Privacy in Pervasive Computing Environment

Gnaneshwari G. R., M. S. Hema

ABSTRACT--- ***Pervasive computing evolved tremendously as an exciting new paradigm to provide data collection, computing, and communication services all the time and everywhere. It has introduced a new world of computing and became an integral part of many fields and application domains. It allows users to interact with wired and wireless networks that support any information technology. In spite of many advantages associated with pervasive computing, communication services have some security risks. For sensitive and confidential data there should be some security mechanisms. In this paper, we present privacy issues and challenges that are preventing people from adopting the pervasive computing environment and we give a survey on the solutions that have been carried to minimize risks.***

Keywords — Privacy Preserving; Pervasive Computing Environment; Access Control; Authentication; Anonymity.

I. INTRODUCTION

Information processing started with the human mind power, expanding his thinking ability provided the computer revolution of mainframe era, where many people used one large computer at a fixed central location. Miniaturization and decentralization of mainframes lead to personal computing era with one system for each individual fixed but decentralized. Further, the Unification of computing and communication is going by surpassing the huge desktop computers and leads to smaller and also more compelling devices. These small and powerful devices provide excellent computing capabilities to process and store data, being movable and low power battery supported. They are able of getting connected to other devices, internet, and/or various complex wireless communication interfaces. The tools such as personal digital assistants (PDAs) and Smartphone's allow a new set of services portrayed by being available anywhere, at any time and for anyone [1] guided us to the era of ubiquitous computing also known as pervasive computing where one person has many computers and not fixed.

Pervasive computing is a thought in computer science where computing is made to perform anytime and everywhere in a network. The general block diagram of the Pervasive Computing Environment (PCE) is shown in Fig: 1. PCE includes sensors, embedded systems, low cost and low power connectivity, smart material and designs, IOT (Internet of Things) applications, pervasive computing applications. The main interest of pervasive computing environments is to address the generation with more comfort by giving mobile gadgets and digital support capable of presenting the appearance of any type of service in environments wherever people reside, operate or socialize.

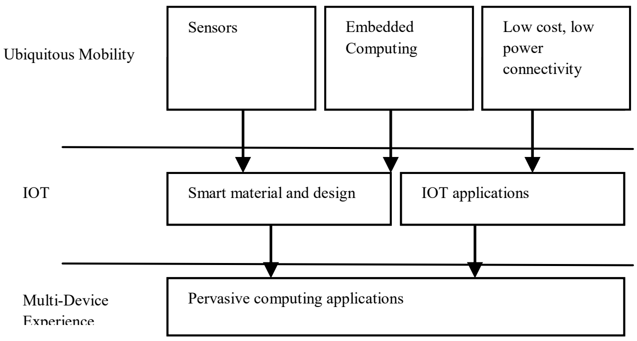
Ubiquitous Mobility
Sensors
Embedded Computing
Low cost, low power connectivity
IOT
Smart material and design
IOT applications
Multi-Device Experience
Pervasive computing applications

Fig 1: General block diagram of Pervasive Computing Environment

II. APPLICATIONS OF PCE

Pervasive computing intends to penetrate and interconnect each sector of life for various applications as mentioned below,

Communication: It influences each and every kind of exchange and release of data, message, and knowledge. It's a precondition to all kinds of learning technology.

Logistics: It offers possibilities for optimizing and automating the complete transport connection of unfinished materials semi-finished materials and finished goods.

Motor traffic: It includes various relief systems that serve the driver quietly.

Military: It helps in preventing and fighting external threats.

Production: It helps a decentralized design that will individually configure, manage and observe itself.

Smart places: A large number of home, hospital, and hotel technology accessories such as lighting, heating, and oxygenating and communication tools become active devices that automatically adapt to individual needs of inhabitants.

E-business: Facilitates automatic fund transfer, supply chain management, internet marketing, electronic data interchange etc.

Personal security: Identification methods, such as electronic identification and the expensive smart cards are some examples of purposes.

Medical technology: To monitor the well-being of each aged in their individual houses [2, 3], as well as for deep implants and many more.

Revised Manuscript Received on July 10, 2019.

Gnaneshwari G R, Research Scholar, Sri Venkateshwara College of Engineering, Bangalore, India. (E-mail: gecgnani@gmail.com)

M. S. Hema, Computer Science Department, Aurora & Scientific Technological and Research Academy, Hyderabad. TS, India (E-mail: ghema_shri@yahoo.co.in)

The paper is organized in the following way in Section I we describe an Introduction and general block diagram of Pervasive Computing Environment; Section II discusses applications of PCE; Section III summarizes issues and challenges in PCE; Section IV includes privacy issues, approaches, and solutions, Section V presents conclusion and future directions for research.

III. ISSUES AND CHALLENGES OF PERVASIVE COMPUTING ENVIRONMENT

The features and wide functions that the pervasive computing offers, makes it reasonable to increased exposures and vulnerabilities. Characteristics that add some additional burden on to the protection subsystem and become major issues and challenges in PCE are:

Expansion of Computing Boundaries: The conventional computing combined software and hardware objects, while pervasive computing stretches the bounds of computing to combine physical areas, building support, and the things contained inside. This physical outreach can help the invaders, spiteful insiders or even questioning system administrators to track users to the most important part and get his or her personal details which make preserving privacy a more difficult task.

Invisibility and Unobtrusiveness: The objective of pervasive computing happens to be invisible and unnoticeable. Thus, technology is installed within everyday things that send and receive data. The installation diminishes the distinctness from the pervasive computing environment enclosing the user. This makes technology more pleasant and acceptable. Ironically, this very quality makes it probable to attack the user privacy without his realization.

Creating Smart Spaces: Sensors and Embedded devices are combined to set natural surroundings into active areas which can sense, “recognize,” and “learn,” completely, making each area aware and tractable. Eventually, the area becomes quite intelligent to get user's intent. Thus becomes a basic component of user’s daily life which leads to privacy risks.

Spot Dependency: Spot data or location information of the user is required to provide most of the services in PCE. To make use of these services the user has to provide his location details to the service provider. Thus the knowledge of user location information can provide a route for its misuse. Location of a user is privacy-sensitive information that can be easily accessible making its security a challenge.

Context Dependency: The applications of Pervasive computing also depend upon the data of context. The information can involve the kind of broadcasting device used by the application, user forms, GPS (Global Positioning System), user decisions, current time, etc. Contextual information can enhance the user attributes which can help in developing privacy protection. But on the other hand, it is difficult to provide adequate protection for context information from context-aware systems. As the data collected by this context-aware systems might have different privacy requirements due to the diversity of awareness and conclusion of users.

Amount of Data Collection: The data collected by pervasive computing is drastically increased when compared with the traditional computing technology. Pervasive computing implementation depends upon the increased amount of data generated and collected with quality and accuracy. The system also provides enhanced processing and analyzing capabilities of data. This minute amount of data gathered and processed leads through users often neglecting and releasing of personal data. Also, the technology makes use of bulk of wireless devices. The devices have limitations for bandwidth, memory, processing, battery, throughput etc. These factors establish a resource constraint upon detailed standards and protocols for privacy protection which depends on the widespread use of such resources.

Role of Service Provider: Service provider plays a crucial role in maintaining and preserving privacy-sensitive data of the user. There is every possibility for ill-usage of data moving through the devices from the service provider. Platform for Privacy Preferences (P3P) from the World Wide Web Consortium (W3C) presents a specification that can stand to guarantee that all data request through the service providers also stipulates purpose, retention, and receivers of the data. While in the real-world guaranteeing that all service providers obey the laws is difficult.

Lack of Ownership: In traditional computing, the resources have ownership and access control. The pervasive computing environments implement dynamic and looser couplings among people and devices. This nullifies the unspecified ways to ownership and handling of resources. But it is tough to achieve privacy check while ownership cannot happen to be determined.

Mobility and Adaptability: Adaptation and mobility are needed to overcome the changing nature, versatility of users, devices and software segments leading to the changes in the physical and virtual environment of the pervasive computing environment.

Wireless Problems: Including several similar standards, Lack of spectrum, Use low power and multiple base stations with intelligent antenna. Extending spectrum usage can cause interference.

Scalability: Hundreds and thousands of distinct devices are hosted at Pervasive computing environments with many users having different functions and priorities supporting various situational data. Unique security services should signify the ability to reflect the lying of mobile and embedded devices accessible at any particular instance of time and support its users.

IV. PRIVACY ISSUSE IN PERVASIVE COMPUTING ENVIRONMENT & RESULTS

The applications of Pervasive computing are dramatically increasing every measure concerning towards the data collected and released. It is obvious that a user in pervasive computing environments wishes to maintain different connections with various smart devices reckless of the software restrictions and hardware specifications. Such devices and applications intend to increase the amount of personal information released to the service providers and third parties. The user inevitably feeds the personal information in an online job application, in shopping malls using credit card etc. Data from sensors and cameras located at different geographical and indoor positions collectively engage in the representation of the necessary service without the conscious or explicit knowledge of the user [4]. This information collected, shared, stored and processed may be inappropriately handled to add up in different that involve prejudice, identity theft, the undesirable advertisement, or constant stalking. It does not stay as a new problem for networks in general but advanced technology has increased several privacy breaches. Hence, privacy protection in pervasive computing is becoming more and more challenging. And almost all the other issues and salient features of a pervasive computing environment are also vulnerable to privacy in one or the other way.

A. Privacy issuse and Approaches

We focus on few prominent issues and approaches towards preserving privacy as shown in Fig 2.

Authentication: Privacy has to ensure that data being shared or communicated is not being hacked by any active or passive attackers. It has to guarantee that the user data which is being collected almost obviously will not be used maliciously or is not being processed by any unauthorized user. In order to ensure about data not being accessed by the unauthorized user, modern approaches are must for entity authentication to validate the user's integrity, in sequence to cope with those new challenges offered due to extreme distribution and mobility of the system.

Access Control: It is to grant access completely to the significant data and avoid unnecessary irrelevant data for any particular service. Access control mechanism is needed to decide whether to permit or reject an assigned unit the liberty to do a specified action. Access control method includes the tests in the field of the database, operating system, and distributed system. But pervasive systems possess unique features which let distinct access control methods. Unrestricted access control (DAC) methods, here the authorizations depend on the characteristics of the subject, which is well-matched for unstructured domains similar to basic internet services. Feature-based installation is dependent on the theme's role within the structured organization like companies, hospitals etc.

Anonymity: Many of the applications in pervasive computing environment do not rigidly need to know the identity of the user. Anonymity provides the user with the functionality which helps the user to be known to others or remains unknown to others or to be known with the different identity. Anonymity is derived from databases (DB) and the distributed approaches and the use of pseudonyms [5, 6].

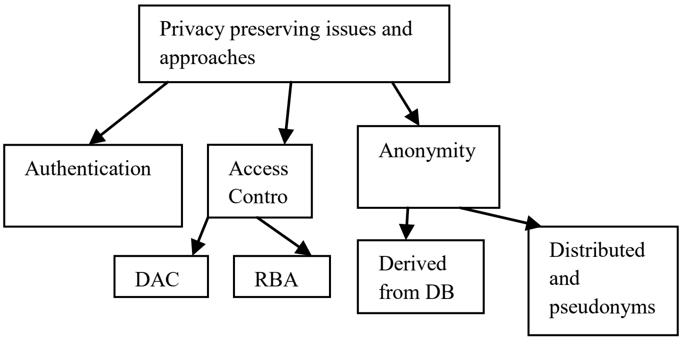
Privacy preserving issues and approaches
Authentication
Access Contro
Anonymity
DAC
RBA
Derived from DB
Distributed and pseudonyms

Fig 2: Different Privacy Preserving Issues and Approaches

B. Solutions

Several research papers have been published related to privacy management technique's in pervasive computing. Few of them are summarized with the highlights of the work as shown in Table I.

Marc Langheinrich [7] proposed a privacy awareness system targeted at ubiquitous computing environments that allowed data collectors to both announce and implement data usage policies, as well as providing data subjects with technical means to keep track of their personal information as it is stored, used, and possibly removed from the system. The author says still the system cannot guarantee our privacy, but creates a sense of accountability in a world of invisible services that we will be comfortable living in and interacting with.

Chun-Ta Li, Cheng Chi Lee, Chi Yao Weng [8] proposed an extended chaotic map and dynamic ID-based user authentication scheme which is suitable for pervasive computing environments and was explained with the example of online financial transaction for remote user authentication to verify the legitimacy of a login user over an insecure communication channel along with ensuring anonymity and preventing denial of service attack and thus the attackers cannot inconvenience the login user.

Emmanouil Magkos, Panayiotis Kotzanikolaou [9] shows how the RL scheme has privacy and security vulnerabilities under his threat model which considered users equipped with front-end entities and back-end authorities and enhanced the scheme with the generic approach for privacy and security in controlling access to pervasive computing environments.

Table I: Various papers on Privacy Preserving in PCE

Reference	Approach	Issues addressed	Security mechanism	Other features
[7]	pawS	Access control	Accountability	Announce and implement data usage policies
[8]	Extended chaotic maps	Authentication	Dynamic ID based	Ensure anonymity and prevent DoS attacks

[9]	Generic scheme	Access control	Public-key and Symmetric-key	Untraceability unlinkability Accountability
[10]	User-centered Privacy Model (UPM)	User control over content, identity, location, and time	Five parties for communication within three layers	Highly scalable, unobtrusiveness
[11]	Service Discovery protocol	Service provider privacy, alternate paths using different keywords	Member ship verification	Authentication, Anonymity, Accountability, Scalability
[12]	Context aware Privacy model (CPM)	Anonymization and obfuscation	Mechanisms for reducing the number of context data	Improve the quality of service
[13]	Siafu context simulator	Anonymity	Defense based on fake requests	defense against shadow attack
[14]	UbiOulu Research	Authentication	Verifying privacy certificates	Privacy toolkit
[15]	Privacy preserving at application layer	Anonymity	Capability based scheme for authorization and authentication	Simple, cost effective, minimum storage, less computational time, efficient.
[16]	Location Fragmentation]	Privacy of location	Vertical Fragmentation	-
[17]	Trust model	Privacy of data mining	Association rule mining with classification	Dynamically make trust decision

The generic approach provided the desired level of privacy against malicious insiders while balancing with competing demands for access control and accountability.

Ali Dehghantanha, Nur Izura Udzir, Ramlan Mahmod [10] presents the evaluation of an XML based User-centered Privacy Model (UPM) and measure unobtrusiveness. It provides user control over private information, content, identity, location, and time. The model is highly scalable because of its distributed decision-making processes and its platform independence. But still work needs to be carried out for concurrent, multiple authentication methods, the probability of collusion attack that can result from the collision of lighthouses and portals, and to communicate without XML format.

Jangseong Kim, Joonsang Baek, Kwangjo Kim, Jianying Zhou J Camenisch and C Lambrinoudakis [11] proposed a discovery protocol for ubiquitous computing environment which performs efficient membership authentication while limiting information leakage concerning to privacy from a semi-honest directory server. The protocol is practical but the transmission cost for membership authentication increases linearly. The author also suggests each service provider divide its subscribers to many subsets, which will reduce processing delay and cost. The protocol further supports anonymous authentication in a service access phase without additional computation cost.

L. Pareschi, D. Riboni [12] proposed the architecture which is the extension of the CARE middleware for context-awareness called context-aware privacy module (CPM). This paper presents preliminary results on anonymization and obfuscation techniques to preserve users' privacy in context-aware service provisioning. The techniques are based on generalizing request parameters as well as the context data provided to the application. Local context semantic aggregation is used to improve the quality of service.

L. Pareschi, C. Bettini [13] considers a specific pervasive computing scenario called per gym and shows that the techniques for the anonymization of service requests are insufficient to protect the privacy of users. The experiment concentrated on protection against a specific class of attacks, called shadow attacks, and not on generic attacks and simplified the assumptions by taking into account the only location.

Tomas Linden, M Rautiainen [14] presents a conceptual framework for enabling technological solution, which aims at realizing the key requirements, trustworthy: privacy certifying hardware, and software, affordable: compatible hardware at low cost, easy to deploy and maintain, open: compatible software easy to create, share, install and interoperate, resilient: should have high resilience towards service disruptions such as network problems, denial of service attacks. It leverages the results from several subfields including privacy-preserving computing, user innovation, free software, living labs, distributed computing as well as distributed web applications.

D.M. Konidala, D.N. Duc [15] provides a scheme for application layer where the user authentication, authorization, and privacy protection are considered. In order to have clear transparency of the work, the protocol does not involve confidentiality and integrity. The scheme is easy and effective which comprises three entities: Authorized server (AS), service providers (SPs), and users. It lets the users to anonymously communicate with SPs and the SPs can authenticate and authorize the users based on the anonymous report proposed by the users. The author says the scheme is original of its kind to introduce capability based privacy preserving for PEC which is cost-effective with respect to storage, computation and time complexity. The SP does not know the user's real identity and also the services accessed by the user.

Jeeva Susan Jacob, Preetha K [16] discusses the issue of Location Privacy of users in Pervasive computing environments. Vertical Fragmentation technique has been proposed as a solution for the attacks on Location Servers and theft of location information. Its effectiveness in preventing third-party attacks and fake users has been analyzed theoretically. Even though internal attacks cannot be prevented, it ensures location privacy for the users of a reliable service provider.

Gianni D Angelo, Salvatore Rampone [17] proposed a mechanism in which the trust model was used to make decisions based on various sources of context and trust data. The architecture was designed for pervasive computing environment which was capable of making a human-like decision. It used the soft computing techniques with the integration of association rule mining and classification. Test results confirmed that the proposed trust model was capable to recognize the tactics adopted by the wicked entities during three typical attacks: counting-based, time-based and context-based. The trust model used to learn the tactics as early as they appear which were not identified by the traditional approach.

GuanghuiWang, Jianping Pan and He, Subin Shen [18] presents a model for protecting location privacy which is important for various location-based services in pervasive computing scenarios. An adjacent subtraction based localization model with localization algorithm which is suitable to efficiently protect users' privacy. The classical method had much computation and communication overheads to achieve privacy-preserving localization. A comprehensive analysis, including correctness analysis, privacy analysis, and efficiency analysis, is presented. Some simulations are conducted to show that the proposed model has equivalent accuracy and efficiency with the classical model.

It can be seen that there remains neither single protocol nor mechanism that can approach the privacy issue and suffice the obligations and expectations of safe pervasive computing. Therefore, it is difficult to find an effective privacy preserving method proposed in the literature. Furthermore, security itself consists of a mix-up of many general features each of which needs thorough research including customized resolutions. It is necessary to consider different application programs of pervasive computing and classify the requirements they impose in conditions of privacy and balance the service excellence. In addition to the exact requirements based on different applications we must also identify some common set of requirements for example: The users to be conscious of the data they are sending and receiving, this requires to know about the activeness of sensors, what type of data is collected, who is collecting the data, what they are going to do with that data. Rules should be imposed on to the organizations that collect responsive data to make them accessible to the owner. User friendly interface, clearly tells what kind of data analysis it performs, how data is used, and how the personal data that is strictly needed should be collected which altogether tells about transparency and minimization of data collection as a first and foremost common requirement.

Considering both general and exact requirements of privacy and then finding out a solution for protecting it will fill the research gap. A single computing approach may not be sufficient to achieve this complex goal. An approach needs to combine the knowledge, techniques and methodologies from various sources. It must be computationally intelligent, possess human like expertise within a specific domain and have the ability to adapt and learn in the changing environment.

V. CONCLUSION AND FUTURE DIRECTION

Pervasive computing makes life more comfortable and simple in digital environments. While it also imposes many new security risks which are related to privacy of the user and data. We have mentioned the applications of PCE, issues, and challenges that lead to threat the privacy. The different aspects of privacy-preserving approaches and solutions in the pervasive computing environment are discussed. Further studies need to be carried out in order to develop/implement more intelligent and accurate approaches for the assent of a pervasive environment in daily life by using soft computing techniques.

REFERENCES

1. Weiser, M., "The computer for the 21st century". Scientific American 265, pp 94-104, 1991.
2. Claudio Bettini, Daniele Riboni, " Privacy Protection in Pervasive Systems: State of the art and technical challenges", Pervasive and mobile computing 17, pp159-174, 2015.
3. P.S. Efraimidis, G. Drosatos, F. Nalbadis, A. Tasidou, "An efficient privacy preserving solution to find nearest doctor", Pers. Ubiquitous computing, 18, 1, pp75-90, 2014.
4. Hyo Jin Jo, Jung Ha Paik, and Dong Hoon Lee, "Efficient Privacy Preserving Authentication in Wireless Mobile Networks". IEEE trans, Mobile computing, 2014.
5. I. Boutsis, V. Kalogeraki, "Privacy preservation for participatory sensing data", IEEE International Conference on Pervasive Computing and Communications, pp. 103–113, 2013
6. D. Christin, C. Roßkopf, M. Hollick, L.A. Martucci, S.S. Kanhere, Incognisense: an anonymity-preserving reputation framework for participatory sensing applications, Pervasive Mob. Comput. 9, 3 ,pp 353–371, 2013.

7. Langheinrich, M., “A privacy awareness system for ubiquitous computing environments”, in the Proceedings of the 4th international conference on Ubiquitous Computing, (Sweden). International Journal of Distributed and Parallel Systems (IJDPS) 3, 3,pp 217-224, May 2012.
8. Chun-Ta Li·Cheng-Chi Lee·Chi-Yao Weng “An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments” Nonlinear Dyn 74:1133–1143 DOI Springer Science+Business Media Dordrecht 2013.
9. Emmanouil Magkos and Panayiotis Kotzanikolaou “Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments” A.U. Schmidt et al. (Eds.): MobiSec Institute for Computer Sciences, Social Informatics and Telecommunications Engineering LNICST 47, pp 53–64, 2010.
10. Ali Dehghantanha, Nur Izura Udzir, and Ramlan Mahmod ´ “Evaluating User-Centered Privacy Model (UPM) in Pervasive Computing Systems” Springer-Verlag Berlin Heidelberg, CISIS, LNCS 6694, pp 272–284, 2011.
11. Jangseong Kim, Joonsang Baek, Kwangjo Kim, and Jianying Zhou J. Camenisch and C. Lambrinoudakis “A Privacy-Preserving Secure Service Discovery Protocol for Ubiquitous Computing Environments” Springer-Verlag Berlin Heidelberg (Eds.): EuroPKI, LNCS 6711, pp 45–60, 2011.
12. L. Pareschi, D. Riboni, A. Agostini, C. Bettini. “Composition and Generalization of Context Data for Privacy Preservation,” 6th Annual IEEE International Conference on Pervasive Computing and Communications, pp 429-433. 2008.
13. L. Pareschi, D. Riboni, C. Bettini, “Protecting Users’ Anonymity in Pervasive Computing Environments,” 6th Annual IEEE International Conference on Pervasive Computing and Communications, pp 11-19, 2008.
14. Tomas Lindén M. Rautiainen, “A Conceptual Framework for Enabling Community-Driven Extensible, Open and Privacy-Preserving Ubiquitous Computing Networks” Springer-Verlag Berlin Heidelberg, (Eds.): GPC workshops, LNCS 7096, pp 156–163, 2012.
15. D.M. Konidala, D.N. Duc, L. Dongman, K. Kwangjo, “A Capability-Based PrivacyPreserving Scheme for Pervasive Computing Environments”, 3rd IEEE International Conference on Pervasive Computing and Communications, , pp 136-140. Mar 2005.
16. Jeeva Susan Jacob and Preetha K.G. J. “Enabling Location Privacy in Pervasive Computing by Fragmenting Location Information of Users” Mathew et al. (Eds.): ICECCS, CCIS 305, Springer-Verlag Berlin Heidelberg, pp 364–371, 2012.
17. Gianni D’Angelo, Salvatore Rampone, Francesco Palmieri, “Developing a trust model for pervasive computing based on Apriori association rules learning and Bayesian classification” Springer-Verlag Berlin idelberg May 2016.
18. GuanghuiWang, Jianping Pan and He, Subin Shen “An efficient privacy preserving localization algorithm for pervasive computing” Computer Communication and Networks (ICCCN), 18 September 2017 26th International Conference.