Flexible Decision for Trust Value in Pervasive Environment

Ajay Mohan
Ph.D Research Scholar
Department of CSE,
M.M. Engineering College,
Maharishi Markandeshwar University,
Mullana (Ambala), Haryana,India
Email id: ajaymohangoel@gmail.com

Dr. Neera Batra
Associate Professor
Department of CSE,
M.M. Engineering College,
Maharishi Markandeshwar University,
Mullana (Ambala), Haryana, India
Email id: batraneera1@gmail.com

Abstract**—**The ability to access information and software applications anytime and anywhere is known as Pervasive Computing. Computing and communication capabilities are embedded in the infrastructure and disappeared from human users. In contrast to desktop computing, ubiquitous computing can occur using any device, in any format and in any location. This paper defines how solutions which already exist are sufficient in order to control processing to the services and for this objective, architecture is implemented called as Distributed access. In this paper, two issues are discussed: (1) to check the authorization of a user by implemented controlled architecture (2) trust value calculation which will help in enhancing the security for a user.

Keywords: *Pervasive computing, Trust Value in Pervasive Environment.*

*****

I. INTRODUCTION

Pervasive computing is omnipresent computers in the surroundings by using large number of objects in day to day life. It integrates the objects in such a way that users are not even aware of their physical presence. But a number of challenges are there before it can be applied on any system and these challenges are related to security and privacy. The problems are faced in terms of poorly defined security parameters. So, it requires security measures which are based on contextual information [2]. Traditional methods for authentication that focuses on security issues are context-insensitive and are not able to adapt to the rapidly changing need of context parameters. Therefore, flexible trust-based authentication is one of the major topics which need to be addressed [4]. However, the enormous amount of personal information gathered makes privacy a main concern in pervasive computing [3].

II. RELATED WORK

In this paper, Changu suh, Young-Bae ko, Cheul-Hee Lee and Hyung-Joon Kim suggests the new intelligent home scenarios based on new and embedded systems. In this, they introduce a new smart sensor device called as ZigbeX. Since it is operated with a battery (AA) for the portability, we carefully design to consider low power consumptions. It can basically sense the physical photo (light), temperature and humidity. However, we think these sensing abilities are not sufficient for the ubiquitous house environments. So, we develop the additional sensing boards have the air pressure sensor, acceleration sensor, gas sensor and motion detection sensor. Moreover, to control the general electronic householders, we design actuator board as an electronic switch [10]. The additional boards are equipped and controlled by our smart sensor devices. Future work of this paper is to develop the position system for exactly detecting the human location by using an ultrasonic technique.

In this paper, Dae-Man Han and Jae-Hyun Lim designs smart home device descriptions and standard practices for demand response and load management "Smart Energy" applications needed in a smart energy based residential or light commercial environment [16]. The control application domains included in this initial version are sensing device control, pricing and demand response and load control applications. This paper introduces smart home interfaces and device definitions to allow interoperability among ZigBee devices produced by various manufacturers of electrical equipment, meters, and smart energy enabling products.

Fahad T. Bin Muhaya proposed a smart card and password based mutual authentication scheme under trusted computing and they claimed that their schemes can resist all types of attacks [17]. This paper first analyses the stolen smart card attack and then propose an enhanced mutual authentication scheme for trusted computing. Proposed scheme includes registration phase, login and authentication phase, update phase and finally security analysis.

Roy Campbell [5] describes that security and privacy issues for pervasive computing are not well defined till now. This paper focuses on security of a system which has not provided by previous distributed computing. It is required to share resources and collaborate new type of interaction among users as well as physical and virtual world.

Almenarez proposed a Pervasive Trust Model which is a computational trust model and it is implemented on a wide range of pervasive devices [8] considering two kinds of trusts, direct trust and recommendation trust. A recommendation protocol is defined to recommend an entity the trust values of other ones. If an entity wishes to interact with another one, it uses this protocol to acquire that entity's trustworthiness degree. Antonio Sapuppo enables social networking benefits to physical world by making ubiquitous networking services that become available by means of wirelessly interconnected smart devices [18].

An Omnipresent Formal Trust Model (FTM) which presents a flexible trust model incorporating a behavioral model to handle interactions is proposed by M. Haque [9]. However, it fails to handle situations where a malicious user can launch strategic attack as the trust value is not modified considering the old behavior pattern. In a similar way, an approach to establish trust automatically has been proposed by Seamons [11] wherein trust is established incrementally by exchanging credentials and requests for credentials, an iterative process known as trust negotiation. With automated trust establishment, strangers build trust by exchanging digital credentials. A trust negotiation strategy controls the exact content of the messages exchanged during trust negotiation.

Sheikh [12] pointed out a service discovery model which is needed that can resolve security and privacy issues. Nature of pervasive environment is volatile that’s why complex algorithms and fixed infrastructure is not used. A trust model secure service discovery model is presented in this paper for a pervasive environment. This model is hybrid as it allows secure and non-secure service discovery. It handles the communication and security issues.

Ray Bertino [13] argued an inherent conflict between trust and privacy because both depend on knowledge about an entity. The more knowledge a first entity knows about a second entity, the more accurate should be the trustworthiness assessment, the more knowledge is know about this second entity, the less privacy is left to this entity. This conflict needs to be addressed because both trust and privacy are essential elements for a smart environment. They proposed a solution to achieve the right trade-off between trust and privacy by ensuring minimal trade of privacy for the required trust. They proposed a model for privacy/trust trade based on link ability of pieces of evidence. They proposed to use pseudonymity as a level of indirection, which allows the formation of trust without exposing the real-world identity. They introduced the liseng algorithm to ensure that the minimal link ability principle is taken into account Equations.

III. PROBLEM FORMULATION

There is a need to calculate flexible trust in situations when the requesting entity has a previous experience with the service and requested entity has the flexibility to take decision up to some extent then access rights will be given to third party but this access is not static [1]. If authorized user will allow third party user to use service only if he is satisfied with third party user, but in case, third party user cant fulfil the requirement to gain access, in that case authorized user is having an option named as flexibility parameter, on the basis of that authorized user will decide if third party is not having any problem, then it will provide some flexibility to third party on own basis.

Steps for Flexibility trust value:

1. If user is new

- Check whether attempt is positive or negative.
- If negative, then assign initial flexible trust value -0.5. Again check, new attempt made or not.
- If yes, check positive or negative, if negative then access rights will not be provided. If positive, check total flexible value and then decide.
- If first attempt is positive, assign flexible trust value +0.5.

2. If user is old, then check attempt is positive or negative.

- If positive, then access rights will be provided.
- If negative, check his/her feedback and provide flexibility level, then check its decision.

3. Stop

Third party user can use a service only if he has been provided the right to do so or only if an authorized user has delegated the right to him, he can delegate all rights that he has the permission to delegate. Else rights can be revoked anytime [7]. Third party user can send request to authorized user to delegate to him the right to access certain services. Authorized user will allow third party user to use the services only if he is satisfied with third party user credentials. He can also provide limited access to him for a certain period or persons to whom third party can re-delegate the right. When third party user makes requests to the security agent who is controlling the service, they need to attach their credentials and ID certificate or a delegation certificate in order to request the security agents who may generate authorization certificates that user can employ as tickets to access a certain service. The trust models used are categorized as:

1. Pervasive Trust Model: Trust relationships are established between entities. These entities are autonomous and few are mobile. These entities can be persons, organizations, departments, etc. and its devices are laptop, mobile and PDA’s. Each entity manages its own security.
2. Formal Trust Model: The Formal Trust Model (FTM) is a combination of Direct Trust Unit and Recommended Trust Unit. Direct trust is formed through direct interactions among the nodes. The satisfaction level of the direct interactions is evaluated using behavior model whereas recommended trust protocol is used to calculate the recommendations to form recommended trust.

A. Problem Formulation

The Problem Formulation is designed to calculate flexible trust value of each entity, analyze the behavior pattern of entity and provide access decision for security purposes. As good feedback increases, Flexibility value also increases and its value decreases as value of bad feedback decreases. A bad feedback decreases the flexibility value by 0.5 that is dependent on the sensitivity of the relationship. An entity can make wrong behavior intentionally or unintentionally. This model supports good trust history. An entity, with a superior trust history has larger growth in flexible trust value with a good behavior and less penalty in flexible trust value with a bad behavior via an entity with a bad trust history.

B. *Trust Value Calculation*

Whenever a new entity joins any pervasive environment, it has neither past experience nor any reference to advocate it initially in order to establish a trust value for interaction. Formulation of an opinion, in this case requires the model to associate itself with risk and assign an initial ignorance value, which can be updated as additional information that becomes available after observing the entities behavior during the interaction [6]. Each service maintains the following information for each entity that is updated during trust evaluation:

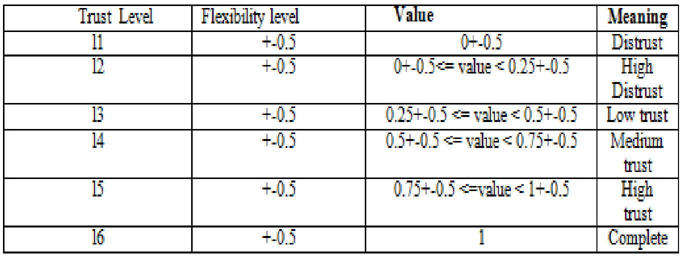
1. Total number of interactions of entity
2. Total number of positive interactions of entity
3. Total number of negative interactions of entity

IV. PROBLEM SOLVING TECHNIQUE

These problem solving techniques observe the behavior of the entity and increment or decrement flexible trust level depending upon positive or negative attempts initially made by entity before completely trusting or distrusting the entity.

A. *Growth/ Decline in Trust Value*

The Initial flexible trust value for positive attempt is assumed to be 0.5 and for negative attempt is -0.5. Depending on the outcome of the interaction, a positive feedback is rewarded by increasing service trust in the entity and negative feedback is penalized by reducing the service trust in the entity [14].The updated trust value is calculated using the previous trust value and impact of current interaction in the form of reward/penalty rate using following equation:



Trust Level	Flexibility level	Value	Meaning
l1	+-0.5	0+-0.5	Distrust
l2	+-0.5	0+-0.5<= value < 0.25+-0.5	High Distrust
l3	+-0.5	0.25+-0.5 <= value < 0.5+-0.5	Low trust
l4	+-0.5	0.5+-0.5 <= value < 0.75+-0.5	Medium trust
l5	+-0.5	0.75+-0.5 <=value < 1+-0.5	High trust
l6	+-0.5	1	Complete

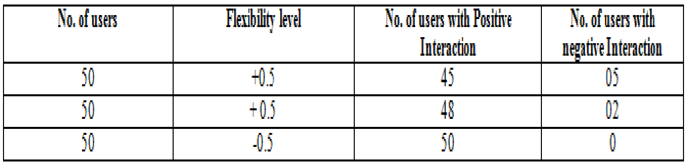
Table 1: Flexibility Levels and corresponding Trust Values

Table 1 shows the flexibility Levels and corresponding Trust values. The trust value shows the level of trust; a service has in an entity. Various Trust levels with flexibility level taken into consideration have been shown along with their range, meaning for each value and description for each trust level [14].

V. IMPLEMENTATION AND USER INTERACTION

Experiments are conducted in order to gather the information regarding the satisfaction level with the working of proposed work. The proposed work is subjected to be tested with 50 users belonging to different categories and different trust levels. 20 users belong to the well known (including family and Friends) category whose trust level is the highest and 20 other users belong to the intermediate(including office people from all departments) category whose trust level is medium and other 10 users belong to very less known category(Technicians and other known people) whose trust level is minimum. All the users are not familiar with the working environment of the proposed work. All the users are asked to avail the provided resources and their positive and negative interactions are tested and shown in Table 2. Results are largely analyzed separately for three different users levels and later combined to get comparative results which concludes that the proposed work checks the trust level with great efficiency and less complexity. On the basis of above explanation, a new table is designed to check the number of users who are interacting positively and the number of users who are interacting negatively. We consider 50 users for this test and on the basis of that we are calculating their corresponding trust values.

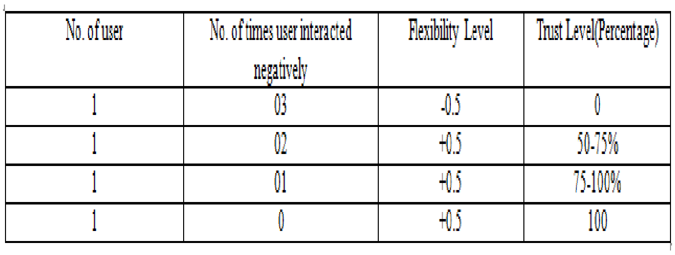
The results for access rights given to all the users from three categories are shown below in table 2.



No. of users	Flexibility level	No. of users with Positive Interaction	No. of users with negative Interaction
50	+0.5	45	05
50	+0.5	48	02
50	-0.5	50	0

Table 2: Users with their corresponding interactions

On the basis of above table, a new table has been derived to check how much number of times, each single user is not interacting positively and on the basis of that we will calculate his/her trust value.



No. of user	No. of times user interacted negatively	Flexibility Level	Trust Level(Percentage)
1	03	-0.5	0
1	02	+0.5	50-75%
1	01	+0.5	75-100%
1	0	+0.5	100

Table 3: Single User with his/her assigned corresponding Flexibility Level

VI. RESULT ANALYSIS

The proposed model observes the behavior of the entity. It also increments and decrements his/her trust level initially depending upon positive/negative attempts made by an entity before completely trusting or distrusting the entity [15].

A. *Growth/ Decline in Trust Value*

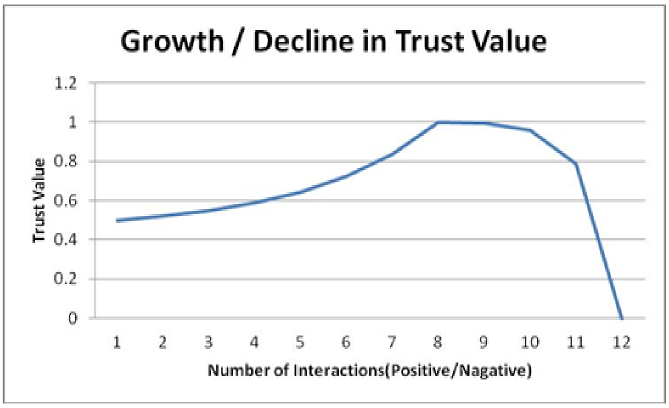


Figure 1: Growth/Decline in Test Value

Figure 1 shows trust establishment of an entity with positive/negative behavior .When positive interactions are made by the user; the trust graph shows a slow growth in trust value whereas for negative interactions, the trust value declines fast comparatively.

B. *Effect of Flexibility Level in Trust Value*

Trust/distrust rate after each interaction is controlled by service security level. The slope of trust increment and decrement is dependent upon the security levels of the requested service. High security level demands pro longed positive interactions to achieve maximum trust and vice versa. The most secure service will have security level 0.5 whereas the least secure service may have the security level equal to 3. The effect of security level on trust value has been depicted in fig 2.

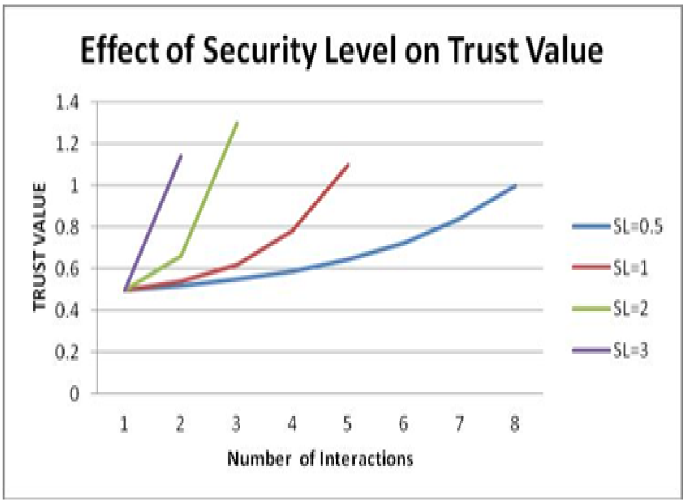


Figure 2: Effect of Flexibility Level on Trust Value

VII. CONCLUSION

The present work motivates the need for developing new trust model for pervasive computing applications. It also proposes a description to calculate trustworthiness of an entity. This work calculates the trust value for security driven third party access in pervasive computing .It supports flexible adjustment in trust value based on entities behavior.

Conclusion drawn on the basis of testing of the proposed work with 50 end-users can be summarized as: the compatibility and easiness to work with the proposed work is found to be almost similar for all users. Future work focuses on extending this work for secure file transfer of different formats such as text file, image file etc.

REFERENCES

[1]. Hamed Khiabani, Jamalul-Lail, Ab Manan, Zailani Mohamed Sidek, “A Study of Trust & Privacy Models in Pervasive Computing Approach to Trusted Computing Platforms”, Technical Postgraduates (TECHPOS), IEEE International Conference, vol. 4, pp. 1-5, 2009.

[2]. K. Ranganathan, “Trustworthy Pervasive Computing: The Hard Security Problems”, In the Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, IEEE Computer Society, vol. 2528, pp. 117-121, 2009.

[3]. L. Kagal, T. Finin, A. Joshi, “Trust-Based Security in Pervasive Computing Environments”, Journal of Computer, vol. 34, pp. 154-157,2001.

[4]. Munirul Haque and Sheikh Iqbal Ahamed, “security in Pervasive Computing: Current Status and Open Issues”, International Journal of Network Security, vol. 3, pp. 203–214, 2006.

[5]. Campbell R., Al-Muhtadi J., Naldurg P., Sampemane G., Dennis Mickunas M, “Towards Security and Privacy for Pervasive Computing” Software Security — Theories and Systems. Lecture Notes in Computer Science, vol. 2609. Springer, Berlin, Heidelberg, 2003.

[6]. M. Weiser, “Some Computer Science Problems in Ubiquitous Computing”, Communications of the ACM, vol. 36, pp. 75-84, July 1993.

[7]. Neera Batra and Hemant Aggarwal, “Autonomous Multilevel Policy Based Security Configuration in Distributed Database”, IJCSI International Journal of Computer Science Issues, vol. 9, issue 6, November 2012.

[8]. F. Almenarez, A. Marin, C. Campo, and C. Garcia, “Ptm: A Pervasive Trust Management Model for Dynamic Open Environments”, In the First Workshop on Pervasive Security, Privacy and Trust PSPT04, vol. 34, pp. 1-8, 2004.

[9]. M. Haque, S I. Ahamed, “An Omnipresent Formal Trust Model (FTM) for Pervasive Computing Environment”, 31st Annual International Computer Software and Applications Conference, vol. 83, pp. 253-270, issue 2, 2007.

[10]. Changu suh et al., “The Design and Implementation of Smart Sensor-based Home Networks” Consumer electronics, IEEE Transactions, vol. 54, issue 3, pp 1177-1184, 2008.

[11]. E. Seamons, “Protecting Privacy During On-line Trust Negotiation”, In the Proceedings of the 2nd Workshop on Privacy Enhancing Technologies, San Francisco, California, vol. 9, pp. 927-931, April 2002.

[12]. Sheikh I Ahamad and Moushumi Sharmin, “A Trust based secure service discovery model in Pervasive Environment”, In Computer Communications, Elsevier, 2008.

[13]. Ray Bertino, Squicciarini, and Ferrari, " Anonymity Preserving Techniques in Trust Negotiations", In the Proceedings of 5th International Workshop on Privacy Enhancing Technologies (PET), Cavtat, Croatia, vol. 3856, pp. 93-109, 2005.

[14]. W. Winsborough and N. Li,"Towards Practical Automated Trust Negotiation", In the Proceedings of 3rd International Workshop on Policies for Distributed Systems and Networks, California, IEEE Computer Society, vol. 1592, pp. 92-103, 2002.

[15]. Suntae Kim, "A Quantitative and Knowledge based approach to choose security architectural tactics", Int. J. Adhoc and Ubiquitous Computing, vol. 18, nos. ½, pp. 45-53, 2015.

[16]. Dae-Man Han and Jae-Hyun Lim, "Smart Home Energy Management System using IEEE 802.15.4 and ZigBee", IEEE, vol. 56, issue 5, pp 735-740, 2010.

[17]. Fahad T. Bin Muhaya, "Security analysis and improvement of a mutual authentication scheme under trusted computing", Int. J. Ad-hoc and Ubiquitous Computing, vol. 18, nos. ½, pp. 37-44, 2015.

[18]. Antonio Sapuppo, Joao Figueiras, "Designing for Privacy in Ubiquitous Social networking", Int. J. Adhoc and Ubiquitous Computing, pp-102.