International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Implementing Trust Management in Pervasive Computing Environment Depending on Trustworthiness Equation

Dr. Mohammed Najm Abdullah[1], Atheer Marouf Al-Chalabi[2]

[1]Computer Engineering Dept., University of Technology, Baghdad, Iraq

[2]Research Scholar, Informatics Institute for Postgraduate Studies, ICCI, Baghdad, Iraq

Abstract: ***The growth in the development of technical devices carried the world to the new category in the field of telecommunications called pervasive computing environment. The security measures boundaries in pervasive computing environment is vulnerable to the several challenges on the security level because the interaction between any entities or devices might be happened at anywhere and anytime, and without prior knowledge of the entities which are available in this environment. To overcome this, trust is one of the most significant means to improve security. In this paper, we propose a trustworthiness evaluation method using the simulation of the trust equation which is used in the market and business management, based on past and present entity interactions, and then, we compare it with another trust model to show the range of its sensitivity and quality to estimate the trust for the sharing process, and conclude that the propose method is more friendly with pervasive computing environment.***

Keywords: Pervasive computing environment (PCE), trust value, trust management, trust equation.

1. Introduction

The growth in the development of technical devices which is entered into all details of people's daily lives (mobile devices, sensors, wireless networks and communications technology) carried the world to the new category in the field of telecommunications called pervasive computing[1, 2].

The terms of Pervasive Computing Environment (PCE) refer to the incorporation of the mobile devices with wireless networking technologies to find out and access services to the surrounding devices which are contributing to create this environment through their interaction with each other's [3-5].

The interaction between entities(devices) in the pervasive environment might be happened at anywhere and anytime, and without prior knowledge of the entities which are available in this environment. So, the sharing information in this environment will be vulnerable to the several challenges on the security level, notably the ability of access unwanted users to this information. Therefore, the security measure boundaries are very difficult to define it.To overcome this, trust is one of the most significant means to improve security which considered as a cornerstone for information privacy and security. The information privacy depends on the trust level between the information receivers and information owners[6-8].

In the pervasive computing environment, the access control policies combined with a cryptographic algorithm to enforce the security policies. These policies are based on their trust negotiation and trustworthiness which includes: user identity, the number of interactions and the location of interaction from where the request originate [9].

Previous literature in trust models for access control presented approaches that either used long time consuming (to calculate and evaluate the trust value by considering different factors for decision making, such as privacy, security and context), or used trust evaluation model that doesn't serve the concept of PCEs.In [10] the authors review the possibility to integrate the trust into the security infrastructure of pervasive computing and this provides flexibility to access control and authentication for known users, and improving trust architecture through including prohibitions, entitlements, obligations and the ability to delegate them. In[11] the authors presenting an approach based on the cloud theory to solve uncertain problems between entities in pervasive computing environments as a cloud, using an algorithm to compute aggregated trust clouds and propagated trust clouds. In [8] the authors proposed trust based access control scheme which is built on the trustworthiness of the devices. They achieved access control depending on the evaluation of the trust value at the request of services, and formulated the recommender and the trustworthiness of the user using fuzzy logic and fuzzy set. In [12-14]they present and illustrate the importance of combining the trust factor with the security and privacy factors in one comprehensive framework to integrate the privacy management framework.In [15, 16] they introduces fuzzy logic into the definition and evaluation of trust, and then they provides a representation of fuzzy rules. In [17]the authors proposed A fuzzy logic based technique for the indirect trust computation in pervasive computing environment which measures the credibility of recommendation to determine the influence of the honesty of each recommendation. The rest of this paper is organized as follows: Section 2 gives a brief explain about how the trust equation simulated and has been evaluated, Section 3 gives a summary explanation of the trust evaluation based on access control scheme which is comparable with our proposal in the section 4, and then, theconclusion are shown in the section 5.

2. The Proposed Trust Equation

It is a mathematical model that devised to illustrate the trace of the (credibility (C), reliability (R), intimacy (I) and self-orientation (S)) on the trust value. Those elements were collected in one equation as shown in (eq. 1), which considered as a major components to determine the amount of trust in the marketing management[18].

$$Trust = \frac{C+R+I}{S} \quad (1)$$

Where:
C: Credibility, R: Reliability
I: Intimacy, S: Self-orientation

2.1 Trust equation concepts

a) Credibility
It is a positive characteristic of the communicator's which effect on the acceptance of the believability of the message by the recipient. Trustworthiness and the expertise are two key components to define the credibility[18].

b) Reliability
It is the reliance amount of the object based on the amount of confidence that built as a result of the familiarity feeling, and the appropriate behavior during the interaction process with the actions[18].

c) Intimacy
It refers to the safety feeling amount with the interacting objects[18].

d) Self-orientation
It is an important factor that enters with other trustworthiness equation factors to indicate the amount of object's focus[18].

2.2 Trust computations factors

There are ten factors involved in trust computations that are grouped into two groups according to the location which are:

a) In this location:
1) Identity of the user
2) The number of sent and received files (Nlsr).
3) The number of positive secrete transaction (Pnp).
4) The number of positive negative transaction (Nnp).
5) The interaction (Nit).
6) The sequence number of repeated error (ERRnum).
7) The maximum file share number with the available entities (MAX).

b) In all locations:
8) The number of re-established connection (Re).
9) The number of error request or response (Ne)
10) The number of sent and received files(NSRf).
11) The interaction (Nat).

The identity of each interaction entity (device) is stored in the database which they have. The identity mostly is the device MAC address. The table of the database contains Information about the smart device ID, the number of sent and received files in this and all locations, the number of positive and negative secrete transaction, the interaction in this and all locations, the maximum numbers of shared filewith the available entities, the number of re-established connection, the number of error request or response and also the threshold value of the reliability (Tr)which the initial threshold value is 0.5 and the maximum value is equal to 1,and the previous trust that has an initial value equal to 0.5.

$$Trust_i = Trust_{i-1} + \frac{C+R+I}{S \times 3} \quad (2)$$

2.3 Simulation of trust equation

Trust equation is simulated as the following:
The trust equation will be:

a) Credibility

$$C_i = \frac{Pnp-Nnp}{NSRf \geq 1} \times R_{i-1} \quad (3)$$

Where:
C_i: Current credibility.
R_{i-1}: previous reliability.

b) Reliability

$$R_i = \frac{1}{100} \times \left(R_{i-1} + \frac{NSRf-Ne}{Nat} \times 0.95\right) \quad (4)$$

Where:
R_i : Current credibility.
R_{i-1}: previous reliability.

c) Intimacy

$$I\left(\frac{NSRf}{Max \geq 1} + \frac{Nit}{Nat} - \left(1 - \left(2 \times \frac{\sqrt{\left(Nlsr - \frac{NSRf}{2}\right)^2 + \frac{NSRf}{4}}}{(NSRf) \geq 1}\right.\right.\right. \quad (5)$$

d) Self-orientation

$$S = \frac{Re + Ne}{(NSRf + Re + Ne)} \quad (6)$$

Trust calculation
Trust value is calculated using an algorithm as shown below:

Algorithm 1 TrustEvaluation

```
1: function TRUSTEVALUATION(MACaddress, Request)
2:     ignorList ← get Ignor List From Database
3:     if !(is (MACaddress) in ignorList) then
4:         if !(is (MACaddress) in the Database) then
5:             insert MACaddress into Database and put reliability value = 0.5
6:         endif
7:         Get MACaddress parameters from the Database
8:         TrustValue ← calculate trust value using parameters
9:         if !(is (Request) is right) then
10:            if (TrustValue ≥ TrustFile) then
11:                Sharing the information with the device that has MACaddress
12:                Update parameters in the Database
13:            else
14:                TrustValue ← calls for evaluation the trust of (MACaddress)
                              from neighbor devices
15:                if (TrustValue ≥ TrustFile) then
16:                    Sharing the information with the device that has MACaddress
17:                    Update parameters in the Database
18:                endif
19:            endif
20:        else
21:            Send Request error to (MACaddress)
22:            Update parameters in the Database
23:        endif
24:    endif
```

The smart device in an interaction environment acts as a client or server. It acts as a client when it request a specific information or it has an information to share with other devices in the environment. Knowing the fact, before the

sharing process, the user sets as set of trust conditions rules on the information that is prepared to share process. So, the interaction share process doesn't happen unless the information trust conditions is met.

The smart device acts as a server when it receives any information from the interacting client device within the border of the spatial interaction.

Each smart device has an ignore table in its embedded database which is contained on the MAC address of the devices which is suspiciously reacted. So, any interaction happens with any device, the first process of the device is to check the interacted MAC address with the ignore table. If the MAC address does not found in ignore table, the trust calculation operation will start as shown below:

a) Trusted node interaction

The trust calculation in the smart device will start directly, if the interacting device has a previous interaction with it. If the trust value of the interacting device is greater than or equal to the trust value of the information which is prepared to share and the ruleshas beenoccurring (if the condition of sharing process be confined to the location), then the sharing process will start and update the parameters of the trust. Otherwise, the smart device will request to all interacting devices in the neighbor in the same location to provide it with the trust value of the interacting device (which has this MACaddress). All devices in the neighbor will equip it with the trust value rating (of the MACaddress interacting device) as shown in the (figure 1). The server device (smart device) will take the average of these rating as a trust value as shown in the (eq. 7) below.

$$new\ Trust = \frac{\sum_{i=1}^{n}(trust\ rating)_i}{number\ of\ devices\ rating} \quad \ldots\ldots\ldots (7)$$

After that, the server device checks if the new trust value is greater than or equal to the trust value of the information to start the sharing process and update the trust parameters in the database, otherwise, there is no process between them until the conditions done.

b) New node interaction

The trust calculation will start with the threshold value which is equal to 0.5, and the interaction share process will accrue with it as it isillustrated in section (a) from this topic.

c) Untrusted node interaction

This device is considered as untrusted because its trust value is less than the minimum threshold, and will not happen any interaction (sharing process) with it until the trustworthiness proven through better interaction (without suspicious interact or get good rating by neighbor device).

d) Suspicious node interaction

The device is considered as suspicious device when it is repeated sequence error request at the same time for a period of time and this device will block at the server device and insert it to the ignore table in the database when it exceed the upper limit of errors which is equal to 0.5.The

$$MaxErr = 1 - e^{\log\left(1 - \frac{ERRnum}{NSRf}\right)} \quad \ldots\ldots\ldots\ldots (8)$$

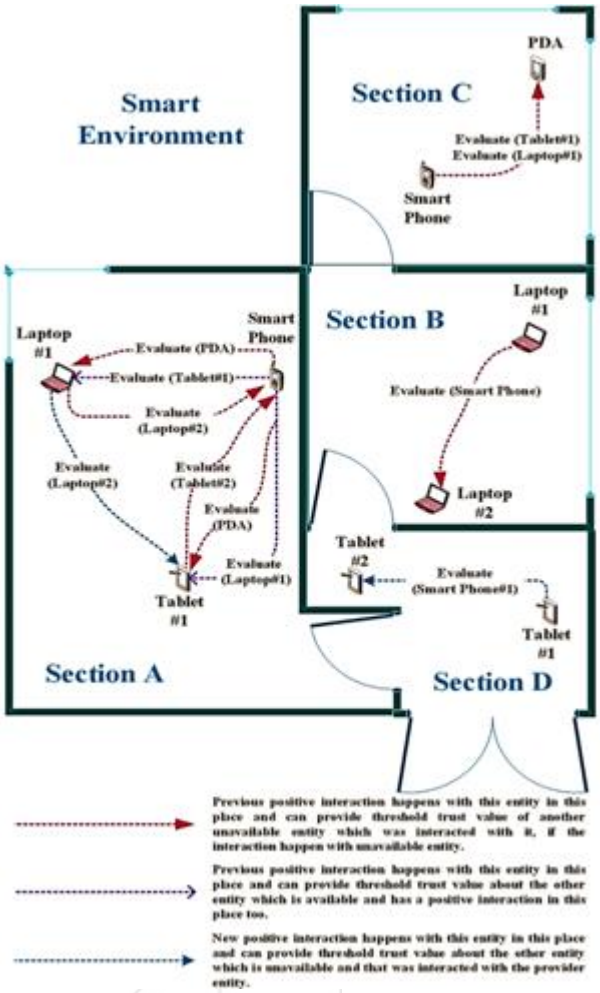

Figure 1: Smart Building Environment

maximum error has been calculated as shown in the (eq. 8) below.

3. Comparison Method: Trust Based Access Control Scheme

The Trust Based Access Control Scheme[8].is based on the trustworthiness of users. The user must be known in the environment which is interacting with it by its device. The user must register his device in the global database on the server to manage the operation in the smart environment.

This technique, which is proposed based on Factors that is involved in Trust Computations which are:
1) Identity of the user
2) Acceptance level
3) Access Rights
4) Success rate
5) Location
6) Initial Trust value
7) Recommender's best trust value

The Trust value is calculated by this method using the steps as it's shown below:
Step 1: Get the initial trust value of the user, identity of the user (UDID number of the device) and time of request (Tr), role (r), acceptance level (al)

Step 2: if the identity is available then retrieve other information such as access rights and location, time of request carried out (Ti)

Step 3: Get the success rate of transaction and time of transaction.

Step 4: If the identity is not available then requester selects the list of recommender and their related information from the global table.

Step 5: get all recommender's trust value for the requested service. Identify the most appropriate trust value from the entire recommender list.

Step 6: If the recommender is a trustworthy entity then find from the domain set of the user, the role and access rights using fuzzy logic predicates.

4. Result and Discussion

In this paper, we take the scenario table which has been implemented in the comparative method [8] (that was explained briefly above) with our proposal and applied it on our proposal as shown in (table 1).

We took a node (such as node A) that has a table in its database which contains (device ID, Nlsr, NSRf, Pnp, Nnp, Nit, Na, MAX, Re, Ne, Tr, $Trust_{i-1}$), and it presented at this location, and has an interaction with the neighbor nodes in the same location or in another location, then we took the (node reference number which is considered as MACaddress, number of request which is considered as the Nit/Nat, number of acceptance which is considered as Nlsr/NSRf) from the (table 1). We entered this value into our proposal equation, taking into consideration that the node which acts as a user considered as an interactive device that always interacting with node A, while the node which as a guest considered as an interactive device that interacting with node A for the first time in this location and has a previous interaction with it in another location.

The trust value and the update trust value in our proposal will be different from the trust value which is mentioned in (table 1) as it is shown in the (table 2).

The updated trust value in our proposal and the previous trust,illustrated in the (figure 2), and the comparison between our method and the other method (which is mentioned above), shown in the (figure 3).

Table 1: The scenario table in the comparison method

Role	Number of Hops	Updated Trust value	Average Recommender Trust value	Ratio of acceptance / rejection	No. of Acceptance	No of Request	Node reference number
user	4	1	0	1	2	2	11
user	5	1	0.9	0.833	5	6	13
user	7	1	0.9	0.8	4	5	24
user	4	1	0.82	0.8	8	10	345
guest	3	0.65	0.45	0.25	1	4	51
guest	8	0.45	0.43	0.333	5	15	406
guest	10	0.43	0.4	0.521	12	23	507
guest	4	0.6	0.45	0.5	6	12	312
guest	8	0.5	.	0.533	8	15	211
guest	25	0.4	0.5	0.333	2	6	200
guest	12	0.4	0.48	0.4	2	5	214
guest	12	0	0.2	0.2	1	5	310

Table 2: The table of node A

device ID	Re	Ne	NSRf	Nlsr	Pnp	Nnp	MAX	Nit	Nat	Tr	$Trust_{i-1}$%	Trust%
11	1	0	2	2	2	0	8	2	2	0.52	50.51	51.6
13	1	0	5	5	5	0	8	6	6	0.53	55.59	58.49
24	1	0	4	4	4	0	8	5	5	0.53	53.35	55.6
345	1	0	8	8	8	0	8	10	10	0.55	66.46	71.5
51	1	0	1	1	1	0	8	1	4	0.5	50.17	50.6
406	1	0	5	1	1	0	8	1	15	0.51	52.2	53.5
507	1	0	12	1	1	0	8	1	23	0.54	65.19	68.5
312	1	0	6	1	1	0	8	1	12	0.52	52.96	54.6
211	1	0	8	1	1	0	8	1	15	0.53	55.84	58.2
200	1	0	2	1	1	0	8	1	6	0.51	50.36	51
214	1	0	2	1	1	0	8	1	5	0.51	50.3	50.9
310	1	0	1	1	1	0	8	1	5	0.5	50.22	50.6

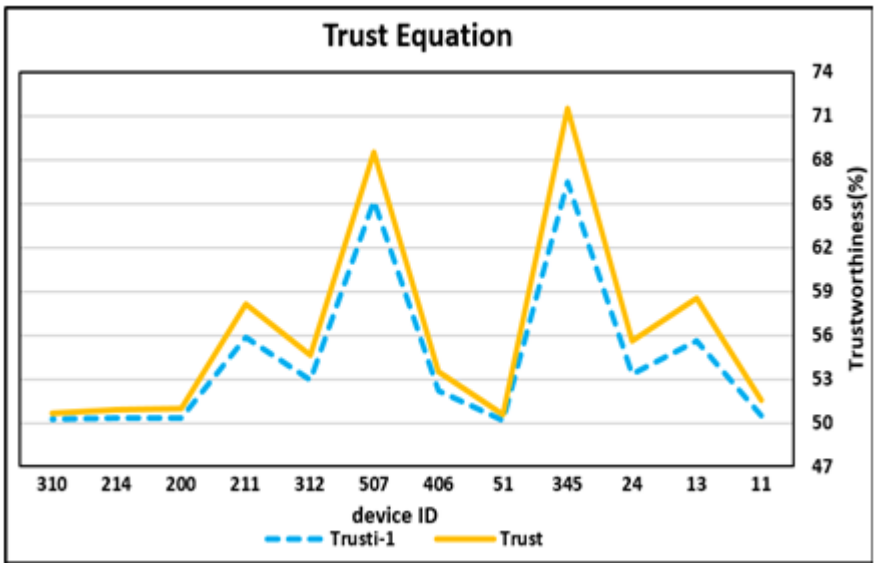

Figure 2: updated trust value and the previous trust using trust equation

5. Conclusion

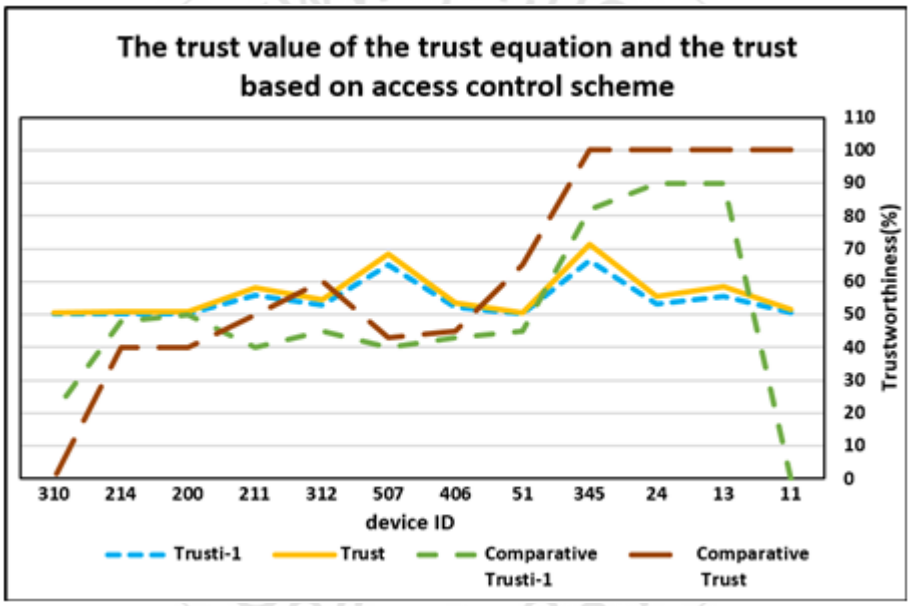

Figure 3: The comparison between trust equation method and trust based control scheme method

In this paper, a new method has been proposedusing trust equation through simulated the parameter ofequation (the smart device ID, the number of sent and received files in this and all locations, the number of positive and negative secrete transaction, the interaction in this and all locations, the maximum file share number with the available entities, the number of re-established connection, the number of error request or response, previous reliability and the previous trust). The proposal equation tested using the parameter which has been used in the literature review "Trust Based Access Control Scheme for Pervasive Computing Environment" and compare the result with this literature. The simulation of the trust equation clarified that the process of building trust value is similar to the human behavior in the process of building trust between them when they are interaction in real life. The result shown that the effectiveness amount of the amount of the smart device presence in the current location, the behavior of its interaction and the amount of the trust from the previous experiences with it, on the gradual growth of the trust. As a result, the mechanism of our proposal is more interactive with the trust cases and the trust building than the previous literature, which either built a blind trust or collapsed the trust without any justification.

References

[1] D. M. N. Abdullah and A. M. Al-Chalabi, "Performance Assessment of RSA, ElGamal and Proposed DHOTP for File Security in Pervasive Computing Environment," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, pp. 1-12, 2016.

[2] M. N. Abdullah and A. E. Korial, "Planning the Path and Avoidance Obstacles for Visually Impaired/Blind People," *IOSR Journal of Computer Engineering* vol. 17, pp. 147-151, 2015.

[3] I. Mezgár and S. Grabner-Kräuter, "Privacy, Trust, and Business Ethics for Mobile Business Social Networks," *Handbook of Research on Business Ethics and Corporate Responsibilities*, p. 390, 2015.
[4] A. E. Korial and M. N. Abdullah, "Novel method using beacon and smart phone for visually impaired/blind people," *International Journal of Computer Applications* vol. 137, pp. 33-39, 2016.
[5] A. E. Korial and M. N. Abdullah, "Indoor Navigation for Visually Impaired/Blind People Using Smart Cane and Mobile Phone: Experimental Work," *Journal of Information Engineering and Applications* vol. 6, pp. 31-40, 2016.
[6] A. Al-Karkhi, A. Al-Yasiri, and N. Linge, "Privacy, trust and identity in pervasive computing: a review of technical challenges and future research directions," *International Journal of Distributed and Parallel Systems (IJDPS)*, vol. 3, pp. 197-218, 2012.
[7] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment," presented at the Proceedings of the 1st International Conference on Cloud Computing, Springer-Verlag, Beijing, China, 2009.
[8] A.M.Hema and K.Kuppusamy, "Trust based access control scheme for pervasive computing environment," in *Recent Trends In Information Technology (ICRTIT), 2012 International Conference on*, 2012, IEEE, pp. 157-161.
[9] D. M. Priyadharshini, P. Anitha, and C. Janani, "Adaptive Secure Document Access Mechanism in Cloud," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 6, pp. 448-451, 2017.
[10] L. Kagal, T. Finin, and A. Joshi, "Trust-based security in pervasive computing environments," *Computer*, vol. 34, pp. 154-157, 2001.
[11] J. Niu, M. Yuan, R. He, and J. Hu, "A novel cloud-based trust model for pervasive computing," in *Computer and Information Technology, 2004. CIT'04. The Fourth International Conference on*, 2004, IEEE, pp. 693-700.
[12] R. K. Chellappa, "Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security," *under submission*, 2008.
[13] M. Riguidel and A. Hecker, "Security, Dependability and Trust in the Future Internet," *Asia Future Internet*, 2008.
[14] J.-L. A. MANAN, M. F. MUBARAK, M. A. M. ISA, and Z. A. KHATTAK, "Security, Trust and Privacy–A New Direction for Pervasive Computing," *Information Security*, pp. 56-60, 2011.
[15] Z. Wu and A. C. Weaver, "Application of fuzzy logic in federated trust management for pervasive computing," in *Computer Software and Applications Conference, 2006. COMPSAC'06. 30th Annual International*, 2006, IEEE, pp. 215-222.
[16] M. Rehak, L. Foltyn, M. Pechoucek, and P. Benda, "Trust model for open ubiquitous agent systems," in *Intelligent Agent Technology, IEEE/WIC/ACM International Conference on*, 2005, IEEE, pp. 536-542.
[17] N. Iltaf and A. Ghafoor, "A fuzzy based credibility evaluation of recommended trust in pervasive computing environment," in *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*, 2013, IEEE, pp. 617-620.
[18] D. H. Maister, R. Galford, and C. Green, *The Trusted Advisor*: Simon & Schuster UK, 2000.