Safety and Security Enhancement for Privacy of Users in Pervasive Computing via P3P and APPEL Protocols

[1]Somayeh Jafari, [2]Masumeh Jafari, [3]Fatemeh Saberi, [4]Rouhollah Yazdani, [5]Shiva Darijani

[1]Department of Computer Engineering, Mashhad Branch, Islamic Azad University, Mashhad, Iran (Corresponding Author)
[2]Department of Computer Engineering, University of Pnu, Shahre Babak Center, Iran
[3]Department of Computer Engineering, University of Pnu, Shahre Babak Center, Iran
[4]Department of Computer Engineering, University of Azad, Kerman Center, Iran
[5]Department of Computer Engineering, University of Azad, Bam Center, Iran

Abstract: This paper explores the challenges facing pervasive computing deals. Pervasive computing environment and the future of computing is a new approach Computers and computing environments, and is intended to accommodate the daily lives of people And it should always be an invisible component. Security is a significant challenge in pervasive computing environment. In this paper, the security of AES has two key protocols. This paper addresses the issue of privacy as a complementary discussion of standards, protocols, tools and other related subjects has been analyzed with it. The key factor to preserve user privacy, without which it cannot be universal computation. Provide guidelines for appropriate interaction with the user-defined policies and compliance for working with user data collected by the central argument of this article. This approach uses a system that detects the position of the building is created based on wireless signal strength meter works. Privacy preservation is also using P3P and APPEL related protocols is done by the system. Finally, simulation results are presented. Method is to compare the simulation a similar system using both real system implementation and Privacy Policy and poster presentations of new models, Terms of service to users by comparing the time being.

[Somayeh Jafari, Masumeh Jafari, Fatemeh Saberi. **Rouhollah Yazdani, Shiva Darijani, Safety and Security Enhancement for Privacy of Users in Pervasive Computing via P3P and APPEL Protocols**. *Life Sci J* 2013; 10(7s):139-147] (ISSN: 1097-8135). http://www.lifesciencesite.com. 23

Keywords; Industrial security applications; Local area identification; Pervasive computing environments; Security supportive architectures

I. INTRODUCTION

Network computing and mobile computation that underlies the Internet, they have quickly become part of everyday life. We expect to devices like PDA or even a home entertainment system can For adoption information on the internet and work on a system are integrated together. Network computing and mobile computation that underlies the Internet, they have quickly become part of everyday life. The goal of pervasive computing, computing access to every place that you need. Privacy is a major factor in the realization of pervasive computing can not be without it. Provide guidelines for appropriate interaction with the user Through the definition of policies with respect to information collected from the user, the main argument of the article. In this paper, using a detection system is located inside a building Based on measuring the signal strength of the wireless network works. Privacy with P3P and APPEL protocols is done by the system. And compare the method is to simulate a real system, the same software system implementation In this structure, based on previous models such as PAWS, a new system was designed with the changes made Privacy poster instead of the system from a centralized server in each building uses And relying on an indoor location detection system, capable of finding and negotiating services and the policy was introduced. Also, the removal of the poster, because of infrared or Bluetooth connections, it's a significant savings in time by negotiating service was created, And general hardware system can be implemented.

II. PERVASIVE COMPUTING

Pervasive computing field has provided a wide range of computational models. Pervasive computing is the integration of the physical world to the information world. Therefore, to provide application services to users, devices and applications deployed In different geographical locations to establish communication with each other, is integrated[20]. In a pervasive computing environment into entities in the environment, with a minimum of human intervention and awareness, to exchange information with each other's work. The importance of information security and privacy in such environments has increased dramatically[17]. In such an open environment and decentralized entities without prior notice from time to communicate with one another's work. The peripheral mechanisms to protect data privacy and security performance and quality Assurance exchanges provide. Pervasive computing device, not PCs, but can be one of the following types: Small tiny - even invisible - either mobile or embedded in any kind of object that can be imagined; More complete expression, any communication that can be spread through interconnected networks, established. Pervasive computing immediate access to information anytime and anywhere makes possible.

III. Privacy Policy

Inspection and deliver such letters, recording and disclosure of telephone conversations, the disclosure of telegraphic and telex communications, censorship, lack of traffic and deliver them, eavesdropping and any investigation unless prohibited by law. So the above privacy in the country guaranteed to the people. With the development of tools to collect, transmit and process information, to create ways to ensure privacy; Because regardless of the strategy, According to conventional computer systems to store large amounts of personal data Unlimited access to the time and place and also allow them to provide analysis and inference[1].

IV. Privacy in pervasive computing environment

Privacy as a fundamental problem in pervasive computing applications is presented.

Privacy as an important issue has been presented by pervasive computing applications. Many models have been created to deal with these risks. For a successful design, we should know what is important for technology and for each project specifically. This is a bit difficult, because there is a few research about the potential users of the pervasive computing which designers can take advantage of it. Aiming to address this need of how privacy can be maintained in an integrated computing environment as mentioned in [2]. Also, many great researches have been conducted in this area such as in [3], which a solution has been studied for privacy. In the follow sub-sections below, unresolved issues and challenging solutions have been classified.

Interestingly, what makes the design more complex is the fact that extensive calculations are typically embedded or invisible, so to detect the presence of users and devices to collect more information *in* which users have a limited understanding of the technology, many problems rise in the area of privacy, design, and safety issues.

A. PSIUM Approach

This model tries to minimize the misuse of user data. This model can utilize the reduction of usefulness of this method for sending data server to access the intended uses, without reducing the quality of service to the user. A system that uses this method sends multiple location-based applications to the service provider. Meanwhile, only one request is the representative of user's actual location. In response to the transmitted data, the system knows how to utilize the information in a right way, and only then provide it to the user. This approach uses virtual incorrect data and this data is difficult to diagnose correctly or incorrectly. Therefore, the abuse of user information like its location will be prevented by the service provider.

B. Privacy controls and feedback in RAVE system

In this approach, the system has the capability to act as attorney for virtual users and receive the information of privacy of user from the environment and if the lack of user compliance with policies was found, then it will notify the user. In fact, this system will notify the user that his or her personal information might be transmitted or exchanged without user’s permission, so that user can to do the appropriate action.

For example, it is possible to imagine an environment with a video camera shooting a movie. Then the user enters this environment, and on the user’s mobile device that is equipped with this system, it is specified as an alert for breaking the privacy laws. In this case, the mobile devices will inform the user to either leave the location or ask the system if possible to run off the video camera.

C. Mist System

The system is a communication infrastructure that its purpose is to preserve privacy in a computing environment. It works in a way that the user's identity and location, separately analyzes the system and creating a protective system of collecting and combining the ordered pair (place identity) to prevent takes

Way to do this is to use special routing algorithm for application server provides indirectly, and in a way that the server does not know the identity of the client.

The system also has the ability to set privacy levels, and allows the user to with greater speed and with a shorter path but with less security, and privacy can be used to the provided services[19].

D. PAWS System

The model presented in the privacy model is PAWS. This paper is related to a comprehensive system for protecting privacy which has been written in pervasive computing. In this paper, a new system called PAWS (Privacy Awareness System) has been used. Being able to review the privacy demands, adapting to the demands of the environment which both are expressed in XML format ensures compliance with our demands.

The structure of this system is that when a user is logged, through an interface such as infrared and

Bluetooth to announce the demands for privacy with P3P protocol. To save power, we can declare it on the address of a web page on the World Wide Web (URL) and to check, only use the web address to receive data again later. Devices and sensors in the environment or in a transaction during its privacy features are expressed, or that a particular device for the extraction of these features is in the environment. Then, using a protocol called APPEL to negotiate to achieve a specified set of features was performed. However, if the user is using a video camera it may not consent to this agreement; so that the camera should be switched off.

It should be noted that the terms of the conditions imposed by the user and the environment, just as we were talking about, is expressed in the P3P standard. This standard is implemented in XML format, and now by the World Wide Web Consortium (W3C) as a proposal for different environments including the Web, will be provided. Also, this format is supported by browsers such as IE 7 and actually this is becoming a standard for expressing privacy features are. For example, a sample privacy policy for a telephone transmission system (Follow-me Telephone) service expressed in the P3P format states that the username and password, and the user's place used to be imprecise to call[13]. Then, the new user will connect this user's temporary-location phone. We also need a database system that stores the data, the accessibility type of each data, and the usage type of these data, as META DATA. In addition, any usage of data should be logged and registered which is called PAW-DB.

Given the brief explanation, this system works to provide necessary tools to protect privacy for users and also helps other systems during the operation to respect the privacy of others, and not to disregard any law. In fact, this approach is a way to express the rules and respect them as a resource. So that when a system is equipped with PAWS, when the system wants to gather information, the system must interact with the user and if the system which plays the role of virtual lawyer, allows then the system can collect that information. If these features are not match with the user profile, the user can refuse the service or use the benefit of similar service.

E. Spirit System

Spirit system is using a special middle-ware called Spirit to access the personal information. The direction of this system for usage is based on a registration. A service provider that would like to present a specified service in the specific location should come on this middle-ware to register. When a user requests the service, the message is sent to the server provider and the system will be notified. Using this approach, privacy can be well kept and a good control over the information that the users put on the system, will be performed. The only drawback to this system is its overload.

V. Position Identification

A proposed system which uses a method of identification for the location within the building has been investigated. Also, the system requires a position identification system within the building.[22] A few different approaches of estimating the position of the user and identify which room the user is located in, are provided as below:

A. PlaceLab

This method is a diagnosis based on measurement of signal intensity in Bluetooth, WLAN and Mobile phone networks. A well-known system in this field is PlaceLab which has been created in research institute of Intel Company [4]. In this system the signal has already been recorded and then compared to the original value, the user position will be estimated with the accuracy up to about 100-meter from the mobile network, and using the wireless network, will be nearly 13-meter [5].

B. RADAR

This method is a diagnosis by combining the multi-source signal strength. One of the popular systems that have been created using by this method is RADAR created by Microsoft research institute [6]. This system provides the accuracy near 1.5-meter which is significant[11].

C. Nibble

This method is based on a probabilistic model using a Bayesian network which is able to present the location of the user with over 97% estimate, if two different access points in wireless network is available[21].

D. BAT

This system is based on a few numbers of transmitters installed in the environment and then using a Digital Signal Processing (DSP) system for calculating the exact location and its changes. Accuracy of this system is at least 3-cm [7].

In [8] using software PlaceLab, a security system to control a location Laptop Institute is presented. The thesis of the system of Locus, which prefers to use the code provided PlaceLab is to confine and take advantage of it. This system consists of a server and a client that is installed on laptops and check the signal strength in comparison with the previously measured signal intensity, the estimated position, laptops and server updates offers.

Systems such as RADAR and PlaceLab need to set up before use and then can leave the laptop or PDA the software installed on it to announce a specific range. The system as a simple application of identify the location within the building has been proposed. As mentioned in [9], the manufacturers improve the RADAR systems have provided the blueprint. This

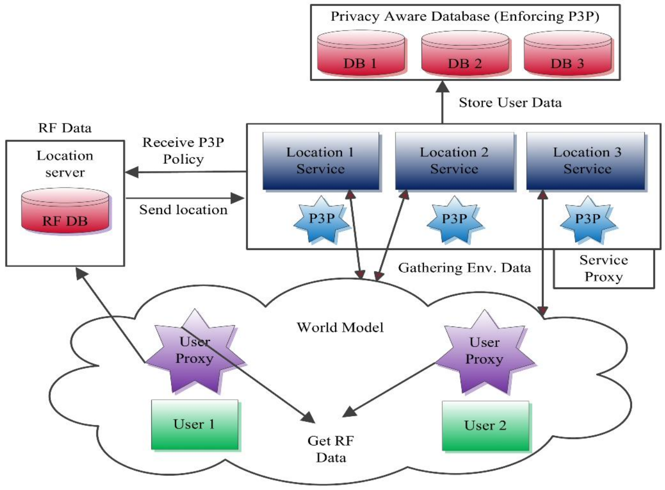

Figure 1. General system of proposed model for enhancing the safety and security for privacy of users in pervasive computing via P3P protocol.

system of continuous location tracking techniques for preventing errors from the noise and the moment has to offer. With this method, and the Find the speed limit, the noise and movement of the moment may be impossible to forecast and estimate the position of the user are excluded. Human body with a high percentage of water absorption for electromagnetic waves is considered. So the users of the environment has a significant impact on the incoming signal and reduces the location estimation accuracy. To solve this problem, several different profiles at different times RADAR system to create and automatically change the active profile.

As mentioned in [10], a method for estimating the position of the user uses the need for early planning and initial training will reduce. In fact, with few data signal intensity access point 27 can be positioned with great accuracy user estimates. This system deals with the location to a specified location and with it a name (e.g., room names) sets. Users can present in different locations, the measured signal strength of access points and specify a location symbol, declaring it to the server. In tests that have been performed, the system could only measure the signal strength and provide 10 times the server was able to place the measure in a small room with a test environment to perform more than 90 percent. The ability of individuals to prevent others from accessing privacy where they include a place to record[12].

1)*Protocol P3P: This protocol is used to express Privacy Policy[13,18]*

2)*Protocol APPEL: This protocol is used to express preferences regarding the user's personal area[18].*

VI. RISKS IN PRIVATE LOCATIONS

A. *User's Exact Location*

B. *Following the User*

C. *Location Identification of the user matches with the known locations*

This part propound as two ways:

1) *Complete Anonymity:* In this method, an attacker with the user's position, but in the way of his search is restricted to K modes. No matter how much large K is, the probability of an attacker access to the exact position where the user is low[15].

2) *K-Unknown:* This method is convenient and affordable. To use its virtual data to be generated if the request includes a request to another location at the K-1, that is not detectable[14,16].

VII. NEW PROPOSED MODEL FOR PERVASIVE COMPUTING

Model is based on the previous model PWAS ETH is listed in the University PAWS to the extent that the system studied and a method for resolving the issue of personal domains has been presented. Initially a general description of the methodology of this model is shown in the figure, we can provide. This system is in place Users will benefit from the services available in the environment and given the choice to use them. The important point is that these services need to underlay data for performing their work, and for accessing to data, it must collect information from user and user interaction environment. For instance, maybe we need to position of the user, or maybe we require xerography of user.

Here, as described in the past, the debate comes to a personal area, should ways to limit the information collected Monitoring, collection and use and also ensure that there is actual compliance. The proposed model and its implementation, a method for making these demands are presented. So that the user specifies a preference for their owning areas have APPEL, which should be expressed in terms of protocol. When the user enters the environment, Services offered by her work and is done automatically by the system but he must supply the services, to select the desired service. And put it in the address specified in this standard.

It is noteworthy that the P3P standard for the Web proposed and for pervasive computing environment, it is the incorporation of additional to be able to cover the debate location, sound, image and... as Fig.1.

Privacy policy proposed system, the selected service received in the form of P3P and using algorithms specified, the user's personal area matching the description does. If this match was done, the user allows using these services and the server become to collect information and perform asked task from user. After data collection, data storage sector will be discussed. Database that keeps information collected, a database should be aware of the personal sphere. Only certain users should be allowed to use certain parts of the data have and these are defined in the Privacy Policy. Also, all data access is logged to be used in possible legal problems.

VIII. Innovative Features in New Proposed Model

Main innovation of this system is using a location system. The system PAWS using a server that was a Privacy Beacon Privacy Policy. However, more quickly, address and receive a prompt return to work on negotiating with other suitable proxy was done on the Internet.

In this system for finding currents services and privacy politics of them, we could use a local positioning system inside the building. In this way, each user device with which he is a personal proxy. Using a wireless interface, the signal to noise ratio measured for the access points and sends it to the server location. The location of the database server with signal intensity and using an appropriate algorithm, the similarity between these measurements with previous measurements examined, and detect the nearest possible position. It should be noted that given that this is the only enough to reach the desired room and it is a place of higher accuracy ensure supplies are adequate for the user. Red-Pin system that works this way has been able to measure the very small number, more than 90-95 percent accuracy in identifying the user in a room that has been reached.

After diagnosing the situation, it is a proxy server (usually in one building is unique) to send the Service and Privacy Policy which can be received. Next, select the appropriate service, the service is available. Privacy policy after this stage, it should be adapted to user preferences and in compliance, the user will be able to use the service provider and the user will begin to collect environmental data. If no matching user is given the proper message.

IX. Improvements of the New System:

This model provides improvements to the model, part of which is as the following:

1)Changes in the policies of the poster features a subtle servers and integration servers in the server location services

2)The use of common hardware to implement the system

3)Improves the system response time

4)Enhance security

X. Different Parts of the Model:

Different parts of the model are as follows:

- Location services

Related services to various places in the system is defined. As was explained, Various services are available in each room, among which the user can select the desired service.

To provide these services must first be extracted from the data model. This requires the application to be submitted and answered.

- Privacy-aware databases

Data must be stored in the database. After data collection, the data storage is discussed. Database that keeps information collected. For each service, a P3P privacy policy format is defined. The possibility of adding certain special characteristics in the form of ubiquitous computing environment as well.

- Location services

Service position is that the user's position, he said. So first, a database of signal strength and its associated parts are formed. Another way is to have an appropriate function for a given signal strength. So we took advantage of the system has been pre-determined. Then a set of received signal strength of the proxy user and then review, the point is detected.

- Proxy Services

The proxy service is responsible for the task of providing the Privacy Policy. To do so, users must first position of proxy services to be delivered by service location Privacy Policy P3P protocol format for the related services are received.

So, this Privacy Policy will be sent to the proxy user preferences adapting the work he is doing.

- Environment Model

The model is used to simulate the environment and if the actual implementation of the proposed system is, Services must have the ability to collect relevant information. This model is able to perform the following tasks.

1) Modeling the motion of a user's environment: Different users which are randomized to enter the building, Randomized to one of several models based

on the motion, the system will move And into the other room to room and eventually out of the door are.

2) Find modeling and signal strength of access points in the environment: To simulate the signal intensity in the environment of a function is defined Based on distance from the point of access points and the signal intensity of the room. Another way of using recorded data of a real system.

When I mentioned are options to test the proposed system. As I explained to a position detection system I have used in the proposed system. So to test it, or should the position detection system was tested in a real environment Or should it be tested in a simulated environment.

I mentioned in the first data set to create a simulation environment and associated signal The second case refers to a method of identifying the location within the building.

I've used the second method the simulation. There are several options for testing, analyzing the characteristics of the data signal within buildings from previous plans, building materials, walls, and... To produce After positioning data to run the place. For proper function, the researchers look at the broadcast signal Of course, I've never used this method. Status and gender gap. Walls of the room and... Research in this area has been fully introduced.

The second way that the measured signal intensity data already take advantage System and measure the actual data that I have used this method I used data from previously measured.

redpin system to estimate the position of the fingerprint method by comparing the received signal strength and signal intensity of the recorded data is used.

3) Environmental information request a spot: Services should be defined based on the data collected are presented to the user. Thus, the model is able to provide data about the user's environment.

- *Proxy user*

Its functions are as follows:

1)Information request signal from the model
2)Send a signal to the server location information
3)Get Privacy policy
4)To comply with the policy demands of the users are expressed in APPEL
5)Inform the user of the Match

XI. Simulation

5-1 Simulation results:

. 5.1.1 Simulation of key components:

1-The two keys to encrypt data, a first for automatic detection and automatic connection to the server is and another to move secure data broadcast to the environment: The first key is to start with a Czech software that the user has access to the software Begin to interact with the server, and if it is not on the same server will reject the connection. The key must be manually set by a person on behalf of the user and the server. The second key, the data are sent to the broadcast And all but the only people who can get This information should be a key on your device.

2- There is a simulated room or area: DB is exactly simulated redpin Points by redpin static simulation to bring the server memory Not any time to request that the server database.

3 – Simulation Services: We service a name, and an ID and a location to Service We define an object p3p.

4 –Simulation users: A name and a location in a file, we appel and two keys I explained before. Each user must have an array of policyrequest object caching. When the user is running As soon as the situation was different If the service interaction and interaction that respond to Policyrequest the answer is recorded and the next time the user is not Only be stored in the output.

5-P3P and APPEL simulation protocols: P3p simulation protocols, including access, there are various conditions. Here are a few of the same relation. APPEL simulation protocols include a statement that includes a series of actions and message.

6- Simulation database to locate users

7- Caching simulation for users to avoid asking the user to re-........? If the user enters an environment that was and will benefit from a service next you will enter the environment. Check conclude that if the user has The request fails again, If a request is active and should not conclude Active class is Which shows the position of the user's position And service that defines the service.

8-AES encryption for security protocols: Encryption of files and is DesEncryption. Data that come in our software, we can send the key is the user's hand Encrypt is a server whose samples are available. That is all the information is sent but only those who could use this information the keys on their device. So this is how we detect and transmit data to the broadcast. The purpose of encryption is we understand that the information received from one of our users. Data are sent as broadcast and they received, But the only people who could use this information, which may be the key And can be decoded. This information will not long be decoded the standard format is decoded The format in which the security is high security. So the second key to encrypt the information.

Position detection:

For this simulation, a position detection system that can make use of the signal to estimate user location has been utilized. In fact, similar to what was written in the actual application situation of detection, it is interesting that just based on the data, signal can be carried out.

Red-pin a fingerprint technique is described and this is the shape of the activation status of red-pin must be introduced into the redpin database. This was the initial launch of the software for the first time and it was necessary for users to stand in various positions with the signaling devices and sending information/signals to the server and convert it into a number of databases that are stored on it. Hence, it is now clear how the positioning is done. The location of each user on each server by sending a signal to the nearest number of signals which is sent and received that are estimated the approximated locations of the database servers.

Privacy:

To implement the privacy policy, we must match the user's preferences that can be defined with privacy policy. In this environment, the ability to read and convert the planned protocol by P3P and APPEL is the logical goal.

The environment is written in C # language that can match the user's preferences and policies. The simulation environment for each user's preference can be automatically selected and consistently be checked with the location where the user is detected.

Environmental models:

The model is in a way so that users can randomly access into the environment. Additionally, the related information to the approved maintenance and service is continuously offered.

A. The program:

1- To perform the following duties, we must necessarily be

a. Each service location must exist in the database Policy in P3P that each service must also be introduced first.

b. Policy in p3p Each service must also be introduced

c. User policies are also essential in APPEL

2- Start the server receives the broadcast signal and information And decrypt all data that identify valid (From Key # 1 - Explain the need to maintain security and prevent the infiltration of small-scale database server may be the keys to the users To send data through the switch which should be able to decode the data) and allow them to provide the information at this time, is a key task created by the system and is sent by the server to the user. *So* after all, the rejection of spurious data through....?

Encryption and decryption are the keys in here. Note that the user's password can be identified, or to be more specific, only the user can decode the encrypted data with your key. So it otherwise, the block of data received from the server could not be parsed.

3- Now that the basic data communication is enabling the user to switch off the server and send a signal to the GPS signal is then a server located in the area or closest service selection, and information services to its users that post does p3p protocol.

Then the user starts p3p analysis and compares their appeal. Then prompt them to call and enable or disable. The important point is that implementing a P3P time with the service user in the system cache and other data matching process will fail.

An example of simulation results

When We Run our software I come Parts and service know Software and services within each area are assigned. Benefit? Accelerating the next operation. This means that if we can link our service with our database REDPIN, When a user enters an area, we can immediately identify the services that we are in the area And the members of each service, per-user detection is the key and it P3P data must be sent to the user is the key Encrypt user is sent to the user. And provides the user with key check. If a log is done right it will log the check service to count there. If there was a check from user history. The user can read the history, and if there was to be added to the history. Then save the operation log and otherwise taking the log read and identify and capture the log. Also redpin at any position does not recognize the fingerprint. Once you enter an area and you can move Come a point A on the stand and say I'm the point A, the server takes your signal strength and location. Now you say I'm open to point B takes the signal intensity... So once these things are done. Now the user can enter the environment from the previous signal is, now the user can enter the environment from the previous signal is, Thus, the signal returns closest to specify where it is located. Also, each user must have an array of Object Caching is policyrequest. When the user running the entire array to keep the user on the server is high speed operation. As soon as the user enters different positions if the service fails to engage And their interactions to be answered in this record is policyrequest And the next time the user does not respond, the output is stored in a single user environment, the Use of resources in this environment. For example, it was found that the user is interacting with the Service 3 Service 3 has been reported previously selected or the user. Below is an example of the simulation results have shown, The free service is first detected in the range of 1 and the check policy and Cach and we've been on a sec. So a second user and a second position of history read it several times. Now we are into the service position 2 position 3 in the Czech policy so we made it a date and seconds Cach eaten. Then a second later, the user's position, and a second later and read it several times in history... This software is an example of output from the set-up position and check.

```
<?xmlversion="1.0"encoding="utf-8"?>
<logs>
<logaction="Check Service S1 in Area 1 and find out this is a new service so do Policy checking and Cache this choice"datetime="9/7/2012 11:44:11 AM" />
<logaction="current area is 1 and pointers is 20,20"datetime="9/7/2012 11:44:11 AM" />
<logaction="Check Service S1 Policy in Area 1 from history"datetime="9/7/2012 11:44:11 AM" />
<logaction="current area is 1 and pointers is 41,52"datetime="9/7/2012 11:44:11 AM" />
<logaction="Check Service S1 Policy in Area 1 from history"datetime="9/7/2012 11:44:12 AM" />
<logaction="current area is 1 and pointers is 62,87"datetime="9/7/2012 11:44:12 AM" />
<logaction="Check Service S1 Policy in Area 1 from history"datetime="9/7/2012 11:44:12 AM" />
<logaction="current area is 1 and pointers is 53,152"datetime="9/7/2012 11:44:12 AM" />
<logaction="Check Service S3 in Area 2 and find out this is a new service so do Policy checking and Cache this choice"datetime="9/7/2012 11:44:13 AM" />
<logaction="current area is 2 and pointers is 52,227"datetime="9/7/2012 11:44:13 AM" />
<logaction="current area is 3 and pointers is 69,423"datetime="9/7/2012 11:44:13 AM" />
<logaction="current area is 3 and pointers is 76,518"datetime="9/7/2012 11:44:14 AM" />
<logaction="current area is 4 and pointers is 105,732"datetime="9/7/2012 11:44:14 AM" />
<logaction="current area is 8 and pointers is 203,754"datetime="9/7/2012 11:44:15 AM" />
<logaction="current area is 8 and pointers is 221,743"datetime="9/7/2012 11:44:15 AM" />
<logaction="current area is 8 and pointers is 243,691"datetime="9/7/2012 11:44:16 AM" />
<logaction="current area is 7 and pointers is 246,517"datetime="9/7/2012 11:44:16 AM" />
<logaction="current area is 7 and pointers is 246,393"datetime="9/7/2012 11:44:17 AM" />
<logaction="Check Service S2 in Area 6 and find out this is a new service so do Policy checking and Cache this choice"datetime="9/7/2012 11:44:17 AM" />
<logaction="current area is 6 and pointers is 240,351"datetime="9/7/2012 11:44:17 AM" />
<logaction="Check Service S2 Policy in Area 6 from history"datetime="9/7/2012 11:44:18 AM" />
<logaction="current area is 6 and pointers is 250,304"datetime="9/7/2012 11:44:18 AM" />
<logaction="current area is 5 and pointers is 254,151"datetime="9/7/2012 11:44:18 AM" />
<logaction="current area is 5 and pointers is 256,17"datetime="9/7/2012 11:44:19 AM" />
<logaction="Check Service S4 in Area 9 and find out this is a new service so do Policy checking and Cache this choice"datetime="9/7/2012 11:44:19 AM" />
<logaction="current area is 9 and pointers is 398,61"datetime="9/7/2012 11:44:19 AM" />
<logaction="Check Service S4 Policy in Area 9 from history"datetime="9/7/2012 11:44:20 AM" />
<logaction="current area is 9 and pointers is 448,61"datetime="9/7/2012 11:44:20 AM" />
<logaction="current area is 10 and pointers is 459,245"datetime="9/7/2012 11:44:20 AM" />
<logaction="current area is 10 and pointers is 442,377"datetime="9/7/2012 11:44:21 AM" />
<logaction="current area is 12 and pointers is 439,678"datetime="9/7/2012 11:44:21 AM" />
<logaction="current area is 12 and pointers is 440,716"datetime="9/7/2012 11:44:22 AM" />
<logaction="current area is 12 and pointers is 445,726"datetime="9/7/2012 11:44:22 AM" />
</logs>
```

XII. Conclusions

In this paper, we have presented a new model which has some significant improvements in comparison with old models in pervasive computing such as removing the poster policy from server providers and integrating them with the location-service provider; utilizing general purpose hardwares for implementation; Improving the system response time. For instance, components used in searching the service, by two states of a poster service and designed model are the same, except on the connection time. This connection time, usually is more than 5 seconds which normally the amount of searching time for the server provider is set on that. By removing this part, in any relationship this amount of time will be saved, because the process takes an average of only 500 milliseconds for reading and processing the policies, which clearly is a significant improvement as it saves us some time in searching the service and to review and implement policies.

Overall, a new structure in pervasive computing with using specified policies was proposed by the services and users' preferences, which could perform the user-defined rules in these policies. In this structure, based on previous models such as PAWS, a new system was designed that with some changes, could use a centralized server provider in each building instead of privacy poster system. Therefore, it could rely on an indoor-location detection system, and had the capability to search the services, and review and discuss over the policies. It also features the announcement of change of policy servers to the intangible servers, and integration service providers with locations in atmosphere can save considerable amount of time, and negotiated service could be created. And general hardware system could be implemented.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and associate editor for their extensive and valuable comments.

REFERENCES

[1] Langheinrich M., "Personal Privacy in Ubiquitous Computing, Tools and System Support," PHD thesis,Swiss Federal Institute of Technology Zurich, 2005.

[2] M.Langheinrich, "Personal Privacy in Ubiquitous computing,tools and System Support, "PHD Thesis, Swiss Federal Institute of Technology Zurich,2005.

[3] S.Dritsas, J.TsaParas 'and D.Gritzalis, "A Generic Privacy Enhancing Technology for Pervasive computing Environments, "PP 103-113,3rd International Conference on Trust, Privacy & Security in Digital Business (TrustBus '06),2006

[4] P.Bhaska,S and I.Ahamed, "Privacy in pervasive computing and open Issues,"

[5] The second International conference on Availability, Reliability and security (ARES'07), 2007

[6] Placelab project, available online at http ://placelab.org

[7] A.LAMARCA et al, "PlaceLab : Device Positioning Using Radio Beacons in the Wild, "Proceedings of International conference on Pervasive computing, 'june 2005

[8] P.Bahl and V.N.Padmanabhan, "RADAR : An In-Bulding RF-based User Location and Tracking System, "Infocom, 2008.

[9] R.Harle and A.Beresford, " The Bat System", Ubiquotous computing workshop,2006.

[10] A.Bangs and S.Haerinch, Location Aware Security Application",Bachelor of science Thesis, Worcester Polytechnic Institute, 2006

[11] P.Bahl and V.Padmanabhan, "Enhancements to the RADAR User Location and Tracking System", Technical Report MSR-TR-00-12, Microsoft Research February 2005.

[12] P.Bolliger, "RedPin- Adaptive, Zero-Configuration Indoor Localization through user collaboration",proceedings of the first ACM International Workshop on Mobile Entity Localization and Tracking in GPS –Less Environment computing and communication Systems, San Francisco, USA, September 2008.

[13] R.want, "you are your cell phone,"IEEE pervasive computing, vol.7, NO.2,2008

[14] N.Li,T.Li and S.Venkatasubramanian,"t-closeness:Privacy Beyond k-Anonymity and L-diversity", In IEEE 23rd International conference on Data Engineering, 2007.

[15] A.Machanavajjhala, J.Gehrke and D.Kifer, "L-diversity:Privacy Bevond K-Anonymity, "In IEEE 22nd International conference on Data Engineering, 2006.

[16] L. sweeny, "K-anonymity:Amodel for protecting Privacy, "PP 557-570,International journal of uncertainty, Fuzziness and knowledge-based systems, 2002.

[17] S.T.Wolfe, S.I.Ahamed, and M.Zulkernine, "A Trust Framework for Pervasive computing Environments ", PP.312-319, The 4th ACS/IEEE International Conference on computer Systems and Applications(DASc'06), 2006

[18] R.K.Thomas,R.Sandhu,"Models, Protocols, and Architeeture for secure pervasive computing:challenges and Research Directions, "Proceedings of the second IEEE Annual Conference on Pervasive computing and communications Workshops (PER COMW'04), 2004.

[19] S.Nagvi and M.Riguidel,"security and Trust Assurancse for Smart Environments,"IEEE International Workshop on Resource Provisioning and Management in sensors network 2005(RP MSN 05), 2005

[20] M.Satyanarayanan,"Pervasive Computing :Vision and Challenges,"PP 10-17,IEEE Personal communications,VOL 8,Issue 4,2001.

[21] SUD. KUMAR, SINGH, ALKA JINDAL,"An Approach for Location privacy in Pervasive Computing Environment", International Journal of Engineering Science and Technology Vol. 2(5), 2010.

[22] Sh. Mohsen, Na.Leila Providing,"location privacy in pervasive computing through a hybrid mechanism", PP 160-173,Int. J. Internet Technology and Secured Transactions, Vol. 2, Nos. 1/2, 2010.

3/22/2013