Adaptive Context Aware Role Based Access Control Model For Pervasive Earning Environment

A.M.Hema, K.Kuppusamy,
[1]Dept. of Computer Science, Thiagarajar College, Madurai
[2]Dept. of Computational Logistics, Alagappa University,Karaikudi

Abstract- With the rapid change in learning environment, there is the possibility for the user to access the learning resources from anywhere, at any time through any device. Thus pervasiveness and mobility of devices made the access control, adaptive in nature. Therefore, dynamically changing context does not have complete leverage on access control for the resources requested by the user. We propose an access control model that adapted by gathering the dynamically changing contextual information, other related data that has an impact on access decisions between the trusted entities/devices. As a result, access control model designed, based on the user behavior, environmental parameters and trust of the entities which are participating in accessing the resources at an instance in pervasive manner. The requested service allowed or denied through the adapted access policies. Results and performance analysis are presented for the proposed context aware role based access control model.
Keywords: Pervasive computing, access control, trust, context-aware, security.

I. INTRODUCTION:

The growth in the information and communication technology connects us by smart e-gadgets to activate our day to day activities in pervasive manner. Because of the impact of the ICT we need to focus on so many factors to preserve our authentication and authorization while accessing the data in smart personalized manner. In every on-line transaction context, trust and role had an authority for secure transaction. Context is defined as, the information to use the situational factors like identity, location, time, network traffic and other surrounding parameters of an entity [1,2]. In pervasive environment, the context awareness term was introduced by Schilit (1994). Context-aware devices may also try to make assumptions about the user's current situation. Three important aspects of context are: where you are; who you are with; and what resources are nearby. The Context-aware devices [4, 8] intellectually capture the circumstances under which they operate, based on rules, situations, requirements and react accordingly to their environment. Thus, pervasive computing personalized the services to the end user according to the context parameters.

In traditional system access control policies are fixed and it is based on server/client architecture. But in pervasive environment we need access decision adaptability rules. On the other hand, the security related challenges like authentication, authorization, access control, integrity, availability and confidentiality needs to meet in context aware adaptive systems. In our proposed system, we have formulated the access control decisions by considering the data like authentication and authorization for accessing the required services. Authentications verify the identity of the user/entity by passwords, special codes and phrases, biometric verification like image. Once the user identity was declared, the user assigned access rights and privileges by admin and audited by audit agent. The access control policies defines the rights as permit everything, partial permission for some services/transactions, not permitted [7]. In our model we have categorized the user type according to the change in the context parameters and trustworthiness along with their assigned roles. The change in context and user interaction behavior is analyzed while fulfilling the need of the user, if it comes from the trusted user with the adapted or assigned role.

1.1 Pervasive Learning:

The term "pervasive learning" was officially coined by Dan Pontefract in his book Flat Army: Creating a Connected and Engaged Organization (Wiley, 2013). In this book, Pontefract defined pervasive learning as "learning at the speed of need through formal, informal and social learning modalities". Learning about the right thing at the right place and time in the right way is best suitable for pervasive environment. Context-aware pervasive environments adapt the user's real situation to provide adequate information for learning. Pervasive learning creates a situation or surroundings to acquire the context information all around the user, where he/she may not be conscious of the learning developments. Developments in pervasive learning environment adds the advantages of

adaptive learning with the benefits of ever-present to provide users, freedom to access to their individual needs with allowable flexibility.

1.2 Proposed Adaptive Context-aware Role based Access Control:

Adaptive context aware pervasive environments adapts user's real situation to provide relevant information for learning based on their requirement. Learning resources were provided to the user according to their assigned roles. Suppose the user wants to access the resource which is not permitted for him, may be processed by the recommender system as temporary delegates for short period of time and the history of such access are stored in the master database for projecting the user interest in future. Hence, the user can play single or multiple roles at a time, but computing system in this state needs a better level of understanding of the situation they are and the complex relations between the various essentials. The ability of adaptability in these situations is forwarded by recommender system, admin and audit system monitor the process of the requests. Adaptive context-aware access control knowledge includes: monitoring users activity, understanding user's requirements and preferences, and using these newly gained information to facilitate access control.

The learning resources are uploaded on server machine and the resources are accessed by the user. The valid user will be permitted to access the resources which are permissible for them according to their active role(R) and trust value (t), time of request for the service/operation/resource (T) and Permissions to access the service (P). User identity is verified by their password verification and by entering the image sequence, from whom the request raised. Credentials are assigned for the user according to their correctness and approximation of the given inputs through the login page. If login page is validated for more than '3' times then credential is reset to zero and email has been sending to the user to intimate about their current status. In an existing system all these activities are monitored by the centralized system.

Once the identity of the user successfully processed, the user were assigned a set of authorization rights, privileges associated with the services or resources. The system administrator assigns the authorization by considering the system security policies. The policies define the privileges varying from the boundary condition that 1) not allow 2) partial permission and 3) full permission.

The proposed Adaptive Context-Aware Role Based Access Control (ACARBAC) adapts itself to the varying environment by developing practically centralized monitoring system that acts as a context server, which acquire and manage the context information for analyzing user requirements. The analyzed output will post the corresponding access control decisions for the trusted entities.

This paper is organized as follows: in Section 2, discuss related works in the area of context-aware models for pervasive applications, section 3 describes the proposed model, section 4 discusses the performance analysis, section 5 presents the results and section 6 concludes with future work.

II. RELATED WORKS

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. Among these models Role-based access control (RBAC) models have been receiving attention as they provide systematic access control security through a proven and increasingly predominant technology for any application in pervasive computing environment. RBAC models are policy neutral, they can support different authorization policies including mandatory and discretionary through the appropriate role configuration. In the past few years, several RBAC extensions have been proposed to address such security requirements [1, 2, 3, 4, 5, 6, 8, and 9].

An effective access control model that is aware of context modifications and change authorizations when location, date, time of access, and resources settings changed in Context- Aware Access Control Model (CAACM) [14]. Cerberus [15] included context-aware identification, authentication and access control and reasoning about context, but the process was complicated to implement. Generic context-based software architecture (Gaia) [16] was aware of physical spaces based on geographic region with limited and well-defined borders, containing physical objects, assorted networked devices, and users performing a varied of activities. This model uses the context of first-order logic and Boolean algebra, which allowed them to describe straight forwarded rules. The Kerberos authentication [17] proposed the process to enable activation or deactivation of roles assigned to a user depending on his/her context. If we consider a user, in an un-secure place like post office, bank or canteen or rest room, the access to sensitive data is not allowed, but when the user is in a work place like laboratory, department library, lecture halls/ class rooms or hostel building rooms is permitted to access the high level priority data such as learning resources. The system [17] is context aware in nature to block the accessing if the user is in unsecured context or allow access if the user is in a secure context. 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. Hwan [10] introduced a formal model for context sensitive access control, where Reference Monitor responsible for making decision. Adopting the user request to his need based choice motivated to implement an adaptive access control according to the changing context and trust value.

Context-aware access control based on ontology [18] was aware of developing the policies based on the user, device, and place for software services that are static in nature. In [19] the context-aware access control policy T consists of two parts: the context attributes set TCA = {teacher/student, class hours/out off class hours, mobile phone/personal comp.} and the operation attributes set TOP = {Read/Write/Read-write}, namely T = {TCA AND TOP}. The context attributes set TCA consists of four sub-attributes, which denotes user uses the device at a particular time in a place, namely TCA = {Who AND When AND Where AND Which}. For example, for the resource R, following policy is established to control access:

Tro(read only) = {{Teacher OR Student} AND {class hours OR out off class hours} AND {At Work place/Learning Place OR Outside Work place}AND {Personal Comp. OR Mobile Phone} AND Read only} Trw(read Write) = {Teacher AND out off class hours AND at college AND Personal Comp. AND Read Write}. The policy Tro represents the context condition under which the resource R is allowed to read-only mode. The policy Trw defines the context condition under which the resource R is operated in the read/write mode. Adopting the user contexts [14, 19] to their need motivated to implement an adaptive access control according to the changing context.

III. PROPOSED FRAMEWORK

This section describes the framework and a working model of the proposed system.

3.1 Architecture

We adopt a centralized approach for access control model for the users in small pervasive environments like a college campus. The architecture of the proposed ACARBAC model is given in Fig.1. The architecture contains three units: Input Unit, Process Unit and service audit unit.

The Input Unit: Valid user is identified and retrieved the credentials and privileges from the central server system maintained on the academic campus. For the "GUEST" user, log history and requirement pattern maintained in the database for future reference.

Service / policy manager unit: It is responsible for providing authorization for the valid user and to adapt the policy decisions at an instance.

Process Unit: Maintains the required credentials of the entity like trust, context and other related parameters. The gathered information about trust and context further processed for adapting the access control policies for the user to access the higher priority resources.

3.2 The proposed framework uses different profiles:

User Profile: It contains data about the user like name, user_Id, password, designation, department, email_id, phone_no and photo to be uploaded during their registration step. These details would guide to classify the user type to authenticate and to provide authorization to access the resource in the learning environment. User type may be in the following category like student, researcher, and guest, teaching faculty or non-teaching faculty. Process unit stores the user profile as profile database in the structured format.

Logging profile: This contains user past interaction history. If the user wants to access the unauthorized resources, in that case, this profile would help the recommender system to decide whether to grant or deny permission to access the requested resources.

Temporary profile: It is the set of all data objects within the system processed by user and history profile for new validation sent on to the service/policy unit.

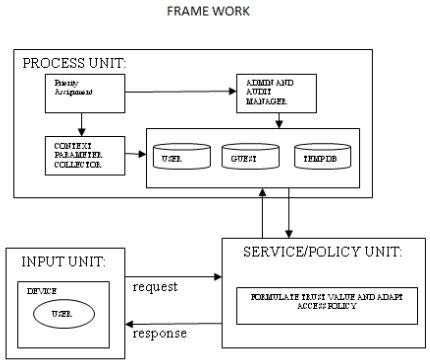


Fig-1: Architecture of the proposed Model

3.3 Working methodology :

The entity/user is treated as subject. The services to the subject are object. The working model is enforced through the identification of the subject before granting or denying access to the objects. Consider User 'U' authenticate himself to the proposed model by validation unit. Next step is to grant authorization for the authenticated user, to access the resource 'R'. Process unit check the request priority and privilege before granting the permission 'P' for the user 'U' to access the resource 'R'. If there is not enough privilege for the requested resource, then permission is granted or denied according to the calculated trust value from the contextual parameters 'C' about that user. The algorithm 1 shows the steps for calculating the access privilege for the requested resource.

Input Unit:

Reads login data from the registered device , store it in the user database. Any change id change like device, role etc., will be adapted by the admin through proper request from the user.

Service Unit:

This unit is responsible for authorizing the authenticated user by obtaining the necessary data from the input unit. This unit formulates the access decision for the authenticated user and fix the privilege and permission policies of the user for the requested resources.

This unit verifies user identity for the registered device/user/entity. Valid user identity was compared with the existing database for identity confirmation. In our model the user type is defined stable at the time of registration. The authorized user accesses the resources coming under his access privilege rights. The privilege 'P' is associated with user type which will be the assigned role 'Role' in our working model. User type 'U' categorized as privilege level 1 to 6 given in the table 1. Role_ids are assigned for the user based on their entered user type as U - user_id . It has been categories like UG – I,II and III year student, PG-I,II year student, teaching staff, non-teaching staff, Office administrator, Head of the Institution or Head of the Department or guest. For Example, if the user_id is entered as student, it implicit information includes programme and stream of study . The privileges for each user type 'U' are listed below :

User Type	User	Privilege(Pi)	
		Service offered	Download Capacity
1	Admin/audit	Monitoring All transactions and audit it	100 Mb
2	Head of the Institution, Deans, COE, HODs, Director for SF course, Course Coordinators, Course Coordinators for SF courses, College Office Admin	Resources of commercial and academic related level	10 Mb
3	Teaching Faculties	Resources related to their academic interests	6 MB
4	Non-Teaching Faculties	Resources like student details, student beneficial documents, Faculties details, faculties beneficial documents	4 MB
5	Students	Resource like learning tutorials, e-	2 MB

		content to their programme specific contents.	
6	Guests	Limited access for the valid resources	2 MB

User type = (user_id)
Algorithm 1:
Input : Access to the resources in direct way
Output : Access grant or deny.
Start :
If: username and password are verified, go for second step verification as selection of image sequence and verify it.
Allow authenticated user for authorized resources.
Else reject as unauthenticated user.
Check resource access privilege :
if it is for higher privilege resource ,
Collect contextual parameter and formulate the formula for access permission privilege rights.
Verify the collected data with the history database.
Verify the threshold level for granting the permission and verify with the service/policy unit.
If confirmation received from the service/policy unit, then assume he is the authorized user to access the resources.
Else: deny the request.
End if:
End if:
End If:
End:
For indirect access of the resources the same algorithm is tested through recommender system , which hold the master user db, log database and nearby privileged user database with resource access rights.
In the process of registration the ACARBAC model, the every User type is defined with the set of resources in his/her privilege. In the process of training the new resource is allotted by calculating the dynamic threshold T to decide the allowable resources. The threshold for the new resource (0 , 1), where 0 represents resource with high priority, and 1 represents a resource with low priority. The allowable upper threshold UT ($\mu + \sigma$) and lower threshold LT ($\mu - \sigma$) are evaluated through the standard deviation and mean from eqn.(4) and eqn.(5) respectively. The yi is the captured value about the particular resource among N types. These values supports to take the access decision on resources. The context data are validated by the checksum value of eqn.(6) using the eqn.(7). Where the eqn.(7) gets the checksum value for the serving resources (R1, R2, ... Rn) at the priority level (P1, P2,..... Pn).

Contextual data	Type	Level of Priority
Location	Canteen ,Recreation club	01
	Classrooms, Laboratory	02
	Faculty Chambers, research lab and Project lab	03
	Heads and Dean Chamber	04
	Principal office, Placements office and administration office	05
Date	August and February	05
	September and March	04
	October, November, April, and May	03
	December and June	02
	July and January	01
Resources	Educational and technical resources	05
	Educational and scientific resources	04
	Open source Software and technical resources	03
	Conference , other related information	02
	Commercial resources	01

Let us consider the user is an undergraduate student trying to download YouTube content from the project lab during the month of June second week or December second week.. According to the access control policy, the

student belongs to the Usertype-1 and don't have the privilege of obtaining commercial resources. At this situation, the context-aware system extracts the contextual information related to the user and requesting resource. The system identifies the location of the user as project lab through an IP or MAC. The assignor has a priority level of 3 out of 5 for the project lab, and date has a priority value of 2 out of 5. The combination of these context checksum values provides proper values to upgrade the User type to higher levels as per the allowable threshold values in the database. On the same, logger collects the past data regarding the involvement of the user on that topic which he/she is request to view the Youtube content. After identifying these, training the request for some time interval is required for better analysis. As per the training set new User type is update for the consent user/entity temporarily for the short span of time. This adapted change in User Type is stored in the history profile as recent data.

Trust Value Evaluation done by these simple formulas:

User _ Id(Uid) = User Type * Allocated BW (privilege level) ------ (1)

Training_period (ti) = No of Request/24*60 for a day. ------ (2)

Total no of users(T0)= ti*(N/6) Where N - Number of Users --- (3)

CCheckSum= Uid * ∑Context value(Cloc , Cdate , Cpast_interaction,Creq_resource) ---- (4)

Rchecksum = Pi * Ri * CCheckSum ------ (5)

TChecksum = T0 * Uid ------ (6)

TFchecksum = Rchecksum + TChecksum ---------- (7)

According to the calculated final trust value (TFchecksum) , permission issued to the user to access or deny the service.

IV. PERFORMANECE ANALYSIS:

4.1 We analyzed the cost effective for the proposed model.

Performance measurements are:

Access Delay: For a particular user U we observed the access time for the same resource/service from different context. The access time varies accordingly with context parameters. The maximum access delay for the requested service is somewhat increased in the order of .5 % for technical resources and .7% for research articles.

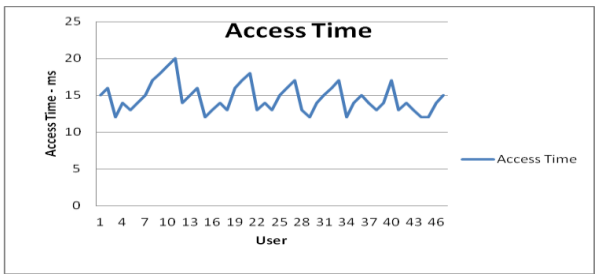
Service processing sequence: To get the access sequence steps we tested the access delay for the same service for 600 students with 1800 request samples. Students belongs to different programmes , accessing same educational content from different locations. Access time delay is directly proportional to number of hub traverse to reach the requested resource from the source. We observed there is an apparent increase in access delay when huge number of request received for the same resource.

V. RESULTS:

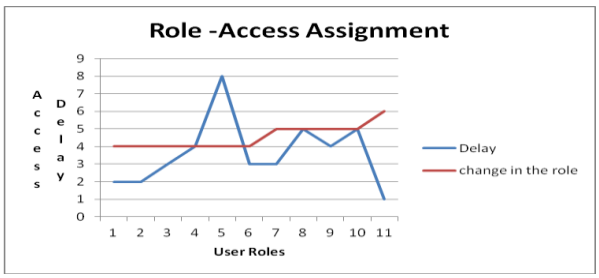
The model performance efficiency has been tabulated as

SECTION	input	Output	Time(ms)	
			RBAC	ACARBAC
INPUT	Raw Data	Formatted Data	10	10
PROCESS	Formatted Data	Y/N status	NA	15
VALIDATION- User Type Identification	Formatted Data	Formatted Data	20	20
VALIDATION –Priority Assignment	Formatted Data	Formatted Data	NA	15

Adding more context parameter is more laborious work to collected the data from all context devices and format them , calculating the total threshold values for each and every services available in that environment. Context data conversion and verification process adds additional 40% time for accessing any privileged services. Following graph shows the access performance for the same service by 200 user at the same time.



Graph – 1



Graph - 2

VI. CONCLUSION

From the above results we observed that if we have included the context parameters as credentials for service access then, there is a considerable delay in achieving the access permission. The request to access particular resource is authorized when the content of request information is relevant to the user's current context information. The user's information is extracted through contextual information like resource, location, time and history. All these together, determine a required authorization for a user and makes the access control adaptive in nature. To minimize the access time, in include the optimization strategy.

VII. REFERENCES:

[1] Ryan, J. Pascoe, D. Morse, "Enhanced reality fieldwork: the context-aware archaeological assistant", Computer applications in Archaeology, 1997.

[2] A. K. Dey and G. D. Abowd, "Towards a better understanding of context and context-awareness", Tech. Report-Georgia Institute of Technology - GVU-99-22, 1999.

[3] Shilit B, Theimer M, "Disseminating active map information to mobile hosts", IEEE Network, 1994.

[4] A. Dey and G. Abowd, "Towards a better understanding of context and context-awareness", Proc. Human Factors in Computer Systems Conf., New York, 2000.

[5] Shahin Fatima, Shish Ahmad and P. M. Khan, "Certificate Based Security Services in Adhoc Sensor Network", in BIJIT Issue 12, Vol .6, No 2, ISSN 0973 – 5658, 2014.

[6] A.M.Hema, Dr.K.Kuppusamy , "Trust based access control schemes for pervasive computing environment" , in Proc. of 2nd International Conference on Recent Trends In Information Technology (ICRTIT), 2012.IEEE Xplore ,Page 157-161.

[7] Alexios Vasileiadis, "Security concerns and trust in the adoption of m-commerce", Master thesis, Mykolas Romeris University, 2013.

[8] Ashema Hasti, "Study of Impact of Mobile Ad – Hoc Networking and its Future Applications", BVICAM's International Journal of Information Technology, Vol. 4, No. 1, 2012.

[9] Yahya, S., Ahmad, E.A. and Jalil, K.A, "The definition and characteristics of ubiquitous learning: A discussion", Int. J. of Education and Development using Information and Communication Technology, Vol. 6, No.1, pp. 117-127, 2010.

[10] Vicki Jones and Jun H. Jo, "Ubiquitous learning environment: An adaptive teaching system using ubiquitous technology", Proc. 21stASCILITE Conf., 2004.

[11] A. S. Patrick, A.C. Long and S. Flinn, "HCi and security system", Proc. of workshop at CHI, USA, 2003.

[12] R.S. Sandhu et al, "Role-based access control models," IEEE Computer Society Press 29(2), pp. 38–47, 1996.

[13] M. L. Wullems Chris and A. Clark, "Toward context-aware security: an authorization architecture for intranet environments", ACM press, Newyork, 2004.

[14] N. Ryan, J. Pascoe and D. Morse, "Enhanced reality fieldwork, the context-aware archaeological assistant", in Gaffney, V. Et al. (Eds.) Computer Applications in Archaeology, 1997.

[15] Gerhard Fischer, "Context-Aware Systems-The 'Right Information', at the 'Right Time', in the 'Right Place', in the 'Right Way', to the 'Right Person' ", Proc. of Advanced Visual Interfaces Conf., ACM, pp. 287-294, 2012.

[16] Campbell and K. Nahrstedt, "Gaia- A middleware infrastructure to enable active spaces", IEEE Pervasive Computing, pp. 74-83, 2002.

[17] Michael J. Covingtony et al, "A context-aware security architecture for emerging applications", Proc. 18thAnnual Computer Security Applications Conf., IEEE, 2002.

[18] A.S.M. Kayes et al, " An Ontology-Based Approach to Context-Aware Access Control for Software Services", Proc. Web Information Systems Engineering Conf., Part I, pp. 410–420, Springer, 2013.

[19] Ali Ahmed, "context-aware access control in ubiquitous computing (CRAAC)", PhD dissertation, University of Manchester, 2010.