Volume 6, Issue 2, February 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security in HealthCare Monitoring: A Pervasive Computing Application

Hitender Singh Jalal
Research Scholar
Bhagwant University, Ajmer, India

Prof. Shishir Kumar
Head, Dept. of Computer Science
Jaypee University, Guna, India

Abstract: ***Pervasive computing is a fast growing area of Information Technology and provides arena to make possible by the rapid growth of microprocessors with inbuilt communications facilities. Pervasive computing has a range of potential applications, from homecare to healthcare from environmental monitoring to intelligent transport systems. Pervasive computing is present everywhere at the same time. Indeed, with the miniaturization of computer hardware, processing units become invisible and integrate into vehicles, buildings, clothes, equipment, and so on. They can be at the same time mobile, integrated and often coupled to the physical environment. The applications are increased by a rapid growing of quantity and diversity of smart devices in the physical environment of users. For all these reasons, pervasive and ubiquitous computing look like a new computing area based on networks of devices and objects evolving in a real world, radically different from distributed computing, based on networks of computers and data storages.***

Keywords: GPS, PDA,

I. INTRODUCTION

Pervasive computing [2,3,8] is a family of technologies that aims to become part of our everyday life. Such technology will be available to us everywhere and for any purpose.

Figure 1.1: Pervasive Computing

Being "online" everywhere and anytime is what pervasive technologies are about.
Pervasive computing is omnipresent computers [2, 4] in the real environment through a large number of objects and new devices in our everyday life. Indeed, with the miniaturization of computer hardware, processing units become invisible and integrate into buildings, clothes, vehicles, and so on. They can be at the same time mobile, integrated and often coupled to the physical environment. They increase application fields of computing by a growing quantity and diversity of smart devices in the physical environment of users. For all these reasons, pervasive and ubiquitous computing appears like a new computing era based on networks of objects and devices evolving in a real world, radically different from distributed computing, based on networks of computers and data storages.

II. OVERVIEW OF SECURITY ASPECTS IN PERVASIVE COMPUTING

Security in the area of pervasive computing has a great concern. As far as pervasive computing is concern the privacy has a major role. Privacy is the ability to keep separate resources or information about themselves, and thereby express selectively. The borders and content of what is considered private differ among individuals, but share common themes. When something is private to someone, it usually means that something is inherently special or secret to him. The domain of privacy partially substitutes security, which can include the concepts of applications and protection of information. Privacy may also take the form of integrity.

© 2016, IJARCSSE All Rights Reserved

III. PRIVACY

Privacy is a very big concern for every individual and it should be protected at all time. Privacy can be defined as the right to be alone and to choose selective information to share with. Basically, this privilege is enjoyed by free people. An appropriate balance is needed between society and privacy. Therefore, a society cannot expect privacy for every single element because a society with total privacy would be not a society at all. Currently, there is a very high demand of providing privacy solutions to users whom communicates and exchanges personal information because people start realizing how important their privacy to them is. In a different angle, privacy can also be defined as a security aspect.

Privacy is quoted as the claim of each individual whom determines personal details and in what extend other can know about them. Every individual wants to preserve in their privacy level, therefore in the current situation based on the evaluation of technology; the real concern is not what type of information is collected but who had access to the individual personal sensitive information. Individuals who tend to know personal information about another individual is known as "privacy violation". Traditionally, privacy technologies has created tools for hiding and controlling disclosure of personal information but at the same time in term approaching privacy management it is important to realize and think how with the help of technology can create visibility and awareness for security aspect.

Alan Westin [13, 17] said privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information is communicated to others. The word privacy is defined as protecting a person's personal and sensitive information [17] from reviewed by others.

Few decades ago, society didn't have any exposure and realization on how important is their privacy to them. The younger generation people are starting to realize how important privacy is in their daily routine. This is because privacy can be violated if an individual tends to capture pictures or record conversations without permission of another party. Therefore, many negative elements may occur based on this situation.

Currently privacy is being a main issue in an individual's daily routine based on exposures of information details available for the society. People need to have the ability to protect selected information to be kept secretively rather than disclosing it out to public. The problem with individual's mentality in third world is that the level of realization of importance about the private information is less compare to the first world countries due to the education level background among society. Thus to that statement above, not all individual do not care about their privacy, just a certain amount of individual do not understand why privacy is important. This is a major advantage to a third party whom can use information gained for personal user.

IV. A USER-CENTERED CONTEXT-SENSITIVE PRIVACY MODEL

With evolution of pervasive computing, computers have become a part of in our life routines. Pervasive Computing is recognized as an age of calm technology where technology becomes as necessity and tends to be omnipresent in our daily life without realizing. Privacy is a major concern in an individual's daily routine and being a treat in a pervasive computing system. The proposed system to solve individual's privacy problems is called "User-Centric Context-Oriented Privacy Model". It is an implementation of the required privacy. This will ensure the user's privacy level before visiting an environment is determined by the user. Therefore, violation of privacy by third party can be reduced due to implementation of security element preserving user's privacy level. Hence to that, the implementation of Privacy Management System [9, 13] will ensure problem of privacy violation can be reduced without facing any distinguish problem.

There is plenty room of improvement to enhance the functionality of the current system. Implementation of Global Positioning System (GPS) [6] to integrate with proposed application. Since the current environment location base is all preset in the system, it will be more sophisticated by using available technology to able to detect the user's current location and based on the user's current location, the user can attempt to search the preferable place to visit. Besides that, the GPS capabilities can be maximized with the functions available by upon after locating the nearest location, the system must be able to direct the user to the preferable location.

Besides implementing GPS to integrate with the system, the location architecture image should display in PDA [7] before making a reservation is another enhancement for future. The current system, user is able to make reservation based on the availability of place by selecting the preferable place but the proposed implementation is to create a display of the environment in image form sent to the PDA and able user to select the preferable location to be. Example, user wants to make reservation and would like to view the image of the restaurant. The system will sent the image of the restaurant architecture and the user can set reservation based on the image where he/she would like to sit.

Another additional feature enhancement to make the system more attractive is by enhancing the design interface of the system with more graphical display style. Another concept that can be implemented is creating famous links integrates to create a convenience environment for the user integrating with the system. The ideology to create a concept of making the system to have more functionality by viewing new updates such as Weather news, Yellow Pages, Shopping, Sports, Money, Currency, Movies, Music, Flash Games, Horoscopes, Health and Fitness Guidelines, Food and Entertaining etc. The features mentioned shall make the system more effective and capable besides making a transaction to visit a place.

Since the response time between the pocket pc emulator and application is slow, the developer would like to implement multi-threading into the system to enhance the improvement of the response time which is due to the heavy processing running in the background. Therefore, this will make the functionality and usability of the system more effective.

Key management is fundamental requirement for security in communications. For security in pervasive computing sound key management is particularly difficult. However, good key management depends on good authentication. We reviewed current notions of entity authentication and confer over here that why we believe these notions are not suitable for the

© 2016, IJARCSSE All Rights Reserved

pervasive computing. We then present our views on how notions of authentication should be revised to address the challenges of the pervasive computing domain, and some of the new research problems. Some brief thoughts on how our revised notions may be implemented and some of the problems that may be faced.

Enabling security will be critical to realizing the exciting future of Ambient Intelligence. But good key management will be critical to securing transactions in the world of pervasive computing. In the wireless computing & security research community, key management is observed as one of the primary problems and an area of active research. But key management itself depends basically on sound authentication. Based on the past experiences of the security community particularly in the area of key management, it has been claimed that understanding and implementing authentication are among the most important challenges facing ubiquitous computing security.

Traditional authentication algorithms have concentrated on the notion of entity authentication, which provides assurance of who is the subject of a secure interaction. It has been argued that the requirements to implement entity authentication are unlikely to be practical in the pervasive domain. Further it is also discussed that the assurances delivered by entity authentication will be of limited value.

Instead of entity authentication assurances are required of which devices are the subject of interaction and what those devices will do. These assurances may be achieved by 'authenticating' a much broader class of device attributes than name. For the pervasive computing domain it is clear that location is an important attribute, but many more attributes are likely to be needed, including source, aspects of current condition, maintenance of integrity, and more. Making this shift is likely to introduce many new possibilities and create new security threats, the increased chances of man-in-the-middle attacks being an possible example. It is also clear that the requirements of which attributes to authenticate will vary from one context to other.

A further concern is the inflexible, binary nature of entity authentication. The much wider range of interaction will need more flexibility in security policies with higher gradations of assurance. Deciding upon the suitable security policy will be important, and devising metrics to facilitate such a decision will be an important research area. The subject of security for ad-hoc and wireless networks is quite new but the area is growing very fast, with key management being one of the major challenges.

However, much of the research in this area focuses on traditional approaches, based on certification or tokenization to solve specific problems within the domain. Both these concentrate on engineering solutions. Thus far we have seen little work that thinks specifically of how authentication needs to be deconstructed and revised. We hope it is clear that the concepts we have discussed strengthen the on-going solution-oriented research. More importantly, we hope that this work will help to foster debate on the new security aspect for the Ambient Intelligence World.

V. PRIVACY APPLICATION HEALTHCARE MONITORING APPLICATION

This study proposes an approach for privacy protection of patients based on active bundles [10]. An active bundle consists critical data, metadata, and a virtual machine. In healthcare monitoring systems, "critical data" are monitored health data. To avoid compromising of safety of patients who need critical help, this approach does not rely on the use of decryption keys provided to specific caregivers (which is a commonly used approach). Instead, it joins the use of privacy policies and safeguard mechanisms included within active bundles, such as evaporation and apoptosis. In our approach, ad hoc caregivers are able to access urgently needed patients' data. Their authorizations are provided via privacy policies encapsulated in metadata of an active bundle including health data.

Protecting patient privacy without compromising their safety is the main problem in pervasive healthcare monitoring systems (PHMSs). The two requirements conflict since the former requires limiting access to patient health data while the latter can be harmed by such limitations.

Current solutions resolving the conflict have two main drawbacks: (1) they require an extensive exchange of messages between a patient's caregivers in order to protect her data; and (2) they depend on using decryption keys that must be provided to specific caregivers.

We believe that especially the second limitation compromises the safety of patients who may need help while the caregivers pre-authorized to access their health data are not available.

We propose a solution that provides patient privacy and patient safety in PHMSs at the same time. This is achieved through the use of active bundles (ABs) that keep the following three components inseparable from each other: (i) sensitive health data; (ii) metadata including privacy policies, and (iii) a virtual machine (VM) that enforces privacy policies. VMs use four safeguard mechanisms behalf of its AB (apoptosis, integrity checks, enforcing privacy policies, and evaporation).

The lifecycle of AB consist of its creation, enabling, and use. Enabling involves three verification steps during which the four safeguard mechanisms are utilized.

The AB mechanism applied for PHMSs has a few salient features and benefits. First, a successful host infiltration is not sufficient for bypassing privacy policies defined for data. Even in such cases an AB prevents data privacy violations because enforcement of the privacy policy is as the data and the privacy policy is an inseparable part of AB.

Second, the AB scheme enforces privacy policies without relying on an application.

Third, our solution allows avoiding compromising safety of patients who need urgent help. It is possible due to the fact that our solution based on ABs does not depend on the use of decryption keys provided to specific caregivers. Instead, it combines the use of privacy policies and safeguard mechanisms included within active bundles, such as evaporation and apoptosis. In our approach, ad hoc caregivers are able to access urgently needed patients' data since their authorizations are provided via privacy policies encapsulated in metadata of an active bundle including health data.

© 2016, IJARCSSE All Rights Reserved

VI. CONCLUSION

In this paper, we have explored the privacy protection issues in pervasive computing and in healthcare monitoring systems in particular, based on an analysis of various researches carried out so far. Each and every issues have been discussed in detail and proposed suggestions to address each of them. The importance of health data is discussed and the privacy protection by pervasive computing is applied. We have chosen the subsequent research area that is the privacy policy management difficulties faced by end users of a pervasive healthcare monitoring system. To solve these issues, our paper proposes an architecture for a privacy-sensitive ubiquitous health monitoring system. The requirement is gathered from end users and application developers. The suggestions will provide a framework that can be used by application developers to develop a privacy-sensitive application for the end users.

REFERENCES

[1] J. Macker and S. Corson, "Mobile Ad hoc Networks (MANET)", *IETF WG Charter.,http://www.ietf.org/html.charters/manetCarter.html,*1997.

[2] IEEE Computer Society LAN MAN Standards Committee, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications", *IEEE Std.* 802.11, 1997, pp. 11-97.

[3] Buchecker, M. (2003). Public place as a resource of social interaction. In proceedings of the workshop on *Space, Spatiality and Technology*, Napier University, Edinburgh. p. 57-61.

[4] M.S. Corson, J.P. Maker, J.H. Ernicione "Internet based mobile ad hoc networking", *IEEE Internet Computing*, 3 (4), 1999, pp. 63-70.

[5] J.M. Jaffe and P.H. Moss, "An infrastructure design for ubiquitous computing ", *IEEE Transactions on Communications,* COM-30 (7): July 1982, pp. 1758-1762.

[6] C.E. Perkins and P. Bhagwat, "design approaches and models of spaces for mobile computers," *ACM SIGCOMM,* Vol.24, no.4, Oct.1994, pp. 234-244.

[7] C. Perkins, "pervasive computing," Chapter 8, Addison-Wesley, December

[8] 2000. Bellotti, V. and Edwards, K. (2001). "Intelligibility and Accountability: Human Considerations in Context-Aware Systems." *Human Computer Interaction* 16: 193-212.

[9] I. Chlamtac and A. Lerner, "Fair algorithms for maximal link activiation in multi-hop radio networks", *IEEE Transactions on Communications COM-3, Issue-7,*
Vol. 35, 1987, pp. 739-746.

[10] C. Siva Ram Murthy and B.S. Manoj, "Privacy issues in pervasive computing" Prentice Hall, 2004.

© 2016, IJARCSSE All Rights Reserved