ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 8, August 2020

CONTEXT AWARE ACCESS CONTROL MODEL FOR TRUSTED USER IN PERVASIVE APPLICATION

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

[1] Thiagarajar College,Madurai,India [2]Alagappa University, Karaikudi,India

Abstract: In modern world of pervasive era, everything happens in distributed digital form. This feature provides an opportunity for the learner community to learn their course from any place at their preferable time span through any e- gadget. In this scenario, there is a possibility for security vulnerability during service access in pervasive manner. Hence, we propose an access control model, adapt dynamically by the context between trusted entities in pervasive environment. Trust computation done on user preference. The access decision to allow or deny the request from the trusted entity is based on the trust computation and the dynamic role of the user. The model was implemented and the results were analyzed for the valid users.

Index Terms— Pervasive, access control, trust, context, role, security.

1. INTRODUCTION

Pervasive computing is the new paradigm of computing world to utilize the resources in pervasive manner. In today's digital world, ICT become a part of the life activity. Hence, we need to be concerned on many factors to preserve our authentication and authorization while accessing the data. In all transaction contexts, trust and role had an authority for secured transaction. Context may be the information like location, time and other surrounding environmental factors of an entity/user. In pervasive computing, context awareness plays a vital fact, defined by Schilit. Context-aware information disposes the user's current situation. Context may be a way of describing the whereabouts of the entity, available resources and the environmental parameters. This information's are delivered by their electronic gadgets under which surrounding they are working to access the requested resource by the defined set of axioms.

Access control policies in traditional system are static and more over they are server centric. But in pervasive environment, access control policies must be adaptive in nature because of the distributiveness and mobility of the entity. Hence, we need to address the security challenges in integrity of accessing the resources. In our proposed system, we have formulated the access control decisions, as authentication and authorization for accessing the required services. Authentications verify the identity of the user/entity by user name, password and by their Date of Birth. Once the user identity was declared, the user assigned access rights and privileges by admin and audited by audit agent. In our model we have categorized the user type according to the context parameter like location, time, and network and entity trustworthiness. The model we concentrate on learning environment in pervasive fashion.

Learning Module in pervasive scenario provide flexibility for the user learning style. Initially the user who like to utilize the pervasive learning feature, checked for their authentication. Then the authorization control assigned to them as by their roles. Context information like location, time and network specification captured for the authenticated user. In addition to these contexts it will add situational parameters of the location of the entity from where the request was initiated to access the service or resource. This feature helps the user to set their preference of learning pattern in flexible manner.

Our proposed model, context aware access control model for trusted user in pervasive environment adapt user's real situation to provide relevant information for learning, based on their requirement. Learning resources were assigned to the user based on the assigned role and location, time at which the request raised and the network type through with the request has transferred to the server. If the user wants to access the resource which is not within his privileges, then the situation was solved by analyzing the user post history and permitted them as temporary delegates for short period of time by the admin. This data was updated in the master database for projecting the user interest in future. The user can hold more than one role at an instant of time, in such scenario computing system provide a better level of understanding of the situation about the user, and handle well the complex relations between the various essentials. The adaptability in these situations is carefully monitored by admin and audit system. Hence, this, adaptive trust based context aware access control model facilitate access control policies to the user/entity by gathering information about user activity, requirements and preferences.

The resources of the learning modules are uploaded on server machine and the resources are accessed by the trusted entities, from their owned places like computing laboratory, library or class room. The valid user will be given permission to access the resources, according to their current active role(R) and service trust value (T), request initiated time (T) and access privileges (P) assigned for the current active role. Credentials are assigned for the user according to their correctness and accurate data entered through the login page. If the user, validate the login form for more than '3' times then credential is reset to zero and malfunction information has been informed to the entity/user through the entered valid email and this has been updated on the global database for future reference. To get authentication, user send a request to admin and user will receive the reply .For the authenticated trusted user a set of authorization rights, privileges were assigned to access the services or resources in pervasive environment in accordance with the current role. The administrator maintains and controls the user authorization and access policies. The entity/user permission rules are updated dynamically with the current role and by the collected information.

Flow of remaining part of the paper is, section 2 illustrate the complete overview on related works in the context-aware models and trust models for pervasive applications domains, section 3 elaborate the working principle and architecture of the proposed model, section 4 give the overall result and performance analysis of the model for different situations, section 5 ends with conclusion and suggestions for future work.

2 RELATED WORKS

Several access control models have been proposed, but Role-based access control (RBAC) models have been considered as important, because of the systematic access control security through a proven and increasingly predominant technology for any application in pervasive computing environment. RBAC can support different authorization policies including mandatory and discretionary through the appropriate role configuration.

In pervasive computing access control domain, RBAC has significant action to concentrate on security issues and to accommodate contextual information such as time and location, in [1] role activation dependencies activated by role trigger action, solved the conflicting role assignment. [2] Objects, user location, spatial role are defined in the form of role schema with logical and physical location boundaries. Access permissions formulated by inherited role with role hierarchy. In [3] Access permission formula defined in terms of trust level as user credentials , transaction history and recommender status.[4] Permission rules defined as combination of time and location of the entity. [5] Spatial-temporal constraints considered for the inherited role of the user for accessing the resources. [6] Updated TRBAC model, with an additional temporal constraints in the form of role activation duration by their separation of duty definition to access the resources. [7] In this model RBAC has extended with location parameter to decide the access permission for the static and dynamic object in the pervasive environment.[8] Author defined the access permission between the trusted user based on their trustworthiness.[9] in this model , formula for the trust relationship between trusted entities includes experience, recommendation, and knowledge in the given context from the context graph.[10] This model utilizes RBAC with an additional environmental parameters to determine the access permission for the requested resource Negative responses solved by delegation role. Most of the models define the access control for the identified and authenticated user. In [11] authors proposed approach to incorporate the concept of trust to RBAC to tackle above problem. The general idea in these works is that the access privileges of a user depend on his trust level.General concept of dynamic trust model in pervasive computing environments had been given by Marsh in his thesis ‘Formalizing Trust as a computational concept [12]. In [13], the authors explained basic scenarios in ubiquitous computing and modeling requirements of trust. A solution to evaluate trust from the past experience was given in [14]. In [15] the author proposed a role based trust model in ubiquitous/pervasive environment, where recommendations were used to make decision. In [16] the authors proposed a novel cloud-based trust model to solve uncertain problems, when it comes to decision making based on these trust values, they just compare with one or two thresholds, which cannot dynamically change due to the change in the environment. Yu [17] defined the concepts for trust negotiations, strategies and protocols, and proposed a couple of strategies for automated trust negotiation between two unknown entities. In [18] author defined the context based authentication framework for pervasive computing environment as context attributes.

3 PROPOSED MODEL

In this section we describe working model of our proposed framework and explanation of trust computation.

3.1 Framework

Our Framework, represented in fig.1, contains: Input Unit, Check unit, Process Unit, Update and Output Unit. The learning resources are posted in centralized server to manage the learning and monitoring activity of the user/student. To implement this framework, we defined the functionalities of each unit. The Input Unit, provide authentication for the user through login form. The user identification further grained by their date of birth, in user preference format. Check Unit finds the correctness of the authenticated user, by assigning the active role .Process unit validate the static permission of the user, and reevaluate the permission rules by their credentials like identification and context parameters. If the request from the user is not within their allow permission level, then to process the request of the user by recommender instruction by analyzing their past interaction and success rate. Update and Output Unit is responsible for providing authorization for the valid user, availability of the requested resource, and updates the calculated trust value for the dynamic access privileges for direct and indirect interaction. The final transaction history maintained as a global database.

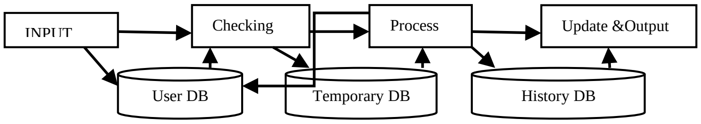

Fig-1: Framework of the proposed model

3.2 The proposed model has different profile databases:

User Database: It contains data related to the valid user. User profile holds information about user name, user id, password, and department, date of birth, stream, email id, phone number and location. 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 was categorized as student, staff, admin and guest. Process unit stores the user profile as profile database in the structured format.

History DB: This database maintains the user past interaction history. If the user wants to access the unauthorized resources, in that case, this DB would help the admin to decide whether to grant or deny permission to access the requested resources.

Temporary DB: This database holds information about the temporary roles assigned to the user according to their request sent to the admin to the access the other group resources. It has all data objects within the system processed by user and history profile for new validation sent done by the admin.

Working Principles of the proposed model:

The entity/user acts as subject and existing resources and services are named as object. Users are identified by their username and password entry, further verified by their date of birth validation. These processes are continued in checking unit for providing the authorization for the user to access the requested resource. .Next step is to grant authorization for the authenticated user, to access the resource ‘R’. Checking unit, validate the user authentication and assign priority for the requested resources for further processing to calculate the final trust value for the requested service in the pervasive environment. Process unit, do transaction for the prioritized request and fix the privilege ‘P’ for the current role of the user ‘U’ to access the resource . For insufficient privilege, decision to provide access permission includes the contextual parameters of that user and the history DB information. The algorithm 1 shows the steps for deciding the access privilege for the requested resource.

Input Unit:

Accept new user registration; store it in the user profile database and history of processed service was stored in history database. This information was entered through the registered devices with the pervasive server.

Checking Unit:

This unit is responsible for authorizing the authenticated user by checking the relevant credentials received from the input unit. For the authorized user, access permission will be updated in the history DB, from the calculated trust value according to the context, trust value for the requested service.

Validation steps:

1. Identify the valid user. If the user was already registered then the login form verifies username and password, where username is roll number for the students, mail id for the staff and for guest it was reset to ‘guest’. The user type is stable at the time of registration.
2. For the valid user second step verification done through their date of birth, as per the format of the user preference.
3. For the authenticated and authorized user, access permission assigned by their current privilege ‘P’ for the current dynamic role ‘R’ by their context ‘C’.

Process Unit: Stores the identity of the user with the current assigned roles in the history DB for the requested resource and allow the user to access the resources according to the user category ‘U’ and privileges.

Output Unit: Record the transaction history and process the request from the trusted user , to allow or deny the access permission according to the calculated trust value and the received context parameters.

‘Role_ids’ assigned to the authenticated user as per their user category ‘U’ ‘user_id’. User category may be of Admin/Audit, Administrative staff (Head of the Institution, HoD , Class Coordinators, Functional Deans), Teaching Faculty, Non-teaching faculty, student, guest. Student category further subdivided and grouped like UG – I,II and III PG-I,II, implicit information of their registered determine the programme under which the student has registered and study stream . Offered services for user type have been initially defined, so that we clearly defined their separation of duties. The assumed privilege and resource details are listed in the table1.

TABLE – 1 : List the user level and their privileges.

User Type	User	Privilege(P)	
		Service offered with access rights	Download Capacity
1	Admin/audit	Monitoring All transactions and audit it (Read,Write,Update and Modify)	100 MB
2	Administrative staff and Head of the Institution	Resources like public communication and circulars, notices from higher education department and academic calendar with event details. (Read,Write,Update and Edit)	5 MB
3	Teaching Faculties	Resources related to their academic (Read, Write)	4 MB
4	Non-Teaching Faculties	Student beneficial documents, Faculties beneficial documents (Read and Write)	4 MB
5	Student	Learning tutorials text form only, on line quizzes related to their learning style. (Read only)	2 MB

6	Guests	Limited access for the valid learning resources (Read only)	2 MB

Algorithm

Input: Receive the request from the entity/user to access the available active resources in the pervasive environment.
Output: Permission Grant or Deny.

```
Start:
    1. Read data from login form check already registered user then sign in otherwise go to step 2.
    2. Read data from sign up form and store it in the user profile, then go to sign in step.
    3. IF: username and password are verified then allow authenticated user for authorized resources, done at check unit by second level by their date of birth user defined format.
Else: reject as unauthenticated user.
    4. Check resource access privilege :
       IF : for sensitive data resource ,collect contextual parameter and calculate the threshold trust for the
            requested service and Cross check with the history database.
       Compare the service threshold level for permission grant, with the calculated trust value, done at process unit.
Else go to step6
    5. $IF: confirmation\ received\ from\ the\ process\ unit, update\ the\ calculated$
     trust value at that instance of transaction and permit the request
                  issued entity/
user to access the resource by grant status.
    6. Else: deny the request.
    7. $End\ if$:
    8. $End\ if$:
    9. $End$:
```

Update and Output unit defines the set of resources for the valid authorized user within his/her privilege. Process unit, set the dynamic access permission by training the data, calculate threshold trust value T to decide the allowable resources. The threshold value for the resources is between 0 and 1. The value of threshold range is evaluated through the standard deviation and mean based on posterior probability concept. The formula for calculating the initial trust value is given in equation (1).

$$Ti = \frac{1}{\sqrt{2\pi\sigma}}\ e - \frac{(x-\mu)2}{2\sigma 2} \quad \text{-------------------- (1)}$$

Where µ is mean and σ are mean and standard deviation.

User verification done by the following formula 2:

$$User(Ui) = f\ (usertype, download\ capacity, privileges) \quad \text{-------------------- (2)}$$

Calculated Time for processing the request from the entity is defined by the following formula 3.

Tp = Tr * success rate * Number of user/user type

Tp is time for getting the permission.
Tr is time to receive the request from the entity.
Success rate is processed request/number of request

Context value is formulated as equation (4).

$$Context\ (C_{total}) = C_{location} + C_{time} + C_{resource} \quad \text{------ (4)}$$

Role activation for the trusted entity while granting the permission , is formulated as (5).

$$R_{current} = R_{actived} * U_{i\ i} * C_{total} \quad \text{---------------- (5)}$$

Final Threshold value of the resource is calculated as in formula 6.

$$T_{threshold} = Tp * C_{total} * T_i * R_{cuurent} \quad \text{----------------- (6)}$$

Where T_i - initial Trust value

Table 2 : List of context parameter with the level of priority

Contextual data	Type	Level of Priority
Location	Unknowns Classroom, Lab, Library Department Chamber Placement Office Administrative Block	01 02 03 04 05
Time Slot	Evening (7 to 10 pm) Evening (4 to 7 pm) Afternoon(1 to 4 pm) Noon (10 to 1 am) Morning(7 to 10 am)	05 04 03 02 01
Resources	UG programme Content:ppt., docx , mp4 file uploaded by their course teacher PG programme Content : ppt, docx, mp4 file uploaded by their course teacher Open source Software Conference (technical , non-technical, academic) Resources with minimal preferences- commercial	05 04 03 02 01

Suppose the student want to access commercial YouTube content, which is rarely related to his course of study, then the decision for providing access permission is decide by the admin by checking the reliability of the request issuer by analysis his past history interaction database. Further the decision depends on the contextual parameter of the requester. In our case, student user type is 5 and his request arrived from the classroom at 5 pm, for that the privileges assumed as, permission to access course content and he don't have the privilege of download/view commercial resources. The assigned priority level for the class room is 2, and time priority is 4. The collected context helps to fix the threshold value for the requested resource by the formula (6). Access permission is updated for the valid user with temporary role for short time period. For such cases, training algorithms was deployed to get better performance. As per the training set new User type is update for the current user/entity temporarily for the short span. The temporary role and user type is updated in the history database and temporary roles are stored in temporary database. Decision for providing the permission to access the requested resource sanctioned for higher calculated the threshold trust value.

4 RESULT and PERFORMANCE ANALYSIS

Performance measurements are:

1. Access time proportion: 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 access time proportion, for the technical services is 0.6 % for students, 0.2% for teacher for the location context 'Lab'.
2. Service processing sequence: To get the access sequence steps we tested the access delay for the same service for 600 students with 1000 request samples. Students belong 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.
3. The student's t distribution sampled for 50 data , we observed that the acceptance level is at 6 the 't' test value almost same as normal distribution value, which is .707 and standard error is about 0.289 and confidence interval for granting the requested resource to the trusted entity is 95%..
4. If the sample size is extended for 1000 samples, standard error is 0.13 with confidence interval of 95%,

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 20% time for accessing any privileged services. Following graph shows the access performance for the same service by 50 users at the same time.

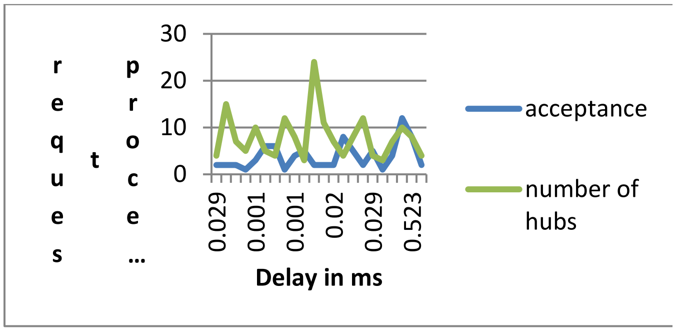

Figure 1 : Access delay of the resource for the request acceptance and travelled hub count

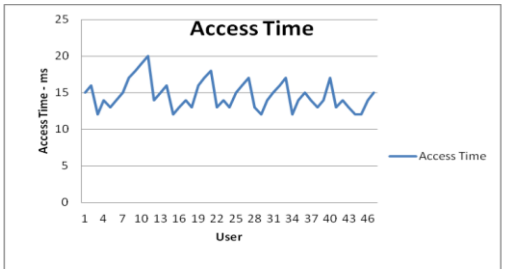

Figure 2 : Access time delay by adding the Context parameters

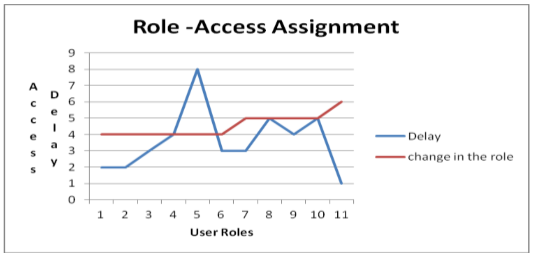

Figure 3 : Updated role at the instance of Request process

Fig 1 shows the access time for different user/entity for the positive acceptance, and the number hubs between the source and destination of the entities. Fig. 2 display the how the context had an impact to access the resource. Fig.3 illustrate role activities.

6 CONCLUSIONS

From the above results and performance of the model, we inferred that the access delay directly proportional to the number of context parameter taken into account to fix the decision for granting the permission or to deny the permission for the requested resource or service available in the environment. The context information improves the security level of the trusted user to access the resources in adapting the mechanism in dynamic manner. Even though the time to access the resource is considerable increased for the proposed model by adding more credentials like context and trust factors, we observed the error rate for rejecting the request is minimum. In future, we like to minimize the access delay for the requested resource by increasing the network bandwidth and by using proper optimization methods.

Acknowledgement

This research work has been written with the financial support of Rashtriya Uchchatar Shiksha Abhiyan (RUSA – Phase 2.0) grant sanctioned vide Letter No. F.24-51/2014-U, Policy (TNMulti-Gen), Dept. of Edn. Govt. of India, Dt. 09.10.2018.

REFERENCES

[1] Bertino, Elisa, Piero Andrea Bonatti, and Elena Ferrari. "TRBAC: A temporal role-based access control model." ACM Transactions on Information and System Security (TISSEC) 4.3 (2001): 191-233.

[2] Chakraborty, Sudip, and Indrajit Ray. "TrustBAC: integrating trust relationships into the RBAC model for access control in open systems." Proceedings of the eleventh ACM symposium on Access control models and technologies. 2006.

[3] Chandran, Suroop Mohan, and James BD Joshi. "LoT-RBAC: a location and time-based RBAC model." International Conference on Web Information Systems Engineering. Springer, Berlin, Heidelberg, 2005.)

[4] Chen, Liang, and Jason Crampton. "On spatio-temporal constraints and inheritance in role-

based access control." Proceedings of the 2008 ACM symposium on Information, computer and communications security. 2008.

[5] Toahchoodee, Manachai, et al. "A trust-based access control model for pervasive computing applications." IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Berlin, Heidelberg, 2009.

[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] Ray, I., Ray, I., Chakraborty, S," An Interoperable Context Sensitive Model of Trust.", Journal of Intelligent Information Systems 32(1), 75–104 (2009)

[8] Ray, I., Toahchoodee, M.," A Spatio-Temporal Access Control Model Supporting Delegation for Pervasive Computing Applications.", In: Proceedings of the 5th International Conference on Trust, Privacy & Security in Digital Business, Turin, Italy (September 2008)

[9] Geepalla, Emsaieb, Behzad Bordbar, and Kozo Okano. "Verification of spatio-temporal role based access control using timed automata." 2012 IEEE 3rd International Conference on Networked Embedded Systems for Every Application (NESEA). IEEE, 2012.

[10] Toahchoodee, M., Ray, I.: On the Formal Analysis of a Spatio-Temporal Role-Based Access Control Model. In: Atluri, V. (ed.) DAS 2008. LNCS, vol. 5094, pp. 17–32. Springer, Heidelberg (2008)

[11] Marsh, S.P, "Formalising Trust as a Computational Concepts" . Ph.D. Thesis , Ray, I., Kumar, M., Yu, L.," LRBAC: A Location-Aware Role-Based Access Control Model.", In: Bagchi, A., Atluri, V. (eds.) ICISS 2006. LNCS, vol. 4332, pp. 147–161. Springer, Heidelberg (2006)

[12] University of Stirling (1994).

[13] Lamsal,P, "Requriements for modelling trust in ubiquitous computing and ad hoc networks", Ad hoc mobile wireless netwoks- Research seminar on Telecommunications software(2002).

[14] Aime, M.D. and Lioy, "A.: Incremental trust: building trust from past experience." In Proc. of IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, Italy (2005) 603-608

[15] Shand, B , Dimmock, N, Bacon , "J : Trust for Ubiquitous , Transaparent Collabration." In Proc. of ACM: Special issue: Pervasive compurting and communications(2004) , 711-721.

[16] He, R. Niu, J.W, Yuan , "M : A novel Cloud-Based Trust model for pervasive computing ." In Proc. of the Fourth International Conference on Computer and Infromation Technology (2004) 693-700

[17] Pierre E. ABI-CHAR 'A Dynamic Trust Based Context aware secure authentication framework for pervasive computing environment', Ph.D. Dissertation , May 2010.