ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Fuzzy based multilevel security access control mechanism for pervasive computing application: Smart Library Management

A.M.Hema[#1], K.Kuppusamy[*2]

 # 1 Department of Computer Science & Engineering, Alagappa University, Karaikudi, Tamil Nadu, India

**2Department of Computer Science & Engineering, Alagappa University, Karaikudi, Tamil Nadu, India..*

[1]jehemaeinkaran@gmail.com
[2]kkdiksamy@yahoo.com

Abstract - In Pervasive computing application, security is prime factor. Because, the application is not limited to desktop but extends to any smart device in distributed and ubiquitous environment. In such situation, it is necessary to have very secured access control policies to access the resources in smart environment. In our proposed system, access control policies are framed on the basis of context and location attribute. This paper proposes context based access control scheme for smart library management using fuzzy rules, to effectively access the resources by an authorized users. It presents the new concept of security of fuzzy controlled system. The application instance shows that the proposed context based fuzzy access control schemes for pervasive computing is effective.

Keywords: Pervasive computing, context, fuzzy logic and fuzzy controlled system.

I. INTRODUCTION

In pervasive applications the surrounding ambience becomes smarter, our actions and existent become noticed and measured by digital devices and sensors which provide computer applications with information about the user, that create new concerns that should be taken into account, one of the major concerns is security where users resources in such environment is vulnerable for unauthorized access.

Access control is a fundamental security technique in systems in which multiple users access the common resources that are exists in smart environment to achieve desire level of security. Authorization is the process of expressing security policies that determine whether a subject, refers to an entity such as a process, device, user or any resources that are connected with the system which the requester like to access . Valid user is allowed to perform an operation like read, write, execute, delete, search, print, and scan etc., on an object. These policies define the subject's permissions to perform an operation on an object. Managing and administering the users' privileges is one of the most challenging tasks in access control. Several access control models have been proposed, such as, discretionary and mandatory access control models (DAC and MAC), Clark-Wilson model, Lipner's Integrity model, Chinese wall model, Task based models, and Role Based Access Control models and RBAC has further been extended up to some level. Among these models Role-based access control (RBAC) models have been receiving attention as they provide systematic access control security through a

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

proven and increasingly predominant technology for any application in pervasive computing environment. RBAC models are policy neutral [5]; they can support different authorization policies including mandatory and discretionary through the appropriate role configuration. In spite of the success of the RBAC, researchers have determined that there are still many application security requirements that are not addressed by the existing RBAC models [5]. In the past few years, several RBAC extensions have been proposed to address such security requirements [1,2, 3, 4,5,6,8,9].

Roles (R) are representation of subjects' responsibilities, and is assigned to them when they become part of the system. In our case, subject role may be a student or a faculty member of an institution. When a student joining in an institution, being assigned the roles of UG / PG / M.Phil. / Research scholar. For faculty members the role may be course teacher / Head of the Department/ Administrative officer/Principal/Dean/Controller of Examinations/Functional Head. Even though a subject can have many roles, they can be activated only one at a time. The proposed model switches between the active and dynamically updated roles. To determine the actions performed by the subject we look into role table and map the role in the permission table. Privileges (PR) are authorizations which allow subjects to execute appropriate actions on selected objects within the system. For example, for III UG student , active role is 'III' , suppose he likes to access content for II or I year ,active role has been updated according to their request and looking for the privileges for further processing.

In the infrastructure of existing services, access rights to a resource are granted only after the execution of a user authorization phase by verifying their username and password. Second step verification done by entering 'date of birth' of the user in their own format. To collect the context information sensors are deployed accordingly appropriate services are provided for them.

II RELATED WORKS

Researchers use context awareness and location awareness in their suggestions for new applications paradigm, access control mechanisms is one of disciplines affected by this new paradigm, efforts made in improving access control mechanisms to be enriched with context aware and location parameter, using our research perspective.

The first attempt to utilize RBAC in contextual manner done by M. Covington [7] provides a model to create and access information from a smart home environment based on environmental role set in addition to their standard roles. Han [10] introduced a formal model for context sensitive access control, where Reference Monitor responsible for making decision. Software components of our smart library management are user profile, user preferences, user handler and service provider. For example, a mobile user enter into the smart zone, his information's are retrieved from the server, verify its identity by second step verification, allowed to access the resources based on their request process

The Fuzzy rules:

Credentials: Username and password, identity, active role, role activation, privileges, location, time-stamp, number of positive responses, device type, requested resource and network access point.

Rule 1: The credentials are checked one by one. If username, password, identity, role, location, device type, requested resource are available then increase the positive response count by one. Identify the network access point and its distance from the user node.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Rule 2: Number of readers accommodated inside the reading room is limited to 50. That value is captured through sensor.

Rule 3: Time-stamp to access the data from the server for students is: i) Aided stream: 1.30pm – 5.30pm

Self-finance Stream: 9.00am-1.00pm

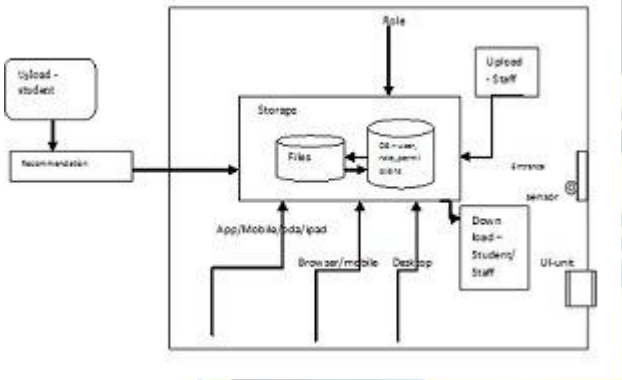

Fig - 1

In our proposed model the valid users are allowed to access the resources available in the smart library building. We assumed that the resources like server, printer, scanner and accessories are connected to the WIFI access point. Valid user identity has been verified by entering the secrete data in the dialog box. Identity of the valid user is verified by their date of birth in their own date format. If the user send wrong entry , count value is updated as negative response. If the value of negative response is equal or greater than '3' then automatically the request has been blocked and denial of service message will be send to the user , who has sent the request. In future if he wants to access the smart environment resources, he will send an request to the admin . Admin will the information to the respective department Head. If the Head will send an recommendation to process the request from the user who have been in the access denied status.

Rule4: Valid user will receive OTP to connect with the library server for the session.

These rules are incorporated to access the resources in the smart library building.

Framework model for our proposed system is listed in fig 1.

Formula to access the resource in smart environment is:

$$\text{Access factor} = \begin{cases} 1(\max)\ (cre>0.9 \text{ and } pr > 5) \\ 0.7\ (0.9< cre >.7 \text{ and } 5 < =pr>2) \\ 0.5\ (0.7 < cre >= .5) \text{ and } pr <= 2) \\ 0.3(\min)\ (cre < 0.5 \text{ and } pr <2 \text{ and } (nr \text{ is set}) \end{cases}$$

Where cre – credentials

Pr – positive response to access the resource.

Nr – negative response for the requested resource.

IV. CONCLUSION

In this paper , we discuss the possibility of implementing the fuzzy rule based access control mechanism for a pervasive appication. The security measures taken into account are i) identity of the source ii) device type , ii) Location , iii) response level v) time-span , for calculating the access factor

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

to access the resource in the samrt library environment.We also set the space to accommodate the valid user inside the reading room is upto 50.In future we can include the domain categorization with respect to the level of security for the services, we can extend our model to upload and download limits for the user and to avoid malicious user or anonymous user.

V. REFERENCES

[1] K. Devdatta and T. Anand, "Context-aware role-based access control in pervasive computing systems," In Proceedings of the 13th ACM Symposium on Access Control Models and Technologies, Estes Park, CO, 2008

[2] Z. Xinwen, O. Sejong, and S. Ravi, "PBDM: a exible delegation model in RBAC," In Proceedings of the 8th ACM Symposium on Access Control Models and Technologies, Como, Italy, 2003.

[3] S. Chakraborty and I. Ray, "TrustBAC: integrating trust relationships into the RBAC model for access control in open systems," In Proceedings of the 11th ACM Symposium on Access Control Models and Technologies. Lake Tahoe, CA, 2006.

[4] R. Sandhu. "Role hierarchies and constraints for latice-based access controls." In E. Bertino, H. Kurth, G. Martella, and E Monotolivo Eds. LNCS 1146, Proceedings of the European Symposium on Research in Computer Security 1996, Rome, Italy.

[5] E. Bertino, P. A. Bonati, and E. Ferrari,"TRBAC: A temporal role-based access control model," ACM Transactions on Information and System Security, 4(3):191-233, 2001.

[6] H. Shen and F. Hong, "A context-aware role-based access control model for web services," In Proceedings of the IEEE International Conference on e-Business Engineering, Beijing, China 2005.

[7] M. Covington M. Moyer, and M. Ahamad. "Generalized role-based access control for securing future applications" [Journal]. - 2000

[8] I. Ray and M. Toahchoodee, "A spatio temporal role based access control model," In Proceedings of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Redondo Beach, CA, 2007.

[9] M. Toahchoodee and I. Ray, "On the formal analysis of a spatio-temporal role-based access control model," In Proceedings of the 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, London, U.K., 2008.

[10] J. Hwan Choi Hyunsu Jang and Young Ik Eom. "CARBAC: Context Aware RBAC Scheme in Ubiquitos Computing Environments" [Journal]. - 2010.