed environment. Integration among the domains varies based on the trust relationship among them by specifying the access rights. Some domain may give full access rights to their trusted domains based on the trust relationship and some may give partial access. The issue here is user may have the chance to access the data from un-trusted domain through their trusted domains. The idea behind the paper is to protect and enhance the secure way of communication among the domains by introducing the Multi Level Security (MLS) Method and Two Server Password Authentication for high assurance security. The Token key and Two Server Password Authentication Key Exchange Manager which prevents the untrusted users access the services through their trusted domain. The proposed architecture also improves the security of the interoperation using trusted web server. It assured by path authentication and authorization which also can reject the un-trusted users from security misuse.

Keywords: service oriented architecture (SOA), web service technology, secure interoperation, multi level security (MLS), Identity Management.

I. INTRODUCTION

Service Oriented Architecture (SOA) plays many important roles for resource sharing and operating interconnected data in heterogeneous distributed environments. Service Oriented Architecture can use the web technology features. It is adopted with web service technology [11]. Establishing interoperability is the first and most important problem of secure interoperation in multi-domain environments. Interoperability means that more number of systems communicate, and share as well as exchange the resources by checking with their identities and policies, and at the same time both systems need to have some common conditions to provide a reliable connection with no faults or confusions. More and more research persons have works to solve different interoperability issues for particular domains such as resource management, enterprise system, business enterprise and healthcare sector. Different development styles may collapse or disturb the communication. In SOA systems, service consumers and providers need to exchange data in a flexible and consistent way. Overall concept of Service oriented architecture technology can be used.

A. Secure Interoperation

Secure interoperation of sharing resources between the systems is most challenging issue. Trust is essential for networking communication and interoperation among system. Some of the key components of identity management [1] are identity provider, service provider mainly used for interoperation of two systems. Identity provider can take charge of establishing trust connection between user and service provider. In a system everyone can trust each other and link with other system by trust relationship. So user of one system can access the other system services. Therefore based on the trust relationship others can also access the system through their trusted systems. There different security levels can implemented in different system. However, the trust relationship needs to be designed carefully.

II. RELATED WORK

There are a lot of international standard organizations working on interoperation between different heterogeneous systems. Jianyong Chen, Guihua Wu, Zhen Ji[1] made an interoperation framework for secure sharing using Authentication assurance level and they clarified about AAL method. For authenticate the user instead of role based access control, they used authentication assurance level. In hierarchy structure of RBAC model, they find out the problem called security violation during the inheritance process. Figure.1 shows security violation, that role of A1 in domain A should not possess the role of A3 privilege. But rA1 in domain A inherits rB3 in domain B and rB1 in domain B inherits rC2 in domain C and rC1

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

in domain C inherits rA3 in domain A. It means that rA1 will have the rA3 privilege and there the security violation can occurs.

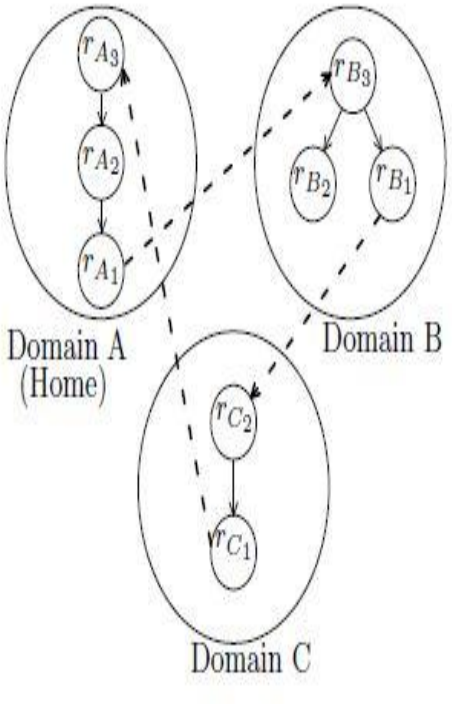

Fig. 1. Security violation in RBAC

In some other cases they used cross domain authorization where the duties of rB2 and rB1 are independent. But the violation of separation of duty (SoD) [1] happens. So the external users access a local domain, it should obey two principles are shown [1]: **Autonomy:** any access permissions authorized within domain must also be permitted, **Restriction:** any access permissions not authorized within domain must also be refused. The trust path can be established by using interoperation path and path discovery algorithm, and we find out the importance of trust relationship. so this method can be used in our proposed framework. Yet, the sharing of services in multi distributed environments has become the major issue. Carles Martinez-Garcia, Guillermo Navarro-Arribas, Simon N. Foley, Vicenc Torra, Joan Borrell [2] proposed a framework for inter domain mapping designed for heterogeneous polices. In multi domain environment the major challenge is to be access control between domains. For access control permission interoperability can be used. There are two level of interoperability [2] 1. Policy level 2. Attribute level

In policy level interoperation, adding up a new domain requires the modification of the interoperation access control policies. Usually it is too complex to be arranged in open environments or specific architectures. In attribute level, If foreign domain enters in local domain means that, foreign domain local attribute translate to global attribute later it translated to the target domain's local attribute. So it is easy to interoperate with their access policies by using attribute level conversion method. A Fuzzy based conversion mechanism [2] used to describe the conversions. Here to define the isomorphic relation between attributes are the major issue due to the heterogeneity of the domains. Lei Lei Win, Tony Thomas, Sabu Emmanuel[3] describes how importance of digital content sharing information in multi domain environment. [3] Digital Rights Management (DRM) technology has been implemented by digital content providers, distributors, and device manufacturers in order to prevent illegal content distribution. They maintain the trust assumption between the entities and this assumption may not promise the content of multimedia transformed in a secure way. So they proposed a distributed mechanism for commercial and user generated contents [3]. The general Registration server is maintained for registering all entities and each user needs to register only to the Registration server and join the Local Domain Manager [3]. Content leakage is the major problem of sharing between distributed domains. Hejiao Huang, Helene Kirchner [4] clearly mentioned the access control policies, which integrated that allow users of one company to interact with other domains. The main challenge of policy integration is detecting the conflicts. They use the designing model called colored Petri nets for identifying and verifying a secure interoperation design [4]. This model is helpful in our proposed model for verifying policy integration and yet it is major challenging issue because of frequent changes in dynamic environment. Umit Kocabicak, Deniz Dural [5] proposed a framework for interoperating multiple e-learning platforms with single sign on using single mediator service. Using this model user can access different e-learning systems with single user and password entry. Security can be provided by using web service technologies. Alberto Polzonetti, Francesco De Angelis, and Barbara Re [6] work towards e-Government. It should interconnected with different public administrations using interoperability architectures. They proposed a distributed interoperability architecture, in which multiple models are developed so that each model can help the interoperation process. In e-Government they share the intelligent documents that should be more secure while interoperation. So they proposed ontology-based methodology architecture for the delivery of intelligent documents within public administrations. As a result of this method may be verified in our proposed environments. A current report on secure interoperation is mainly focus on interoperation between two different heterogeneous systems. In this case, every user in their system can make trust relationship with other system for secure sharing of resources. So it is possible of fraudulent users can make changes through their system trusted system. So it is always necessary to develop a general framework for secure interoperation of sharing resources.

III. EXISTING SYSTEM & ITS ISSUES

There was a problem while using inheritance of user from other systems. It mainly uses role inheritance path from home domain to visited domain. The problem occurs in hierarchy structure of RBAC model, there are some security misuses. This will occurred based on the trust

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

relationship between both systems, so users and others are in Circle of Trust have trust based link for communication of information. Security misuse can also occur in separation of duty (SOD) [1] of users. The violation of separation of duty happens by using cross domain authorization. Using Authentication assurance level, the degree of authentication method which also reflect the degree of confidence for identity that the user declared. The authentication based on set of authentication items and authentication levels, if the users involved in that domain have to be register in the central identity managements. If there are frequent changes to the registers of administrator, the group administrator must make frequent updates to those who are in the system, and security misuse can be occurred. So this is demerits of existing system. To avoid this problem, the Multi Level Security method can be used.

IV. PROPOSED SYSTEM

A. *Objective*

There is a need for secure interoperation while accessing, sharing, and retrieving the data services among two or more different distributed domains or within their sub domains. This is most essential and challenging issue these days in every distributed environment. To protect and enhance the secure way of communication among the domains by introducing the Multi Level Security (MLS) Method and Two Server Password Authentication Key Method. The Token key and two server password authentication key exchange Manager which prevents the services accessed through their trusted domain. The proposed architecture also improves the security of the interoperation.

B. *System Architecture*

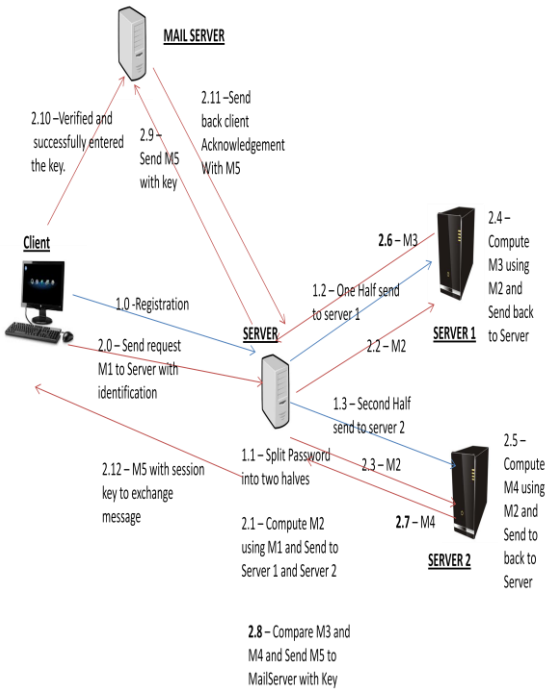

Fig. 2. *System Architecture*

It is simple architecture of our proposed system. Generally in a multi distributed domain environment may have many users who have a trust relationship with that domain or their sub domains for sharing services. There is always need secure interoperation among those different domains when they sharing of services. So here this University Domain system will provide the services like Internet of things, Wi-Fi access, e-Learning, Digital Libraries, and etc., to the trusted college domains and within the trusted domain users. One of the college domain and university domain may be maintain trust relationship with another college domain for accessing and sharing of services.

C. *Domain Model*

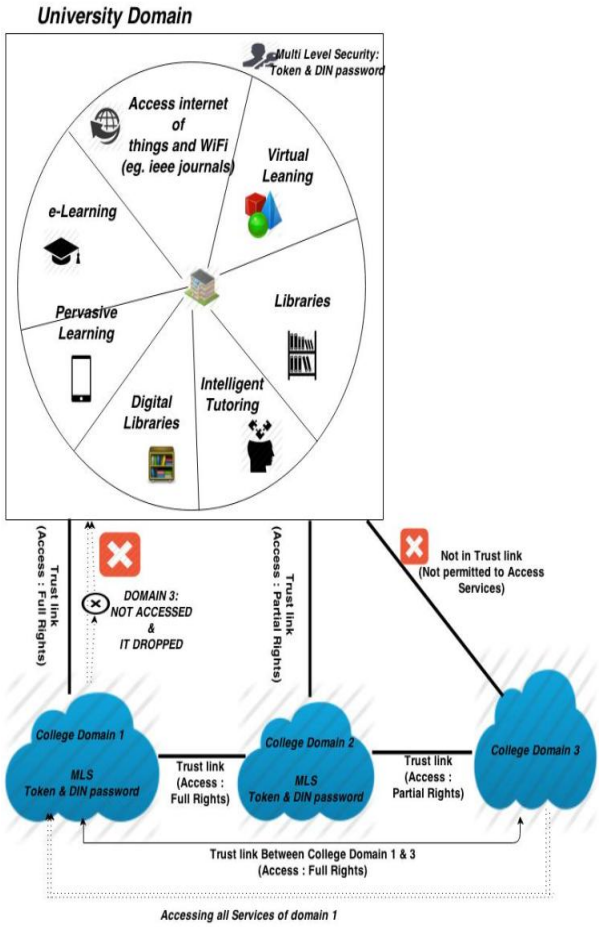

Fig. 3. *Domain Model*

The Identity Providers will identify the user identities with their policies and Service Provider will provide the services to the trusted users. Identity provider of the system as well as their users can become a Circle of Trust. Some of users may also relationship with some other systems. So they belong to another Circle of Trust. Therefore two different system of their Circle of Trust of users can have trust relationship. Based on their trust relationship both systems can share the resources independently. There are group of users, identity provider and service provider in the Circle of Trust. So based on the trust relationship, the users in Circle of Trust of another college domain can also access, retrieve, download and

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

sharing of their services from the system. Therefore users in other college domain can use to access all the services through their trusted college domains. There security can be violated [1]. So that should be prevented by Multi Level Security Method (MLSM) of tokens and passwords. By using multi level security, the Domain Identity Number (DIN) passwords can be assigned for the users those who are in the particular Circle of Trust of the domain and Tokens to be assigned for the particular college domain/system along with their trusted domain. So the other college domain users can enter the system by putting their username and password along with their Token key password for accessing and sharing services. So here the security misuse of one particular domain services may use by some other untrusted users.

Two Server Password Authentication Key Method, the user first register, then the password can stored in two servers. While registration, the main server will split the password into two halfs and one half is send to server1 and stored. And another one half is send to server2 and stored. After this client can send the request M1 to server with identification. Then main server will compute M2 using M1 and send M2 to both the server1 and server2. Then server1 will receive the M2 and compute the M3 then it send M3 to the server. Meanwhile server2 will receive M2 and compute the M4 then it send bace to M4 to the Server. After this the main server receives the M3 and M4 from server1 and server2 respectively. And it will computer the M5 using M3, M4, and the server will send M5 with session key to the Mail Server. Client will access the mail server and verified the key and enter the key successfully, then send an acknowldegement. Finally the MailServer will send client acknowledgement with M5 to the main server. After all this process, the main server will send M5 with session key to the client for exchange the message. So the other domain users can enter the system by putting their trust relationship of user's username and password for accessing and sharing services. If one server is compromised due to hacking or even insider attack, passwords stored in the server are all disclosed. The Tokens can change automatically for every minute and linked with trusted university domain and college domain. Therefore the untrusted college domain users won't access the services of University Domain. It dropped the request access from the unauthorized users from a particular college domain by using trusted web server. The different system may assign for different types of authentication for user authentication. So users from other Domain Circle of Trust not allowed to accessing the services because of tokens password mismatch and two server password authentication key exchange method. Therefore the University Domain can be more secure from fraudulent users.

D. Explanation

Secure Interoperation is more important in these days while sharing of resources among two or more different distributed domain or within their sub domains. The both system need interoperation when they want to access or share services. So consider three different university domains having different characteristics and policies sharing their resources among them in a distributed environment. Here the university domain and college domain can build trust relationship with some other college domains. Integration between the domains varies based on the trust relationship among them by identifying the access rights. Some domain may give full access rights to their trusted domains based on the trust relationship and some may give partial access. Many users from college domain/system can make trust relationship for sharing of resources. This will create a chance for fraudulent users to access the university domain services through their trusted college domain. This prevented and enhanced the secure way of sharing their services by using Multi Level Security method for high assurance security. It involves tokens key and two server authentication passwords which can be prevents the services accessed through their trusted domains. It is linked with trusted web server. In trusted web server check if the user wants to access the services means, first the request send to the trusted web server. It will check the user authentication and authorization information for involving and accessing the system. It also verified token key and passwords from token key and password manager. If the process has been done, it permits the users.

E. Feature Of Proposed System

To avoid the security misuse from fraud users, the proposed architecture can make secure sharing of resources/services between different interoperating domains. So the only trusted college domain users can use the services of university domain. Other fraudulent users from some other college domain system can block by trusted web server.

V. CONCLUSION

Secure interoperation is more important in distributed multi environments. It has become a challenge for users those who are experience on the internet. A Architecture is proposed to improve the facility of interoperation among different University Domain System. Interoperation can be done by using Multi Level Security. It enhances and provides the secure way of communication among domain of users, and also in order to prevent the security abuse at the time of sharing resources. In future, this architecture can be implementing for large scale industry and some other related systems like business to business environment and public administration. This architecture can be extensible for large distributed environment.

REFERENCES

[1]. Jianyong Chen, Guihua Wu, Zhen Ji., "Secure interoperation of identity managements among different circles of trust", Computer Standards & Interfaces 33(2011) 533-540, Springer, 2011.

[2]. Carles Martinez-Garcia, Guillermo Navarro-Arribas, Simon N. Foley, Vicenc Torra, Joan Borrell, "Flexible secure inter-domain interoperability through attribute conversion", Information Sciences 181(2011) 3491-3507, Springer,2011.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

[3]. Lei Lei Win, Tony Thomas, Sabu Emmanuel, "Secure interoperable digital content distribution mechanisms in a multi-domain architecture", Multimed Tools Appl(2012) 60;97-128, Springer,2012.
[4]. Hejiao Huang, Helene Kirchner, "Secure interoperation design in multi-domains environments based on colored Petri nets",Information Sciences 221(2013) 591-606, Springer,2013.
[5]. Umit Kocabicak, Deniz Dural,"Secure and interoperable e-learning platforms based on web services", Procedia-Social and Behavioral Sciences 55(2012) 1265-1271, Springer,2012.
[6]. Alberto Polzonetti, Francesco De Angelis, and Barbara Re,"Interoperability in Cooperative Environments for Public Administration: Metadata and Intelligent Document Issues and Applications", International Journal of e-Education, e-Business, e-Management and e-Learning, Vol. 1, No. 1, April 2011.
[7]. P. Pacyna, A. Rutkowski, A. Sarma, K. Takahashi, "Trusted identity for all: toward interoperable trusted identity management systems", Computer 42 (5) (2009) 30–32.
[8] J. Crampton, "On Permissions, inheritance and role hierarchies", Proc. 10th ACM Conf. Computer and Comm. Security (CCS '03), Oct. 2003, pp. 85–92.
[9] L. Gong, X. Qian,, "Computational issues in secure interoperation", IEEE Transactions Software Engineering 22 (1) (1996) 43–52.
[10]. Wu F, Mahajan V, Balasubramanian S., "An analysis of e-business adoption and its impact on business performance" Academy of Marketing Science, 2003, 31(4): 425-447.
[11]. S. Cantor, J. Kemp, R. Philpott, and E. Maler (Eds.), "Security assertion markup language v2.0", OASIS Security Services Technical Committee Standard, 2005.

BIOGRAPHY

Mr.T.Muthukumaran. Assistant Professor, Department of Computer Science and Engineering in Dr.Navalar Nedunchezhiyan College of Engineering. He holds M.Tech in Computer Science and Engineering from Sri Manakula Vinayagar Engineering College, Puducherry, India. His areas of Interest are Service Oriented Architecture, Computer Networks, and Network Security. He has many International Journal Publications.