ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

Privacy, Security and Trust Related Issues in Pervasive Computing

Rohit Tiwari[1], Monika Kohli[2]

Assistant Professor, Computer Engineering & Information Technology Department,

K.J. Institute of Engineering & Technology, Savli, Vadodara, Gujarat, India[1,2]

Abstract: Our routine life can have a consistent assimilation of automated infrastructure with the help of pervasive computing environments having interconnected devices and services promise. With the possibilities of adding new devices to the herd of pervasive computing devices and developing new and effective applications to enhance functional performance, there is another flip of the coin is there having privacy and security issues in pervasive computing environments, which are, unfortunately, not delved into an appropriate extent. The user experience is made superior by accessing the context information about the resources and users and their physical location by the pervasive computing application, but eventually helping in exploitation, which was not possible in the traditional distributed computing because of its nature of abstracting away the physical location of resources and users. The need of resource sharing and collaboration is giving birth to different types of communication not only amongst users but between the physical and virtual worlds as well. And it is making the separation of physical security from digital security altogether is very difficult. There are so many new vulnerabilities has been exposed by the pervasive computing paradigm and existing policies and security mechanisms cannot provide adequate guarantee do deal with this new environmental exposure. In this paper, the authors are putting their combined efforts to explore the challenges for security and privacy into pervasive computing environments.

Keywords: Pervasive Computing, Privacy, Security, Transparency, Interoperability, Scalability

I. INTRODUCTION

We are experiencing the confinement of an innovative computing paradigm that promises to have an insightful effect on the manner we work over computers, devices, physical spaces, and other people. This novel technology draws a picture of a world where embedded processors, computers, sensors, and digital communications are reasonably priced commodities which are available all over the place. This is completely removing time and place barriers by making services available to users every time and everywhere. Pervasive computing will encircle users with a relaxed and suitable information atmosphere which is an amalgamation of physical and computational infrastructures into an incorporated habitation. This environment will feature a propagation of hundreds or thousands of computing devices and sensors providing new functionality, offering dedicated services, and boosting efficiency and communication. Context-awareness will allow this environment to become accountable for helping users, by customizing itself to their requirements, while executing jobs and cluster activities as per the nature of the physical space as well. This information-affluent and dynamic environment is known as an active space. And this space has people who are able to communicate with custom applications which are tagging along with the user, defining and controlling the activities of this active space and/or cooperating with distant users and applications.

II. ARCHITECTURE OF PERVASIVE COMPUTING

As pervasive computing is treated as a system having interaction among a horde of assorted devices which are connected to each other through wireless communication technologies. The devices from specific environment are able to share their functionality with the neighbouring devices for the achievement of reciprocal profits. The primary components of the architecture of pervasive computing are basically categorized in three research areas namely Basic Research, Technology-oriented Research and Applied Research.

A. Basic Research: The basic research part in the architecture of pervasive computing is all about making a firm base over which the complete system can be dependent upon. As shown in the figure this part is a composition of Sensor Networks, Embedded Computing and Distributed Computing. The Sensor Networks are an amalgamation of Sensor Fusion-where the sensors are being fixed in the devices, Sensor Selection-where the appropriate sensors are selected as per the requirements, and Distributed Data Analysis-where all the data collected by different sensors is being analysed for further course of action [2].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

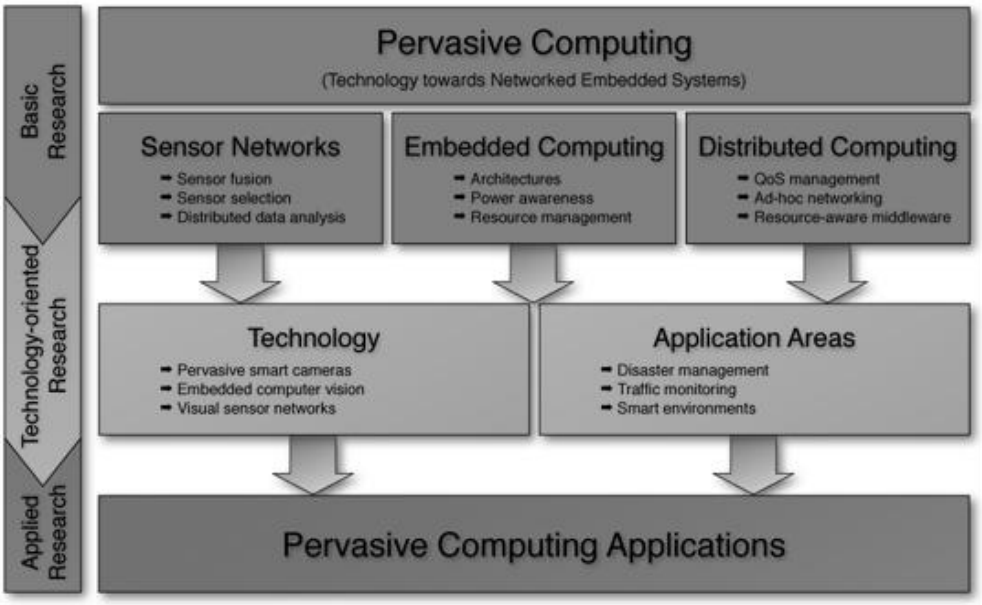

Fig. 1Architecture of Pervasive Computing

The second subpart Embedded Computing is having core infrastructural architectures, awareness of power usage during the operation, and the resource management of whole system is being performed by this part only. The final subpart known as Distributed Computing is managing Quality of Service (QoS) throughout the pervasive computing system, and it is also responsible for the implementation of Ad-hoc Networking and a middleware which is providing services to the resources.

B. Technology-oriented Research*:* The middle part of the architecture deals with the technological aspects and applicable areas of pervasive computing. The technological aspects are dealing with the pervasive smart cameras providing an embedded computer vision with the help of visual sensor networks. While the application areas of pervasive computing are having ongoing research for pervasive computing to be implemented for disaster management and traffic monitoring, and for creating smart environments.

C. Applied Research*:* The final component of the pervasive computing architecture is talk about the actual implementation of this technology in the real life and actually making this wonderful technology to contribute towards making human life better. Some of the examples of pervasive computing to be incorporated in the human life are Smart Clothing, Healthcare Monitoring System, Smart Home, Smart Cars etc. and all these applications are implemented completely with the help of pervasive computing design and implementation approach.

III. SECURITY CHALLENGES

Here in this segment, we will be addressing the significant challenges and requirements to secure the environments of pervasive computing. Being additional in features and providing extended performance, the pervasive computing making itself susceptible to further unwanted exposures and vulnerabilities. Here we are addressing the features of pervasive computing adding additional load to the security subsystem.

A. The Extended Computing Boundary*:* When it comes about consisting program and data, the traditional computing can be said circumscribed with the world of virtual computing. The physical locations of resources and users can be abstracted away as implicated by the latest distributed computing research. On the other hand notwithstanding, the influence of Pervasive computing can be extended beyond the computational infrastructure, and also at the same time it is perusing to embody the surrounding physical spaces as well. Just to improve the end user experience, the location and other related information of resources and users are being exploited almost every single time by the applications of Pervasive Computing. The physical security and the information become independent under such situations. And as a result of this, these environments are made susceptible to additional extreme security threats, which can be compared between the threatening of devices and people in the physical world and threatening for their programs and data in the virtual realm. And this is the prime reason for the traditional practices of security became incompetent by not addressing digital security in a proper manner.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

B. Privacy Issues*:* The privacy of the users of the pervasive computing users is always at stake because of its physical and geographical coverage. Spaces with better intelligence and better capabilities of computing, which are considered to be technically omnipresent, can be constructed by adding active spaces having active sensors and actuators. Such active spaces are capable of being customized as per the preferences of the user and also capable of capturing and completely utilizing the context information, by using innumerable embedded devices and sensors. But, looking at the other side of the coin, it is quite unfortunate that this feature may act as the prime reason to pose a severe threat to the user's privacy viz. this functional aspect can be misused by malevolent insiders and/or invaders, or even by some snooping system administrators to track or electronically stalk specific users. This whole system can be considered as a dispersed observation system which is recording considerably abundant statistics about users. There is a complete list of such environments where in there is generally an affluence of personal and sensitive information, to which the security is a must. At the same time, there can be situations, when the users are not willing to be tracked.

C. User Interaction Issues*:* Pervasive computing applications are comparatively having a very rich user interface for user's interaction with the active space and it is considered as one of the most fundamental and important aspect of the development of pervasive computing applications. To provide user input and output, in parallel to the controlling of physical aspect of the space, there is an assortment of multimedia mechanisms are being practiced. The security properties of the space can be affected by the set of users in the space at any moment of time. Users in the space are not capable enough of being prevented effortlessly from seeing and hearing ongoing things in it, and it is caused by the nature of such interactions. And while designing the access control mechanisms this must be taken into appropriate considerations. The active space should be allowed by the access control mechanisms to be used by devices and users in such a manner that not only facilitates the collaboration, but also enforces the suitable access control policies and averting unauthorized usage. And that is why there is a need for consideration of physical and virtual aspects of access control altogether for such spaces.

D. Security Policies: The security mechanism in pervasive computing must be defined and managed using a flexible and expedient method and that too in a vigorous and malleable fashion. The administrators are equipped with a Policy Management tool to enforce a better and superior control over the conduct of entities in their systems by enabling the capability to stipulate, contrivance, and implement rules by the systems administrators. These systems administrators are enforcing most of the network policies nowadays with the help of scripting applications based tools. The comprehensive database of reciprocal device and resource interfaces is being managed by the policy management software. As there is a constant need to update all such tools to accommodate new software or hardware, makes the overall system management difficult. And because of this the functionality of the ordinary low-level management tools becomes limited compelling them to enforce only generic policies. There is a possibility of administrators not knowing the exact scenario of consequences of their policy management actions, as major policy management tools are dealing with such low-level interfaces. The objects may cause unanticipated cross effects and objectionable behaviour because of dependencies among them. Also, the security policies cannot be disclosed as it may be treated as a fissure in the security system. And that is why any unofficial personnel should not be allowed to know anything about the changing behaviour of the security policy in a specific context.

IV. SECURITY REQUIREMENTS

The architectural aspects of the pervasive computing are giving birth to new susceptibilities, and this is why, instead of being considered as additions or addendums, the privacy and security implementation procedures, providing assurance, should be defined and conscripted in the initial stages of design process. Efforts has been made in the past to accommodate security with anonymity into the existing systems, but all went in vain being neither effective nor efficient. In this particular section, the authors will be discussing the crucial requirements which are required to provide a successful and sustainable security system for pervasive computing paradigm [6].

A. Transparency and Unobtrusiveness: The essence of pervasive computing is all about transmuting its end users into first class entities, thus by enabling them not to provide more and more attention and efforts to the computing technology. All the security systems should be transparent enough not to distract the end users by mixing into the implementation mechanism.

B. Multilevel: The security mechanism should be devised in such a manner to cater security at different levels and these levels will be built upon so many factors including environmental circumstances, chronological situations, system policy, accessible resources, context information etc., because we cannot have one security system serving all requirement at once. And that is the prime reason create a multilevel security system defined in different levels to cater the requirements of different types of users.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

C. Context-Awareness: It has been observed that the conventional security systems are found context insensitive and static in nature. On the other hand, pervasive computing is integrating situational and contextual information, thus by transmuting the computing atmosphere into a responsive space. The context information should have been used extensively by the security services. But at the same time this received contextual information must be verified against its genuineness and reliability. However, it is not possible for a policy to change its behaviour in a particular time or under a particular situation. Therefore it becomes obligatory at times to prevent such incorrect context information acquired from reprobate or faulty sensors.

D. Flexibility and Customizability: The security system should be malleable, lithe and customizable as per the requirements. In the real world there is a possibility of having the working environments with extreme situations and insufficient resources. The security system should not only survive such conditions but, when there is ample availability of resources, it should be capable enough to grow and provide supplementary functionality. As the working milieu is dynamic itself, the tools required for defining and managing policies should be same as well.

E. Interoperability: It has been proved that a specific security practice is not sufficient and/or cannot guarantee the success of securing completely, because there are numerous diverse security technologies are not only evolving but also being deployed. And that is the prime reason and making it a compulsion that not only various security techniques should be supported but the security requirements should be negotiated as well.

F. Extended Boundaries: Nowadays it has become compulsory for the security mechanisms to integrate some facets of the physical world as well, which was missing in the earlier traditional security systems as those were constrained to the virtual world viz. with the help of this the intruders can be prevented from entering into physical places. In a nutshell, there should be an independent kind of relationship between physical and virtual security.

G. Scalability: It is the capability of pervasive computing environments to accommodate hundreds or thousands of miscellaneous devices. The security mechanisms should be in such a manner that it is able to provide the assurance of security to all embedded and mobile devices in the network at any specific fraction of time. Apart from this, a great number of users having diversified roles and rights and working under diverse situational statistics, must be supported by such security services.

CONCLUSION

There are so many new upcoming challenges to the privacy and security of end users, which are a result of shifting from the traditional computing approach to the pervasive computing archetype and these upcoming challenges cannot be resolved with the measly variation of prevailing privacy and security systems. The pervasive computing environs are quite prevalent to the susceptibilities and acquaintances, if the security and safety issues are not addressed initially in the design stage.

It is still a possibility in near future that we will not only be able to create a comprehensive and fully integrated pervasive computing, but their real-life implementation will be possible as well. Although it has not been experienced yet, but security is considered to be an indispensable part of the entire pervasive computing system. It must be kept in mind, while addressing the security requirements, that at present there is no single protocol or a security system which is able to handle all the security concerns and cater all of the expectations and requirements of the secure pervasive computing.

ACKNOWLEDGMENT

This work was supported by **Dr. Ashok Kumar Jetawat,** the authors thank to, for his kind guidance in the research and as reviewer to this research paper. The author would also thank the KJIT management for their astonishing support in the research.

REFERENCES

[1] Khan, V.J., Markopoulos, P, Eggen, B., Metaxas, G., Evaluation of a pervasive awareness systemdesigned for busy parents. Pervasive and Mobile Computing, 6(5), pp. 537-558, 2010.
[2] Lee, A., Boyer, J., Drexelius, C., Naldurg, P., Hill, R., & R. Campbell, (2005) “Supportingdynamically changing authorizations in pervasive communication systems”, in the 2nd InternationalConference on Security in Pervasive Computing.
[3] Z. Liu, P. Naldurg, S. Yi, R. H. Campbell, and M. D. Mickunas, "An Agent BasedArchitecture for Supporting Application Level Security," presented at DARPAInformation Survivability Conference (DISCEX 2000), Hilton Head Island, SouthCarolina, 2000.
[4] E. A. M. Luiijf, "Information Assurance and the Information Society," presented atEICAR Best Paper Proceedings, 1999.
[5] Creese, S., Goldsmith, M., Rosco, B., &Zakiuddin, I., (2003) “Authentication for pervasivecomputing”,in the Proceedings of the First International Conference on Security in PervasiveComputing, (Boppard, Germany).

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

[6] Garzonis, S., O'neill, E., Kostakos, V., Kaenampornpan, M., & Warr, A., (2004) "A novel approachfor identification and authentication of users in a pervasive environment", in the proceedings of the2nd UK-UbiNet Workshop, (University of Cambridge, UK)
[7] Kagal, L., Finin, T., & Joshi, A., (2001c) "Trust-based security in pervasive computingenvironments". IEEE Computer, 34(12), 154-157.
[8] Chatfield, C., &Hexel, R., (2005) "User identity and pervasive computing: User selectedpseudonyms", in the Workshop on UbiComp Privacy: Privacy in Context,, (Tokyo, Japan).
[9] Haque, M., & Ahamed, S. I. (2006). Security in Pervasive Computing: Current Status and OpenIssues. International Journal of Network Security, Vol.3 (No.3), 203–214.
[10] M. Román, C. K. Hess, R. Cerqueira, A. Ranganat, R. H. Campbell, and K.Nahrstedt, "Gaia: A Middleware Infrastructure to Enable Active Spaces," IEEEPervasive Computing (accepted), 2002.
[11] A. Zimmermann, A. Lorenz, R. Oppermann, An OperationalDefinition of Context, 6th Int'l and Interdisciplinary Conference onModeling and Using Context, 558-571, August, (2007).