REST Journal on Emerging trends in Modelling and Manufacturing
Vol: 5(4), 2019
REST Publisher
ISSN: 2455-4537

Website: www.restpublisher.com/journals/jemm

Context Based Service Access framework for Pervasive application: Comparative Analysis of AHP and Fuzzy AHP

A. M. Hema[#], K.Kuppusamy[*]
[#]Department of Computer Science, Thiagarajar College, Madurai, Tamil Nadu, ,India
[*]Department of Computer Science and Engineering Alagappa University, Karaikudi , Tamil Nadu, India
[1]jehemaeinkaran@gmail.com, [2]kkdisamy@yahoo.com

Abstract
Significant advancement in the area of communication technology paves a way for a pervasive environment. Role based access control policies provide fixed security in the access control mechanism. RBAC being used in combination of contextual parameters to improve the security in access control mechanisms. Because of the mobility of the entities, we need to adapt new access control policies accounting the contextual parameters. In this paper we developed a new access control based on preference of the contextual parameter for the trusted entity based on fuzzy Analytical Hierarchy Process (AHP). We observed that the access control preferences are by location, network, time and initial trust value of the requested service in dynamic situations. It provides flexibility and scalability in enforcing security policy between trusted entities.
Keywords: Pervasive, fuzzy AHP, trust, context, Access control.

1. Introduction

Most important advancements in communication technologies have shifted personal computing to pervasive environments. For static situation, network security is defined as access control policies, based on authentication and authorization of the entities. But in the pervasive computing environment, due to the device's mobility we need to adapt dynamic access control policies. Therefore, we have proposed new access control framework based on the context of the trusted entities for accessing the objects or resources in the pervasive environment. While framing the rule for the access control framework we have to consider the basic network security measures such as confidentiality, integrity and availability of the entities. Confidentiality ensures that the protected data is shared between the right users; integrity shows that request is from the authorized user and availability meets the authorized user request if the resource is in an available state. Access control policies provide authorization to the authenticated user by a set of rules as privileges to access the resources. In a pervasive environment, the entities are facilitated with dynamic access control policies based on the nature of the network, location, time of accessing the resources, initial trust value and recommender or delegator. Fuzzy Analytical Hierarchical Process (AHP) selects the order of preference of the contextual parameters for defining the access control policies in a pervasive environment. The delegation of access rights is strongly computed on trust level of the recommender system .User is authorized to access the resources by their defined access rights in mandatory access control model. User Identity is used in discretionary access control. Role of the user is significant in case of Role-based access control models. All these traditional models are static and centralized system. In context based access control model, the access is provided to resource owners and administrators according to resources location. They have defined access policies completely based on context [1]. Hence in this paper, we have explored context based access control framework by Fuzzy Analytic Hierarchical Process using extended Analysis method for the trusted entities, to provide dynamic rights. Rest of the paper is organized as follows: Section 2 gives a literature review, Section 3 explains the fuzzy AHP process for the trust value computation to decide the service access control and Section 4 concludes the paper.

2. Literature Review

Trust is an important factor in internet based e-commerce services, in which trust is calculated by means of reputation and dynamic trust values are formulated mathematical [2]. In [3] trust value was calculated by assigning the credential to nodes, updating private keys , managing the trust values of each node and making appropriate decisions about nodes' access rights. In [4] the formal definition of trust had been postulated for pervasive and distributed environment. Trust description, trust evaluations are established and included. Trust level was used to make decision in accessing the resources between trusted entities [5]. In all cases trust become very important factor and context parameters are taken into account to adapt dynamic access control policies. So context parameters can be viewed as value based factors to fix the consistency in providing security for accessing the resources. Hayashi et al.[6] present a probabilistic model for context-aware scalable authentication in order to enable the selection of appropriate active authentication factors given a set of passive authentication

factors. Filho and Martin [7] propose an owner-centric QoC-Aware Context-Based Access Control model that takes into account both context information and its QoC indicators to grant and to adapt access permissions to resources. Chakraborty et al. [8] introduce a context-aware model-based solution to prevent privacy in mobile application. Most significant parameters to calculate the trust value to access the request service in direct way. In this scenario, we have taken only direct request. [9] Defines the AHP theory. In [10] cloud user behaviour was analysed using fuzzy AHP. The following table.1 lists the common factors which had an influence for doing the service transaction.

Table 1: Factors to be considered in decision making to provide the service or not.

parameter	1	2	3	4	5	6
Location	Undefined	Classroom	Lab1	Lab2	Lab3	Lab4
Time	Morning	Forenoon	Noon	Afternoon	evening	
Network Access Point	Unknown	Work-Wifi	Celluar	Hotspot	Leases Line	
Initial trust value	Low	Medium	High			

To decide whether to allow or deny the requested service by the entity/user we need to collect various contextual parameters and trust value. As every parameter contribute in the calculation of the trust value to allow the entity/user to access the service or to deny the request from the entity. From the decision making perspective whether to allow or deny the user/entity to access the service, we need to consolidate these parameters into a single integrated form. To do this consolidation, MCDM (Multi Criteria Decision Making) method links between the parameter, of which their relative attribute to the overall trust value derived. Among various MCDM methods Fuzzy AHP has the advantage of handling both tangible and intangible. Fuzzy AHP has been widely used in a variety of policy selection, decision making, adaptive learning, recommendation system. Fuzzy logic is an approach that deals with uncertain data and imprecious knowledge. Fuzzy AHP is used to take decision under uncertainty circumstances.

Steps in Fuzzy AHP phase process:

Step 1: Define the requirement. Here our requirement is to decide whether to allow or deny the request from the trusted entity to access the service in context based access control framework.

Step 2: Create comparison Matrix.

Step 3: check for consistency.

Step 4: Setup triangular fuzzy number.

Step 5: calculate the weight value of the fuzzy vector.

Step 6: Rank and set the decision for allow or deny the access control permission.

Table 2: Priorities for security alternatives with respect to the Network Access Point

Network – undefined	Allow	Deny	Priority	Network – Classroom wifi	Allow	Deny	Priority	Network – Lab1 Leased line	Allow	Deny	Priority
Allow	1	1/9	.1	Allow	1	5	.833	Allow	1	7	.875
Deny	9	1	.9	Deny	1/5	1	.167	Deny	1/7	1	.125
Network -Lab2 – Leased Line	Allow	Deny	Priority	Network – Lab3 leased Line	Allow	Deny	Priority	Network – Lab4 leased Line	Allow	Deny	Priority
Allow	1	7	.875	Allow	1	6	.857	Allow	1	6	.857
Deny	1/7	1	.125	Deny	1/6	1	.143	Deny	1/6	1	.143

Table 3: Pair wise Comparison Matrix – AHP process

Context/Trust	Location	Network Access Point	Time	Initial Trust value	Priority
Location	1.000	0.200	3.000	6.000	0.225
Network Access Point	5.000	1.000	7.000	8.000	0.632
Time	0.333	0.143	1.000	2.000	0.088
Initial Trust Value	0.167	0.125	0.500	1.000	0.053

Table 4: Normalized Matrix – Fuzzy AHP using geometric mean method.

Context/Trust	Location	Network Access Point	Time	Initial Trust value	Priority
Location	1 1 1	1/6 1/5 1/4	2 3 4	5 6 7	0.255721
Network Access Point	4 5 6	1 1 1	6 7 8	7 8 9	0.617147
Time	1/4 1/3 1/2	1/8 1/7 1/6	1 1 1	1 2 3	0.088799
Initial Trust Value	1/7 1/6 1/5	1/9 1/8 1/7	1/4 1/2 /3	1 1 1	0.038333

Table 5: Normalized Matrix – Fuzzy AHP using extent analysis method

Context/Trust	Location	Network Access Point	Time	Initial Trust value	Priority
Location	1 1 1	1/6 1/5 1/4	2 3 4	5 6 7	0.345
Network Access Point	4 5 6	1 1 1	6 7 8	7 8 9	0.607
Time	1/4 1/3 1/2	1/8 1/7 1/6	1 1 1	1 2 3	0.038
Initial Trust Value	1/7 1/6 1/5	1/9 1/8 1/7	1/4 1/2 /3	1 1 1	0.013

Table 6: Fuzzy number Scale definition is as follows:

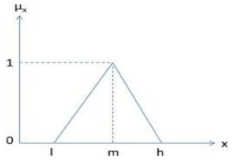
Saaty scale	Fuzzy Number Scale
1	Equally Importance (1 1 1)
3	Weakly importance (2 3 4)
5	Fairly importance (4 5 6)
7	Strongly Importance (6 7 8)
9	Absolutely Importance (9 9 9)

Fig 1: Represent Fuzzy triangular number. Where 'l' represent lower bound, 'm' – middle value and 'u' represent upper bound value. Membership function is μ_x, which range between 0 and 1. Let represent a fuzzified reciprocal nn-judgment matrix containing all pairwise comparisons between elements i and j for all$\in$ i,j {1,2,…,n}

$$\tilde{A} = \begin{pmatrix} 1,1,1 & a_{12} \ldots. & a_{1n} \\ a_{21} & 1,1,1 \ldots. & a_{2n} \\ : & . \ \ldots & : \\ a_{n1} \ldots\ldots\ldots; \ldots\ldots & & 1,1,1 \end{pmatrix} \quad \text{--------- (1)}$$

$$\mu_x = \begin{cases} (x - l)/(m-l) & , \ x \in (l,m) \\ (u-x)/(u-m) & , \ x \in (m.u) \\ 0 & \text{otherwise} \end{cases} \quad \text{--------- (2)}$$

Where $l_{ij} \leq m_{ij} \leq u_{ij}$. If $l_{ij} = m_{ij} = u_{ij}$ the fuzzy number gets a crisp number. In equation (1) where and all are triangular fuzzy numbers with l_{ij} the lower and u_{ij} the upper limit and m_{ij} is the point where the membership function $\mu(x) = 1$. The membership function $\mu(x)$ of the triangular fuzzy number may therefore be described as (Chang, 1996, 650):



Basic operations on fuzzy arithmetic are: Assume M_1 and M_2 are two triangular fuzzy numbers with M_1 is (l_1,m_1,u_1) and M_2 is (l_2,m_2,u_2) , then the basic operations are

$$\tilde{M1} * \tilde{M2} = (l_1 * l_2 , m_1 * m_2, u_1 * u_2) \quad \text{------- (3)}$$

$$\tilde{M}_1 + \tilde{M}_2 = (l_1 + l_2 , m_1 + m_2 , u_1 + u_2) \quad \text{---------- (4)}$$

$$\tilde{M}_1' = (1/l_1 , 1/m_1, 1/u_1) \quad \text{---------- (5)}$$

We will need these operation laws in order to be able to estimate priorities out of the fuzzy matrix A .

In case of extent analysis method the decision priority calculated as:

Step 1: calculate the fuzzed pair wise comparison matrix.

Step2: calculate fuzzy synthetic extent with respect to its i_{th} alternatives.

$$\tilde{S}_i = \sum_{j=1}^{m} \tilde{M}_{g_i}^j \otimes \left[\sum_{i=1}^{n} \sum_{j=1}^{m} \tilde{M}_{g_i}^j \right]^{-1}$$

---------- (6)

Step3: calculate degree of possibility:

$$V\left(\tilde{M}_2 \geq \tilde{M}_1\right) = hgt(\tilde{M}_1 \cap \tilde{M}_2) = \begin{cases} 1, & if\ m_2 \geq m_1 \\ 0, & if\ l_1 \geq l_2 \\ \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)}, & otherwise \end{cases}$$

---------- (7)

we can find the non – fuzzy weight vector was :

$$W = \left(\min V\left(\tilde{S}_1 \geq \tilde{S}_k\right), \min V\left(\tilde{S}_2 \geq \tilde{S}_k\right), \ldots, \min V\left(\tilde{S}_n \geq \tilde{S}_k\right)\right)^T$$

----------(8)

In case of geometric method of fuzzy AHP we calculate priority as:

$$\tilde{r}_i = \left(\prod_{j=1}^{n} \tilde{p}_{ij} \right)^{1/n}$$

---------- (9)

and

$$\tilde{w}_i = \tilde{r}_i \otimes \left(\sum_{i=1}^{n} \tilde{r}_i \right)^{-1}, i = 1, 2, \ldots, n$$

---------- (10)

For AHP we need to find the consistency Index (CI) which is defined as

$(\lambda_{max} - n)$ and Consistency Ratio is defined as CR = CI / RC where RC – Random consistency value ----- (11)

CI = ----------

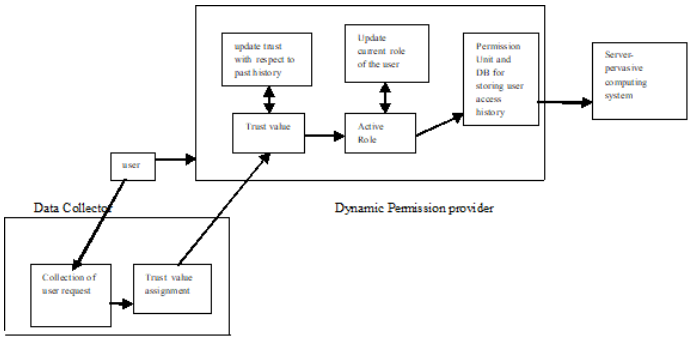
(n – 1) $CR \leq 0.1$

To simplify the calculation of the CR, we used the crisp value m_{ij}. If the CR exceeded the tolerable level of 0.1, we excluded the pairwise comparison matrix of this combinational context for further analysis, because this could affect the overall results negatively.

3. The trust value computation:

Final Trust value computation is done by the context factor preferences from AHP, fuzzy AHP processes. To validate the process steps we have taken the academic learning pervasive environment. The calculation configuration comprises list of context and trust factors to Allow or Deny the service request based on the importance of each context and trust value.

The context based Access Control Framework is shown in the figure 1.



a. Data Collector unit: This unit manages all requests from the trusted entity. Global database stores the information about history of the trusted entity and the available resources in this environment. Based on the calculated trust value, this unit provides the access permission control decision for the requested service.

b. Dynamic Permission provider: This unit calculates the consistency ratio, non-fuzzy priority vector using extent analysis method and geometric method.

We have developed web based learning system to illustrate the above situation. Through login page we identify the user .The credentials are username and their date of birth. To do authorization we check this input with the existing global database. We had another table with permission rights for the available service in the environment. To define the decision control for service access, we have taken four different context and trust parameters, listed in table 1. Each context aspects can have six

different states. Location has six different states : like unknown, classroom,lab1,lab2,lab3,lab4 , while time has five states , network access point has five states and trust related parameters have three states as : low, medium and high.

Now we evaluate the context aspects with respect to importance in the security level. The context and trust parameter importance to achieve the security level, done by pair wise comparison and the priority of each parameter is calculated using AHP and Fuzzy AHP process and tabulated in Table3.

Table 7 : Relative Pair wise matrix for ALLOW state calculated for all the three AHP method using the above formulas

Context/Trust	State	Alternative (A)	Priority value(P)	A * P(AHP)	FAHP(geometric mean method)	FAHP (extent analysis method)
Location	Lab2	0.875	0.279272	0.225	0.255721	0.345
Network Access Point	Work	0.857	0.482524	0.632	0.617147	0.607
Time	FN	0.68	0.118007	0.088	0.088799	0.038
Initial trust value	Medium	0.2	0.040066	0.053	0.038333	0.013

From the above table we observed that the preference of accessing the resource by the trusted user in pervasive environment is mainly depends on the network access point, then by their location. But the initial trust value also had some influence while calculating the decision matrix weight value for giving the permission to allow the user to access the resources. We observed that location ie proximity of the user is more sensitive in case of FAHP – extent analysis than other two method.

Conclusion

In this paper, we process a context based access control framework that includes user's context like location, time and network type they have used and trust aspects like initial trust value assigned to the available services in the environment, rate of allow permission depends on the user interaction history. The framework compares the AHP structured method with the fuzzy AHP for dynamically evaluating user's context and trust values, and provides the appropriate decision. We use academic learning environment, as a test implementation case, to evaluate our proposed framework and method. The results have demonstrated the efficiency in enforcing the service access control.

References

1. Filho, J.B., Martin, H, "A generalized context-based access control model for pervasive environments", ACM Workshop on Security and Privacy in GIS and LBS, 2009

2. Bo Tian, Kecheng Liu, Yuanzhong Chen,"Dynamic Trust and Reputation Computation Model for B2C E-Commerce", Future Internet., vol.7, pp.405-428, 2015.

3. AzzedineBoukerche,Yonglin Ren, "A trust-based security system for ubiquitous and pervasive computing environment", Elsevier.,vol.31,pp.4343-4351,2008.

4. DaoxiXiu ,Zhaoyu Liu, "A Formal Definition for Trust in Distributed Systems", Spring verlag Berlin Heidelber. Pp.482–489, 2005.

5. A.M.Hema,K.Kuppusamy, " Trust based access control scheme for pervasive computing environment ", in Recent Treads in Information Technology (ICRTIT),2012 International Conference on,2012,IEEE,pp. 157-161.

6. Hayashi, E., Das, S., Amini, S., Hong, J., Oakley, "Casa: context-aware scalable authentication." In: Proceedings of the Ninth Symposium on Usable Privacy and Security; SOUPS '13. New York, NY, USA: ACM. ISBN 978-1-4503-2319-2; 2013, p. 3:1–3:10.

7. Filho, J.B., Martin, and H. "Qacbac: an owner-centric qoc-aware context-based access control model for pervasive environments." In: Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS; SPRINGL '08. New York, NY, USA: ACM. ISBN 978-1-60558-324-2; 2008, p. 30–38

8. Chakraborty, S., Raghavan, K.R., Johnson, M.P., Srivastava, M.B. "A framework for context-aware privacy of sensor data on mobile systems.",In: Proceedings of the 14th Workshop on Mobile Computing Systems and Applications; HotMobile '13. New York, NY, USA: ACM. ISBN 978-1-4503-1421-3; 2013, p. 11:1–11:6.

9. Hamed Taherdoost, "Decision Making Using the Analytic Hierarchy Process (AHP); A Step by Step Approach", International Journal of Economics and Management Systems,vol2 , 2017

10. Junshe Wang, Jinliang Liu, and Hongbin Zhang,"Access Control Based Resource Allocation in Cloud Computing Environment", International Journal of Network Security