

Dynamic Trust Level Decision in Pervasive Environment

Sonali Goyal¹ and Neera Batra²

¹⁻²Maharishi Markandeshwar University, Mullana, Haryana
sonaliguglani21@gmail.com, batraneera1@gmail.com

Abstract—Pervasive computing expands the computing part in physical world. Goal of this technology is to create ambient intelligence where devices are embedded in the environment in order to provide connectivity all the time. However, not all information needs to be visible to all and needs to be shown only to the authorized users. This paper describes how existing solutions are sufficient for controlling access to the services and to achieve this objective, distributed access architecture has been implemented which supports complex and derived information. This paper focuses on two main issues: (1) to access the required information about a user that whether a user is authorized one or not and to achieve this goal an access controlled architecture has been proposed and implemented (2) to calculate the trust value which is helpful in reducing the influence of intruders by making a service prove that authorized client is accessing the information.

Index Terms— security in pervasive computing, trust evaluation, smart environment.

I. INTRODUCTION

Pervasive computing is a technology that pervades the user's environment by making use of multiple independent information devices (fixed and mobile, homogenous and heterogeneous) interconnected seamlessly through wired or wireless computer communication network. But a number of critical challenges need to be addressed before it can be widely deployed although it seems promising. These critical challenges include Security, Privacy and Trust. The problems are faced in terms of poorly defined security parameters and due to its dynamic nature. Moreover, pervasive applications and services use knowledge of surrounding physical and environments spaces. This requires security measures based on contextual information which must be adequately protected from security breaches [2]. Traditional authentication and access control mechanisms that focus merely on digital security are context-insensitivity i.e. they are unable to adapt to the rapidly changing need of context parameters and thus are inadequate for securing new exposures and vulnerabilities within pervasive computing environments. Therefore, trust-based authentication and authorization are one of the topics which have the potential to become the next hype [4]. The enormous amount of personal information gathered in pervasive computing makes privacy a major concern. Most personal information is confidential. Therefore, a pervasive computing environment must provide controlled access to confidential personal information.

II. RELATED WORK

Suntae Kim represented a quantitative approach used to choose security architecture tactics by using a knowledge base. This base is composed of specifications defined in RBML (Role based Meta modeling language) and their relationships. In this paper [15], tactic cost estimation is calculated, then computed based upon selection factors and finally analysis of sensitivity has been carried out. Kagal proposed a trust model for pervasive computing environments. This model is not a computational trust model and uses certificates to determine whether an entity is trusted or not. In this Kagal's suggested architecture [3], each environment is divided into some security domains and for each security domain a security agent is leveraged. The security agent is responsible for defining security policies and applying them in the corresponding domain. Interfaces of available services in a domain are also provided by its security agent. When an external user requests a service offered in a domain, he must provide a certificate from one of the agents which are trusted for the security agent of the domain. Then, he must send its request accompanying the acquired certificates to the security agent. The security agent checks the validity of the certificates and responses the user's request.

Dheerendra Mishra presented a system named as connected healthcare which is a platform to deliver clinical service door to door. It uses a smart card facility [16] which quickly identifies the incorrect IP and it satisfies all security attributes in order to achieve three factor authentications. This paper resists all the attacks by proposing a scheme consists of five phases: registration, login, authentication, session key computation and password change. 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.

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 F. Almenrez [9][10]. 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.

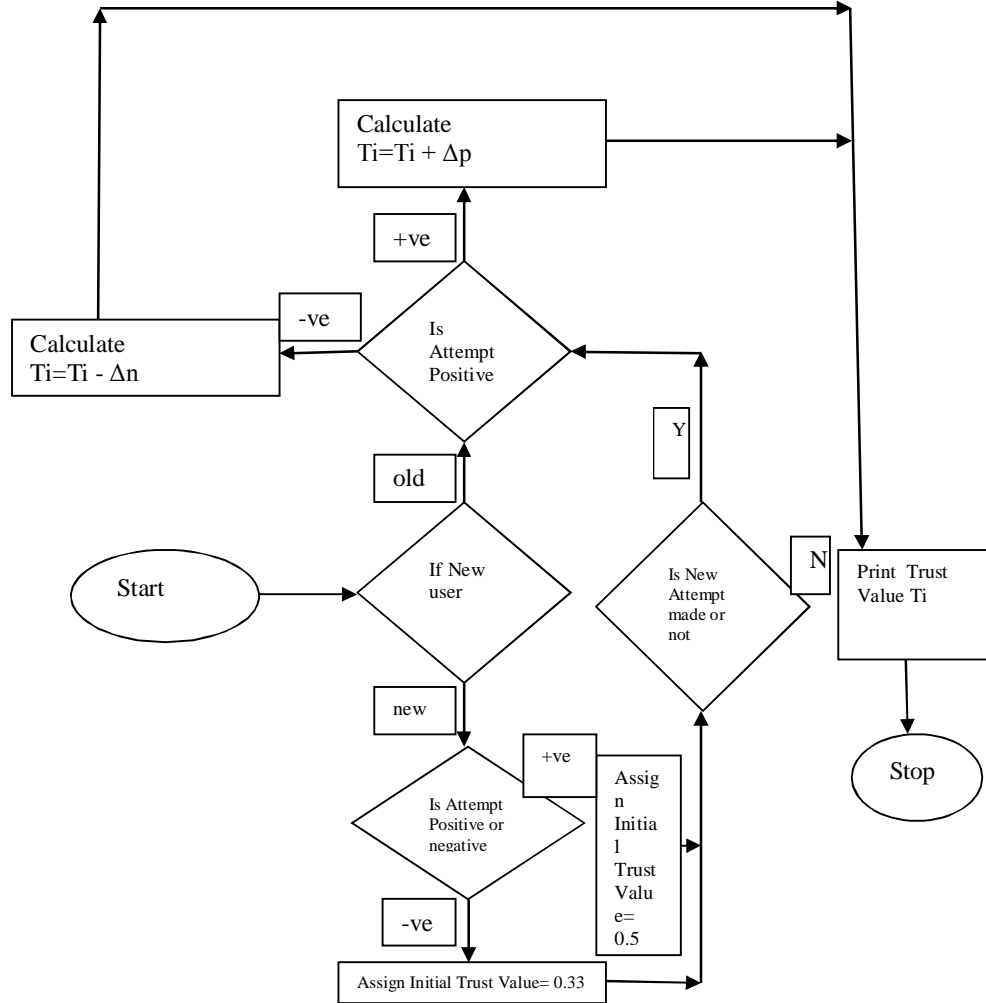
In a similar way, an approach to establish trust automatically has been proposed by Seamons [11] wherein trust is established incrementally by exchanging credentials and requests for credentials, an iterative process known as trust negotiation. With automated trust establishment, strangers build trust by exchanging digital credentials. A trust negotiation strategy controls the exact content of the messages exchanged during trust negotiation.

Winslett [12] pointed out how to establish trust without a trusted third party or a zero-knowledge approach; strangers will have to disclose some of their credentials. The question is whether it is safe to disclose sensitive credentials. Almost all existing research focuses on establishing trust using digital credentials. Many different mechanisms are proposed as to how to protect sensitive credentials. We believe that digital credentials are the key factor in initial trust negotiation phase; however, other factors such as experience and knowledge should also be included in future trust negotiation.

Seigneur [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 DOMAIN

The problem domain provides support to calculate trust in situations when the requesting entity has a past experience with the service. Access rights given to third party are not static but change based on delegations



Flow Chart to Calculate Dynamic Trust Value

and revocations. Third party users are assigned generic rights based on the credentials, the Security policy and authorized user delegations that can be used to request access to other services. An Authorized user with these access rights can in turn delegate the requested right. Third party user can access a service only if he has the right to do so or if an authorized user has delegated that right to him, he can delegate all rights that he has the permission to delegate. Rights can likewise be revoked [5]. Third party user can send request to authorized user to delegate to him the right to access certain services. If the authorized user is satisfied with third party user credentials, he will allow him to use the service and may also decide to limit access to a certain period or persons to whom third party can re-delegate the right. The security agent is responsible for honoring the delegation, based on the delegator's and delegate's credentials and the policies. When third party makes requests to the security agent controlling the service, they attach their credentials and ID certificate or a delegation certificate to the request security agents who may generate authorization certificates that users can employ as tickets to access a certain service. The trust models used are categorized as:

Pervasive Trust Model: Trust relationships are established between entities. All entities are autonomous and

some of them are mobile. Entities can be persons, organizations, departments, etc. and its devices are laptop, mobile and PDA's. Each entity manages its own security.

Formal Trust Model: The Formal Trust Model (FTM) is comprised of Direct Trust Unit and Recommended Trust Unit. Direct trust is formed through direct interaction experience among the nodes. A behavior model is used to evaluate the satisfaction level of the direct interactions. A recommended trust protocol is used to evaluate the recommendations to form recommended trust.

A. Problem Formulation

The Problem Formulation is designed to calculate trustworthiness of each entity, analyze the behaviour pattern of entity and provide service access decision in compliance with security policies. Trust value increases with good behaviour and decreases with bad behaviour. A bad behaviour decreases the value with the rate that is dependent on the sensitivity of the relationship. An entity can make wrong behaviour intentionally or unintentionally. This model supports good trust history. An entity, with a superior trust history has larger growth in trust value with a good behavior and less penalty in trust value with a bad behavior via an entity with a bad trust history. Reward / penalty rates change with the behaviour of entity.

B. Trust Value Calculation

When new entity joins a pervasive environment, it initially has neither past experience nor any reference to advocate it to establish a trust value for interaction. In this case, formulation of an opinion requires the model to take risk and assign an initial ignorance value, which can be updated as additional information 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 n_t
2. Total number of positive interactions of entity n_p
3. Total number of negative interactions of entity n_n
4. Security level s_i where $0.5 \leq s_i \leq 3$

IV. PROBLEM SOLVING TECHNIQUE

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

A. Growth/ Decline in Trust Value

The Initial trust value assumed for positive attempt is 0.5 and for negative attempt is 0.33. Depending on the outcome of the interaction, a positive behaviour is rewarded by increasing service trust in the entity and negative behaviour is penalized by reducing the service trust in the entity [7]. 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:

$$t_i = t_i - 1 + \Delta p \text{ for } I_{cur} \text{ (Positive Interaction)}$$

$$t_i = t_i - 1 - \Delta n \text{ for } I_{cur} \text{ (Negative Interaction)}$$

For positive behavior, reward rate Δp is calculated as: $\Delta p = \alpha * n_p / n_t * 2^{n_p} * s_i$

Where α is a constant and its value is 0.01.

Reward rate increases with consecutive positive interactions. Similarly for negative behavior, penalty rate Δn is calculated as:

$$\Delta n = \alpha * n_n / n_t * 2^{n_n} / s_i$$

In table 1, the trust value shows the level of trust; a service has in an entity. Different Trust levels taken into consideration have been shown along with their range, meaning for each value and description for each trust level.

- 1) Entity is distrusted when current value approaches to 0.

Rate of trust/distrust is controlled by service security level that is defined by the service [14].

TABLE I: TRUST LEVELS AND CORRESPONDING TRUST VALUES

Trust Level	Value	Meaning	Description
11	0	Distrust	Total Distrust
12	$0 \leq \text{value} < 0.25$	High Distrust	Lowest Possible Trust
13	$0.25 \leq \text{value} < 0.5$	Low trust	Not Much Trust
14	$0.5 \leq \text{value} < 0.75$	Medium trust	Average Trust
15	$0.75 \leq \text{value} < 1$	High trust	More trustworthy than most entities
16	1	Complete	Full Trust

V. IMPLEMENTATION AND USER INTERACTION

The experimentation carried out at MM University, Mullana, Ambala, is based upon different means to gather the information regarding the satisfaction level with the working of proposed work. The proposed work is subjected to be tested with 40 users belonging to different categories and different trust levels. 15 users belong to the well known (including family and Friends) category whose trust level is the highest and 15 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 given equations and table, 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 40 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.

TABLE II: USERS WITH THEIR CORRESPONDING INTERACTIONS

No. of users	No. of users with Positive Interaction	No. of users with negative Interaction
40	30	10
40	35	05
40	40	0

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.

TABLE III: SINGLE USER WITH HIS/HER ASSIGNED CORRESPONDING TRUST LEVEL

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

The proposed work has been implemented using PHP at front-end and SQL Server at back-end.

A. Snapshots of the System

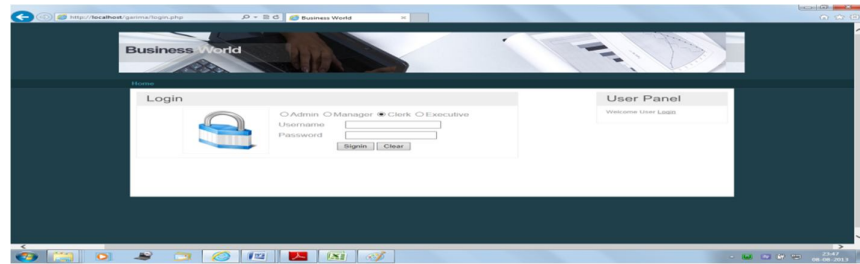
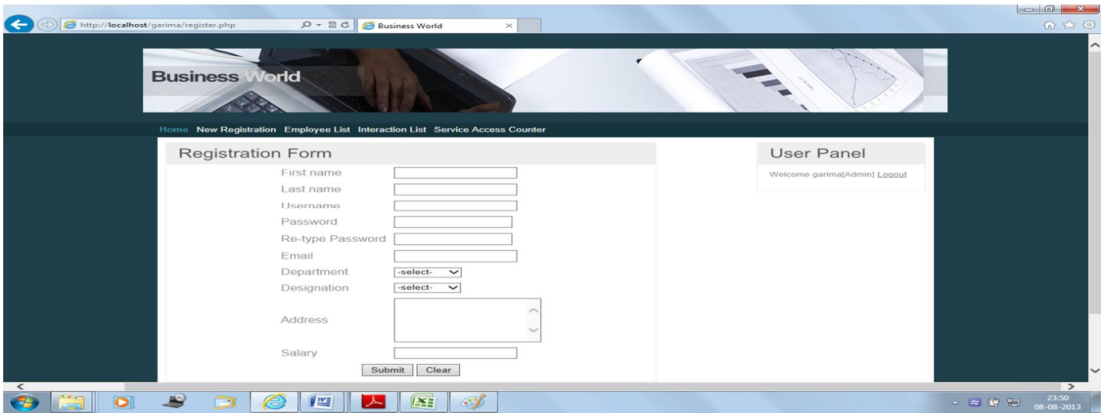


Figure 1: Login Page

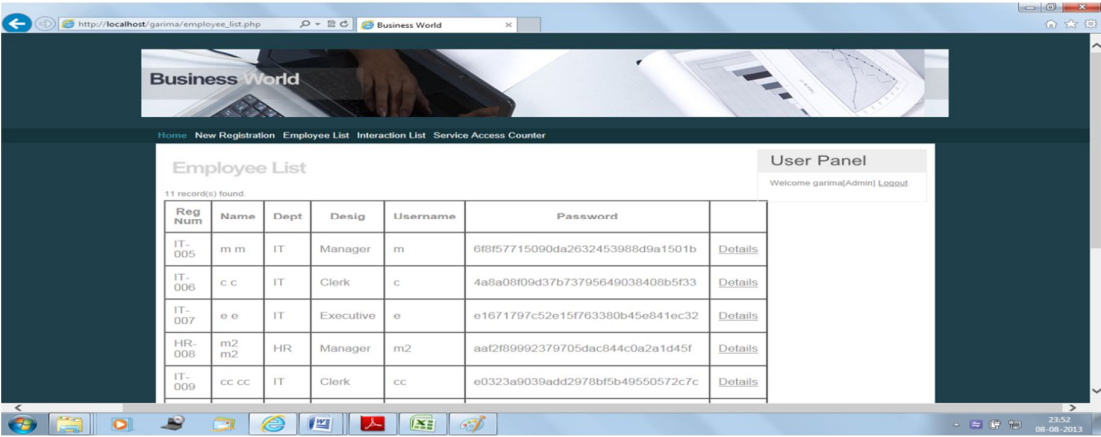
Figure 1 describes the login page where any user can login himself and use the services provided by the authority.



The screenshot shows a web browser window with the URL `http://localhost/garima/register.php`. The page has a header with the "Business World" logo and a navigation menu with links: Home, New Registration, Employee List, Interaction List, and Service Access Counter. The main content area is titled "Registration Form" and contains several input fields: First name, Last name, Username, Password, Re-type Password, Email, Department (a dropdown menu), Designation (a dropdown menu), Address, and Salary. There are "Submit" and "Clear" buttons at the bottom of the form. On the right side, there is a "User Panel" with the text "Welcome garima/Admin" and a "Logout" link. The browser's taskbar at the bottom shows various application icons and the system clock indicating 23:50 on 08-08-2013.

Figure 2: Registration Form

Figure 2 shows the user's registration form. Here Administrator is authorized to register the user details and creates user's username and password.

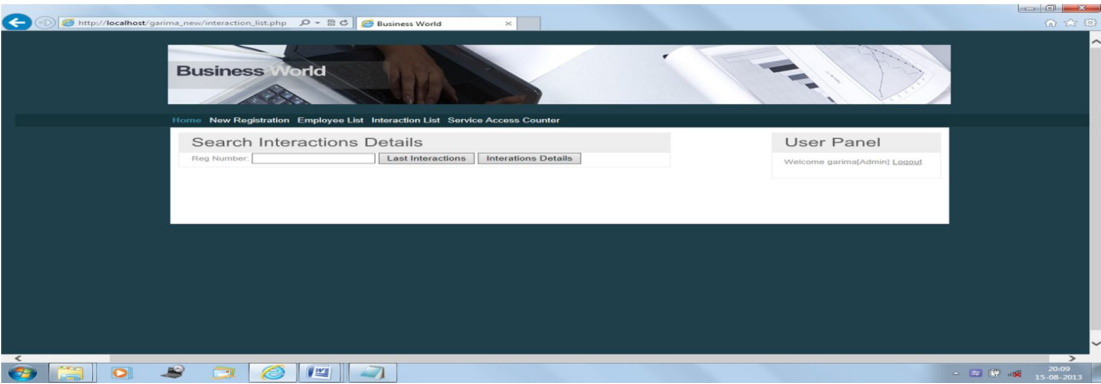


The screenshot shows a web browser window with the URL `http://localhost/garima/employee_list.php`. The page has the same header and navigation menu as Figure 2. The main content area is titled "Employee List" and displays a table with 11 records. The table has columns: Reg Num, Name, Dept, Desig, Username, Password, and a Details link. The "User Panel" on the right shows "Welcome garima/Admin" and a "Logout" link. The browser's taskbar at the bottom shows the system clock indicating 23:52 on 08-08-2013.

Reg Num	Name	Dept	Desig	Username	Password	Details
IT-005	m m	IT	Manager	m	68f57715090da2632453988d9a1501b	Details
IT-006	c c	IT	Clerk	c	4a8a08f09d37b73795649038408b5f33	Details
IT-007	e e	IT	Executive	e	e1671797c52e15f763380b45e841ec32	Details
HR-008	m2 m2	HR	Manager	m2	aaf2f89992379705dac844c0a2a1d45f	Details
IT-009	cc cc	IT	Clerk	cc	e0323a9039add2978bf5b49550572c7c	Details

Figure 3: User Access Detail List

Administrator can view user's records for each access and the user details such as his service access details are shown in Figure 3.



The screenshot shows a web browser window with the URL `http://localhost/garima_new/interaction_list.php`. The page has the same header and navigation menu. The main content area is titled "Search Interactions Details" and contains a search bar with a "Reg Number" label and a "Last Interactions" button. There is also a link for "Interactions Details". The "User Panel" on the right shows "Welcome garima/Admin" and a "Logout" link. The browser's taskbar at the bottom shows the system clock indicating 20:49 on 15-08-2013.

Figure 4: Interaction Detail List

Administrator can also search the details of any particular user if required as shown in Figure 4.

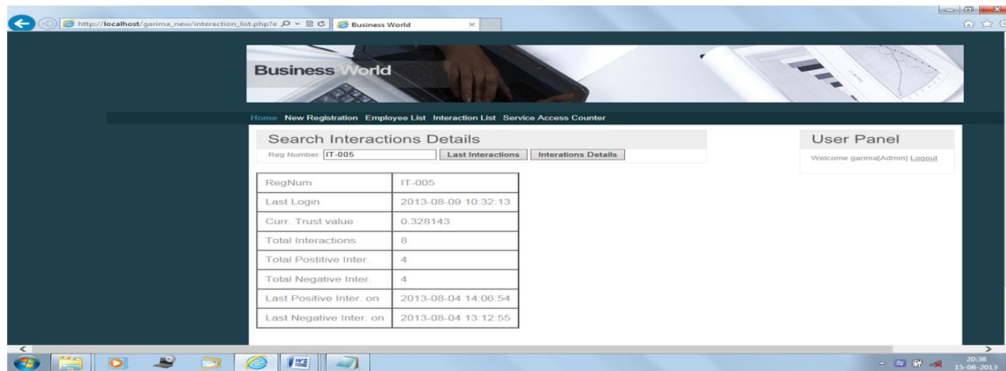


Figure 5: User Last Login Interactions Detail List

The details of last login interaction of the user are shown in Figure 5 where administrator can view the number of attempts made by a user as last positive interaction and negative interaction of service.

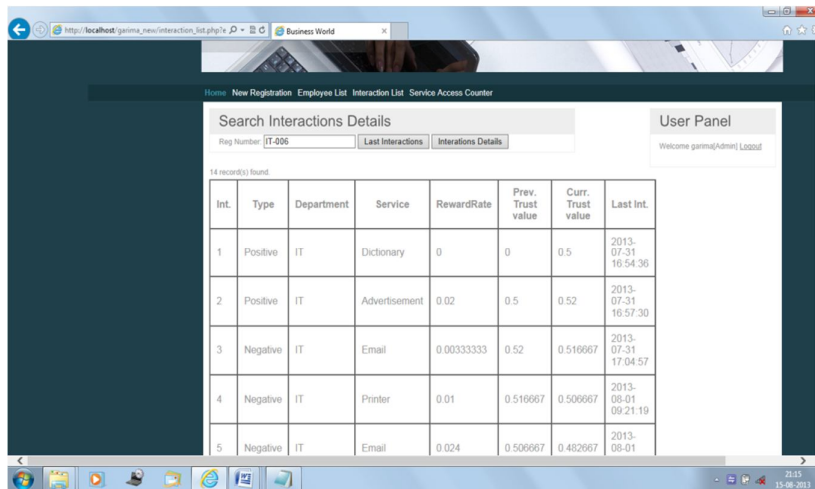


Figure 6: User Attempts and Trust Value Detail Form

As shown in Figure 6, administrator user can view the details to avail any service, attempts made by user corresponding to his trust value.

B. Snapshots of User Panel

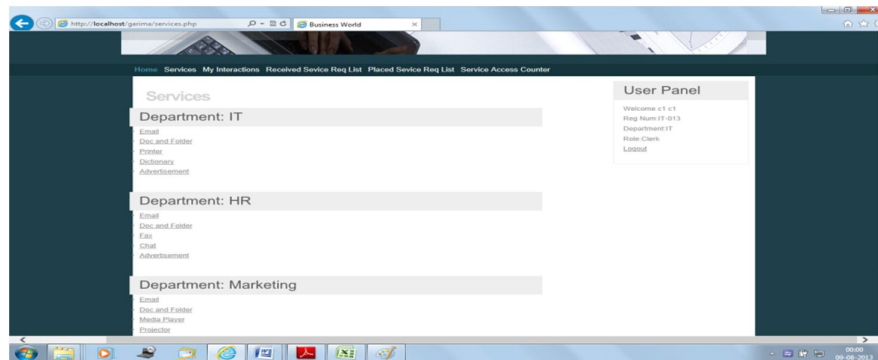


Figure 7: Department Level Services given to User

Figure 7 shows the services provided to the user by each department.

The screenshot shows a web browser window with the URL `http://localhost/gamma/validate.php?id=IT&u=Adv`. The page has a header with the "Business World" logo and a navigation menu with links: Home, Services, My Interactions, Received Service Req List, Placed Service Req List, and Service Access Counter. The main content area is titled "Service Request.." and contains a "Key Verification" section. This section has a message: "user your's secret to access service you are authorized for otherwise use service key for guest login". Below this message is a "Secret key" input field with four asterisks and a "submit" button. To the right of the Key Verification section is a "User Panel" with the following text: "Welcome c1 c1", "Reg Num: IT-013", "Department: IT", "Role: Clerk", and a "Logout" link.

Figure 8: User Secret Key Verification Form

User must have entered the secret key to access the services provided by any department as depicted in Figure 8.

The screenshot shows the same web browser window as Figure 8, but the URL is `http://localhost/gamma/geto_service.php?id=IT&u=`. The main content area now displays a message: "You are authorized to access service". The "User Panel" on the right remains the same, showing user details and a "Logout" link.

Figure 9: Access Authorizing Message Sent to User

As shown below in figure 9, a message gets displayed which confirms about the authorization given to the user to access the service.

C. Snapshots of Third Party User

The screenshot shows the same web browser window, but the URL is `http://localhost/gamma/validate.php?id=HR&u=Far`. The main content area is titled "Service Request.." and contains a "Service Request.." section with a "Recommending to" input field containing the text "HR-014" and a "submit" button. Below this is a "Key Verification" section with the same message and "Secret key" input field as in Figure 8. The "User Panel" on the right remains the same.

Figure 10: Service Request Form

If an employee is not authorized to access the service by him, he can send a request to the recommended user (who already has a right to access that service) through recommended ID as shown in Figure 10.

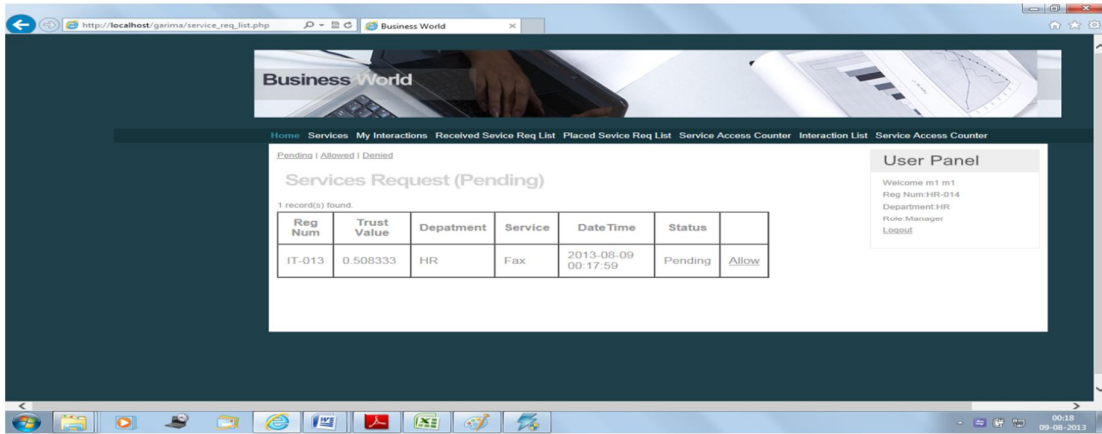


Figure 11: Recommended ID Received Service Request Form

Through recommended ID, one can view the details of requested service sent by third party user and also view the requesting third party user's trust value so that the recommended user can take decision about whether to allow or deny for demanded service depending upon requesting users trust value as shown in Figure 11.

VI. RESULT ANALYSIS

The proposed model observes the behaviour of the entity and also increments/decrements his/her trust level initially depending upon positive or negative attempts made by an entity before completely trusting/distrusting the entity [8]. The increment/decrement factor for a given positive/ negative interaction is calculated by using equation 1 and 2 respectively.

A. Growth/ Decline in Trust Value

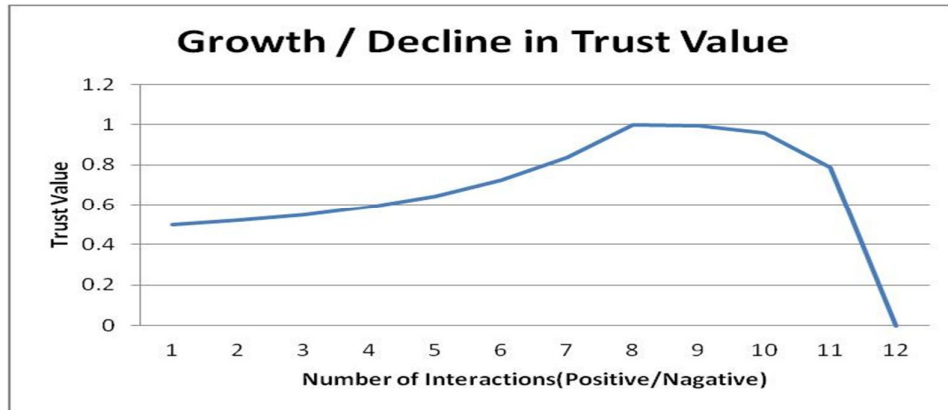


Figure 12: Growth/Decline in Test Value

Figure 12 shows trust establishment of an entity with positive and 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 Security Level in Trust Value

Trust/distrust rate after each interaction is controlled by service security level. The slope of trust increment/decrement is dependent upon the security level 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 13.

An important property of trust model in pervasive environment is to be adaptive, having the capability to adjust in accordance with behavioral pattern changes. The proposed model is compared with FTM [13] trust

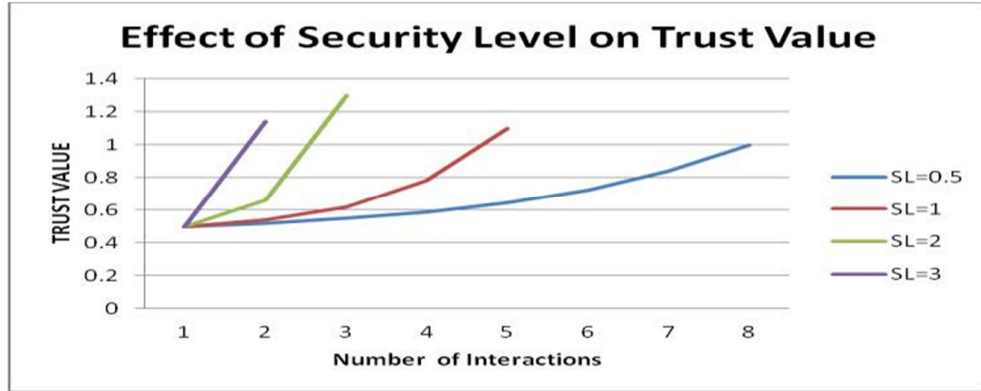


Figure 13: Effect of Security Level on Trust Value

model on the basis of random positive and negative interactions made by users as shown in Figure 14. The comparison shows that the FTM model trusts the entities very early as compared to the proposed model. Due to early trust of FTM, the chances of attack increase which may be preferably reduced by using the problem domain.

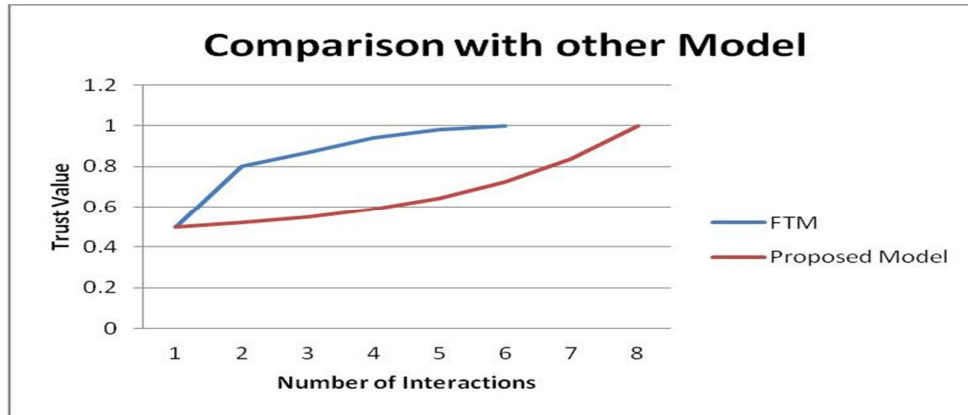


Figure 14: Comparison with Other Model (FTM)

VII. CONCLUSION

This present work motivates the need for the use of a new trust model for pervasive computing applications. A formula to calculate trustworthiness of an entity has also been proposed. This present work calculates the trust value for security driven third party access in pervasive computing. It supports dynamic adjustment in trust value based on entities behaviour thus minimizing human involvement in security management. Conclusion drawn on the basis of testing of the proposed work with 40 end-users can be summarized as: (i) the compatibility and easiness to work with the proposed work is found to be almost similar for all users. (ii) The system does not require any training or any specific skills to operate it. 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] Web link <http://www.nist.gov/pc2001/aboutpervasive.html>.
 - [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] S.I.Ahamed, M. Haque, M. Endadul, F. Rahman, N. Talukder, "Design, Analysis and Deployment of Omnipresent Formal Trust Model (FTM) with Trust Bootstrapping For Pervasive Environments", Journal of Systems and Software, vol. 83, pp. 253 - 270, 2010.
 - [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] J. Seigneur, and C. Jensen, "Trading Privacy for Trust", In the Proceedings of the 2nd International Conference on Trust Management, vol. 2995, pp. 93-107, 2004.
 - [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] Dheerendra Mishra, Ankita Chaturvedi, Saurav Mukhopadhyay, "An Improved biometric based remote user authentication scheme for connected healthcare", Int. J. Adhoc and Ubiquitous Computing, vol. 18, nos. ½, pp. 75-84, 2015.
 - [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.