Journal of Advances in Computer Research
Quarterly pISSN: 2345-606x eISSN: 2345-6078
Sari Branch, Islamic Azad University, Sari, I.R.Iran
(Vol. 6, No. 2, May 2015), Pages: 1-10
www.jacr.iausari.ac.ir

A Comparative Study on Quality of Privacy in Pervasive Computing in Health-care Systems

Soroor Mohammadi Bezanaj✉[1],Hamed VahdatNejad[2]

1) Islamic Azad University of Science and Research Brach, Birjand, Iran
2) Department of Computer, University of Birjand, Birjand ,Iran

Soroor.mohammadi67@gmail.com; hamed.vn@gmail.com

Received: 2014/05/19; Accepted: 2014/07/05

Abstract

It's not long since the advent of pervasive computing by Mark Weiser and one of its main usages is in healthcare systems. As this technology has been introduced only recently in this field and because we are dealing with peoples' lives and their data, providing a high level of privacy and security is of great importance. Various studies have been performed in which a certain method has been used to reach the mentioned goals. In this paper we have two major goals, introducing this technology and its benefits in healthcare domains and studying and comparing the five most related articles done in this domain by some criteria. By comparing these works we can achieve a useful result in the current methods in order to provide privacy and establish security.

Keywords: *Pervasive Computing, Privacy, Security, Healthcare System*

1. Introduction

A health care system is an organization of computers, facilities, trained people and institutions that give patients health services. In the recent decades pervasive computing has been used in health care systems to reduce costs and improve the services given to patients. These systems make it easier for nurses and doctors to work. One of the reasons for using pervasive computing in the health care area is that doctors and nurses usually do not sit in a special place and most of the time they are in an emergency situation so they need to use technologies in an easy and fast way.

Privacy is defined as:"a complex social process that persists in one form or another as a fundamental feature of the substrate into which ubiquitous computing is threaded" [8] .If applications become more aware of the context of the user they can adjust themselves more easily in order to help him. On the other hand, as applications become more familiar with the user they are more of a risk to his privacy. So, we can say that using ubiquitous computing has its own deficiencies; the most important can be privacy invasion [8]. For most people having a fully controlled access is a serious concern in protecting their privacy [8]. Personal Health Records usually contains extremely private information that are needed to be secured perfectly with well-managed controlled access only. The federal government of the United States empowered HIPAA (Health Insurance Portability and Accountability Act) to put a standard for managing the security, privacy and data exchange of personal medical information. HIPAA specifies the needs for quality in healthcare in patient care.

Benefits of using pervasive computing in health care systems have attracted the attention of many researchers in the last few years. Thus, much research in this subject has been done in these years. As has been mentioned before in many of these studies, authors have named privacy as one of the most important challenges in ubiquitous health care systems. Therefore, the goal is to show the importance of how to protect the privacy in pervasive health care systems and look through some of the papers in this area and provide a survey on approaches that they have proposed in solving this problem .

In part II of this paper we have described a series of definitions that are needed for a better understanding of the issue. Section III is dealing with the expressed issues and requirements and in part IV there are some related works. In part V the study of selected articles by chosen criteria is discussed and finally in part VI the conclusion of the paper is accessible.

2. Definitions

In order to better understand, it is best to start by defining some basic concepts in this filed.

2.1 What is Context?

In a well-known definition context is defined as: "Any information that can characterize the situation of entities (i.e. whether a person, place or object) that are considered relevant to the interaction between a user and the application" [1]. Context is typically the location identity and state of people, groups and computational and physical objects.

2.2 Context Awareness

Context-awareness is defined like this: "A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task." [2].

2.3 Data or Information Privacy

Information privacy, or data privacy is defined as: "The relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them .Privacy concerns exist wherever personally identifiable information is collected and stored – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as: healthcare records and biological traits, such as genetic material. The challenge in data privacy is to share data while protecting personally identifiable information. The fields of and information security design and utilize software, hardware and human resources to address this issue [9]".

2.4 Privacy in Healthcare systems

Most people believe their health information is very important, needing the strongest legitimate protection. Old laws in many states and the old tradition of doctor-patient privilege have been the most critical aspects of privacy protection for years. The federal Health Insurance Portability and Accountability Act (HIPAA) was established in 2003 and it set a nationwide guide for the privacy of health information. Still HIPAA only applies to medical records kept by health care providers, health plans, and health

clearinghouses and only if the facility performs certain actions electronically. A great amount of health related information exists outside of the health care facilities and the files of health plans, which are beyond the reach of HIPAA [10].

3. Privacy in Pervasive Healthcare: Requirements and Issues

In order to better understand the problem of protecting privacy in pervasive health care systems in this section we present a scenario of a pervasive hospital.

"In a hospital all doctors, nurses and interns have hand-held devices such as PDAs or smart phones. They are also equipped with location detectors. Doctor Smith is responsible for checking the interns and to see whether they are in the correct rooms and are doing their jobs correctly or not. This can be done easily because all the interns note the things that they are doing on their PDAs and there are some webcams in rooms so their activity can be seen by the person in charge. While visiting the patient, Smith encounters a question and needs some help so through his PDA he calls for another doctor .He can also ask his questions through video chat or by sending a text message.

Linda who is a nurse can see her work time table on her PDAwhich is also visible for Angela who is the head nurse. Through this, Angela can check Linda's tasks. These tasks will be automatically deleted from her work time table after she has ticked them. In case of a delay Linda and Angela will receive a warning. She has a delay in one of her works so after being informed, Angela would find her location from a map shown on her PDA and then she would see her by the camera that is installed in that room. She understands that Linda is chatting with one of the nurses so she sends a message to her in order to ask her to continue doing her tasks. In all patients' rooms there are finger-touch displays. The patient can observe his treatment's procedure, chat with his doctor or nurse or use some common services like calendar and television. If there are any drugs prescribed the cost will be calculated immediately and the price can be shown in the patient's display. As a doctor or a nurse come close to the patients the display in the room visualizes the patient's record after identifying the doctor or nurse. If there are any lab results or x-rays they will also be presented to the doctor."

According to the above scenario the following issues and requirements should be addressed:

- Quality of privacy: It is very important that their location at their rest time should not be shown to other people including, Smith. For example if someone is in the dining room, his activities mustn't be shown to other people. The patient's record, lab results and financial affairs mustn't be shown to unrelated people .
- Security: Financial information should be stored and transferred in a safe way. Only the staff from the financial sector can have access to them. The patient's record must only be seen by the related doctor or nurse. So the system's security should be in a way that prevents unauthorized people from accessing these data.

4. Related Works

In [11] JakobBardram presented an initial outline of the design of a Personal Medical Unit (PMU) for storing and synchronizing personal medical data with other clinical computer systems. The paper primarily discusses the motivation for such a pervasive healthcare device focusing on the potential in having the patient as the data integrator. The paper also outlines the preliminary design of the PMU Architecture.

In [12] the research aims to enable a patient-centric, instead of the existing hospital-centric, pervasive healthcare environment. They proposed the MiCARE services as an essential framework to support a dynamic, mobile, and context-aware environment. While taking care of the patient, it should both ensure and enforce the context-aware authorization of different data objects in dynamically changing context. By integrating the technology of context-awareness, rule inference, digital rights language, and P2P infrastructure they practiced context-aware authorization in dynamic healthcare services. The workflow engine eXFlow2.0 with Web services support is another product they have developed. The engine is mature enough to be deployed for B2Bi of back-end heterogeneous systems.

The paper entitled 'Identifying and Utilizing Secure Paths in Ad Hoc Assistive Medical Environments'[13],[14] describes a system that allows dissemination of medical information over ad hoc networks. The limitations and requirements for a system that manages medical information over unstable topologies are described. A solution based on advanced management techniques, which enables secure and privacy enhanced transmission of medical data, is analyzed. Also, a number of measurements in the context of a large number of participating mobile users are presented in the paper. Other works have been performed and we have chosen the five best for comparing and studying which we will discuss in the next part.

5. The Study of Selected Projects by Chosen Criteria

In this section we will study thoroughly the selected papers. For this purpose we have chosen certain criterion. This survey is trying to determine the papers that have included security and if so the techniques used. The second aspect we will put into account is to find out what approaches have been used for protecting privacy. It has to be indicated whether the papers' focus is on the patients records, and if not can we use their techniques in health care systems. Another thing that we will survey is to see if the user has any role in protecting his privacy or not. In the end we will determine which of them has proposed any practical application.

In [3] for a better understanding of privacy the authors started their survey in a hospital and their focus was on the patients' records. They started studying the tasks of different people in the hospital such as doctors, interns and nurses. They prepared four scenarios and presented them to some of these people in order to understand their reaction in different situations.

In these scenarios the pervasive services such as displaying information in a personal device , tracking the location of people, exchanging information between different tools, receiving sound and picture from their activities and identifying individuals and etcetera has been taken. During interviews with various people they found that location, identity, time, activity, and accessibility are the issues that need their privacy to be preserved when using a context-aware service. They use these findings to help designers, provide a level of confidence in their applications and to design Privacy-aware applications. The

authors addressed this issue in their article indicating the presence of a trade-off between the amounts of privacy a user expects and value of pervasive services provided by an Application, so for presenting this issue they introduced the concept of QoP (Quality of Privacy) , according to this concept a user can request a level of QoP meaning that the context aware application should behave in a way that the user becomes satisfied and also the level of pervasive service does not decline. Ontology allows the balancing of tradeoff by using ECA model. Ontology has three components: 1 – An event that describes the need for performing an action which is characterized by location, identity, time, activity and artifact. 2 - A condition that specifies the rules defining the action that should be performed. 3 - An action which involves a series of functions that may be applied to the privacy laws becoming strict or weak.

In the architecture they use, privacy is set in both sides of the user and the environment. In this architecture, a broker undertakes the communication between the services that are based on a protocol that use the mentioned ontology for management of QoP. There is a context-aware filter in the user's side that allows him to set the level of privacy in the rate that he wants. So the level of QoP between the user and the broker becomes negotiated. There is also a filter at the server's side that does the same work. Server filter is an agent that monitors transportation of information between the broker and other agents and its work is like client filter with the difference of negotiating at the side of server and deciding the requests that should be rejected.

They used SALSA and developed it according to the mentioned ontology so they could provide a proper language for transporting information between agents themselves, agents and users or between agents and services. They proposed an application in which information can transport easily between different devices and has a menu which we can choose different programs and services from it. They keep high security and reliability by using a method in which the sender can encrypt or sign a message or present information that is sent to a user or he can do the same task for each arbitrary message. Therefore in this paper they presented an application in which security and privacy are respected and the user has a role in protecting his privacy.

In paper [4], the authors pointed to the sensitive nature of medical information in healthcare systems and mentioned that this information should be gathered from different places without damaging the privacy. They also indicated that their method needs an architecture which is based on some rules and decides whether it should respond to a query or not. System represented by them has three characters: 1-data privacy: meaning that the query requester knows no information about the data used for calculating the answer and can only learn from it so he does not know more than he needs.2- query privacy: It means that the data owner does not know anything about the query and just knows that a query is running.3-anonymous communication: someone who asks the query and who is the data owner do not know each other. In the system that they proposed a query is divided into different sections but it works as if it is centralized. Intermediate results go to a third party for delivery and reaching a final result. This third party is called blind computer and is used for keeping the systems security high. The system runs some fake queries so that the third party wouldn't understand which of the information it has is real. In this system the query asker should pay a price to know the answer so if he wants to know more he should pay more. Tokens are the money used in this system, are supplied by the system to organizations that are authorized to perform queries.

The tokens are assigned to organizations according to their need for running queries. This way, they would only know as much as they need and not more, so if an organization pays more it can know more and therefore the level of privacy is declined. There are two phases for answering to a query, global search and query execution. Each patient has an identifier. The third party hides the ID of the data owner and responder so nobody would be aware of the other's IDs. In global search, IDs are given to a series of data handlers which point to a record and therefore this provides a way for sending a message in an unknown way. They have used a security system in their project which puts labels for each data in order to protect the patients' records. This way, the asked question itself does not disclose any important information and privacy is saved. Another mechanism used is that each data has an owner and some readers and only its owner can change the information or its label. In this paper the patient has no role in determining the level of privacy.

The paper [7] discusses the security and privacy of remote pervasive systems and after introducing the benefits of this technology it points out the challenges in this domain that are security and privacy. Since information collection and transferring is from the patient's body and environment, it is very important that transferring and collecting are done in a secure way and the privacy of patient is protected. In order to survey the challenges of security they divide the environment to several phases so they can have a more careful survey. They divide the environment to four domains: A, B, C and D. Part A is related to collecting information from the patient's body sensors. Part B is related to the method of transferring the collected data to other parts so some challenges like security and privacy advent in this part. Part C is related to the mechanism of saving and analyzing the data so the same challenges are presented here too. Finally part D is related to the access of doctors to data so this task should be done safely and in a secure way and privacy should be protected. Different types of attacks are mentioned in this paper. The first type is external passive attack in which the attacker can only access and read the data and cannot change or manipulate them. The second type of attack is external active attack in which the attacker in addition to accessing the data can also use or change them. The third and fourth types of attacks are internal passive or active attack in which the attacker itself is part of the system and can easily read or change and manipulate data. In this article they have considered both types of internal and external attackers so it can read or change data. This assumption has four security requirements. At first the connection between the sensors and the local server should be secure, and the transferred data must not compromise the privacy meaning that personal data and data related to individuals should not be transferred. The third requirement is that the transferring of data should be done securely. Finally the system should be designed in a way that accessing data from different points would be possible as we don't have a single point of failure. The authors state that if the transferred data does not reveal any information about its owner and the owner cannot be tracked, it does not threaten the privacy. The goal of their method is to access the electronic records of patient in a network securely. The connection between doctors' phones and sensors is done securely through the Internet. This task is done by establishing a secure session between doctors' phone and the healthcare providers' server. This server is a place where the data is stored. The mentioned session uses handshaking TLS system which encrypts the transferred data. Some conditions should be established to transfer any important information: authentication of doctor, connecting device, environment and the receiver person of healthcare. After the establishment of these conditions, information

transferring can be done. In order to have a secure connection and to protect the privacy in this approach, negotiation is used too. We should mention that in this article the user has no role in setting the level of privacy.

The focus of paper [5] is on the patients' records. At the beginning of the article the authors mention the need for using sensors for controlling many diseases. If we use them in a mobile and pervasive way, the flexibility of the patient does not become limited. As these sensors need to be used in a network we are confronted with some challenges like security and privacy. The application that is proposed uses a three layered network: 1) Sensor layer in which two types of sensors are located. One type is used for collecting vital signs from patients' bodies and the other type is used for collecting the parameters of the environment. The sensors that receive the vital signs are on a fabric belt. Bluetooth is used for transferring the data that is gathered from patients' bodies and the technology of wireless Zigbee is used for the conduction of the data gathered from the environment. For transferring the data to upper layers Bluetooth security authentication and encryption are used. The security between sensors is established with a polynomial-based encryption. The second layer is mobile computing network layer in which some computing devices like laptops and PDAs, and an ad hoc network for routing, and an infrastructure-base network for connecting to a local station are used. The computing devices use SMS in order to report, which its security is protected with public key cryptosystem; also there is a part for authenticating the mobile computing devices. Next a secret key and a public/private key pair are provided. 3) Backend layer: this layer is located on the Internet and includes some fixed stations and servers for providing services to lower layers and this layer process the data gathered by mobile computing devices. The authors proposed three types of applications: in home, in nursing home and in hospital application. As mentioned before the connection between a sensor and a mobile computing device is established by Bluetooth so for securing this connection authentication, encryption and key management are used. The part that handles the security uses hardware-accelerated cryptography. In this article the authors tried to keep the connection between mobile computing devices secure and the third layer provide public key mechanism. A third party is also used in order to provide authentication. Finally after analyzing the performance and the security of the proposed applications they concluded that the presented approach was efficient and security and privacy were provided.

The focus of paper [6] is not on medical records but the authors mentioned in all parts that one of the uses of their definitions is in medical domain. At first the authors mentioned that the contexts that are related to humans are important. The information of context is indicated with a series of indexes named Quality of Context (QoC). One of the reasons of the importance of QoC is protecting the privacy of users. As services must not receive their needed information with a quality higher than their needs, the user should set the level of quality of the information related to him. They introduced five indexes: precision, freshness, spatial resolution, temporal resolution and probability of correctness. They defined precision "granularity with which context information describes a real world situation". For example, the air temperature of a patient's room can be presented with different models. Sometimes there is no need to share information with high level of precision because some important information may be disclosed and the privacy's level lowers. They defined freshness "the time that elapses between the determination of context information and its delivery to a requester". For example a doctor may ask to know the rate of a patient's breath in a specific period of time.

Freshness is effective in the level of privacy too meaning that maybe a user wouldn't like the data related to him to be shared in a high level of freshness because it may disclose some important information about him. Some data because of their freshness will present some private information to services. They define spatial resolution "the precision with which the physical area, to which an instance of context information is applicable, is expressed". A user may want the rate of spatial resolution of the data related to him to be low because of some security and privacy reasons. They defined temporal resolution "the period of time to which a single instance of context information is applicable" which is like spatial resolution and the user can set it in order to prevent some important data to be disclosed. For example it is possible to express the date of a doctor's entrance to a hospital in two models, in the first model it is possible to express it just by telling the date and the second model is more complete where it's possible to express it by telling the date, minute and the second of entrance. By using the second model some important information may become transpired. They define probability of correctness "the probability that an instance of context accurately represents the corresponding real world situation, as assessed by the context source, at the time it was determined". Sometimes it necessary for a user not to allow the system or the context requester to be sure of the accuracy of the data they receive for security reasons. Therefore when sharing data this fact is put into account and the information sent is in a way that there is no certainty of it to be hundred percent true.

Table [1] briefly illustrates the comparisons done:

Table1: The comparison of papers

Papers' name	Is the security mentioned in the paper?	Name of the approaches which provided the security	Is the privacy mentioned in the paper?	Name of the approaches which provided the privacy	Is the focus of the paper on the patients' records?	Dose the user have any role in setting the level of his privacy?	Do the authors present any application?
Quality of Privacy (QoP) for the design of ubiquitous healthcare applications	☑	Encryption, Signing the messages	☑	Introducing the concept of QoP, negotiation between different parts	☑	☒	☑
Privacy enforcement for distributed healthcare queries	☑	Labeling the data	☑	Data privacy, query privacy, anonymous communication	☑	☒	☑
Ubiquitous Health Monitoring Systems: Addressing Security Concerns	☑	Authentication, establishing a secure session, handshaking TLS system	☑	Dividing the environment to 4 parts and establishing the privacy in each part	☑	☒	☑
Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks	☑	Authentication public key, cryptosystem	☑	Has not be stated	☑	☒	☑
Quality-of-context and its use for protecting privacy in context aware systems	☒	☒	☑	Defining 5 indicators namedQoC	☒	☑	☒

6. Conclusion

As this technology has been introduced recently in pervasive healthcare systems some challenges like providing privacy and establishing security appear in this field. Various studies have been performed. After studying many of them, we have selected the five most related articles and compared the methods used in them. In future we can survey more articles and by comparing them, we can choose the best approach in later projects.

7. References

[1] Bricon-Souf, Nathalie, and Conrad R. Newman. "Context awareness in health care: A review." *international journal of medical informatics* 76.1 (2007): 2-12.

[2] Abowd, Gregory, et al. "Towards a better understanding of context and context-awareness." *Handheld and Ubiquitous Computing*. Springer Berlin/Heidelberg, 1999.

[3] Tentori, Mónica, Jesús Favela, and Victor M. González. "Quality of Privacy (QoP) for the design of ubiquitous healthcare applications." *Journal of Universal Computer Science* 12.3 (2006): 252-269.

[4] Siegenthaler, Michael, and Ken Birman. "Privacy enforcement for distributed healthcare queries." *Pervasive Computing Technologies for Healthcare, 2009. PervasiveHealth 2009. 3rd International Conference on*. IEEE, 2009.

[5] Huang, Yueh-Min, et al. "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks." *Selected Areas in Communications, IEEE Journal on* 27.4 (2009): 400-411.

[6] Sheikh, Kamran, Maarten Wegdam, and Marten van Sinderen. "Quality-of-context and its use for protecting privacy in context aware systems." *Journal of Software* 3.3 (2008): 83-93.

[7] Elkhodr, Mahmoud, Seyed Shahrestani, and Hon Cheung. "Ubiquitous Health Monitoring Systems: Addressing Security Concerns." *Journal of Computer Science* 7.10 (2011): 1465.

[8] Tsai, Tse-Ming, Jiann-Tsuen Liu, and Y. J. Hsu. "MiCARE: context-aware authorization for integrated healthcare service." *Proceedings of the 3rd international workshop on ubiquitous computing for pervasive healthcare applications, Nottingham, England*.2004.

[9] http://en.wikipedia.org/wiki/Data_privacy

[10] https://www.privacyrights.org/fs/fs8-med.htm

[11] Bardram, Jakob E. "The personal medical unit--a ubiquitous computing infrastructure for personal pervasive healthcare." *Proc. 3rd. Ubiquitous Computing for Pervasive Healthcare Applications, Nottingham, UK* (2004).

[12] Tsai, Tse-Ming, Jiann-Tsuen Liu, and J. Y. J. Hsu. "MiCARE: context-aware authorization for integrated healthcare service." *Proceedings of the 3rd international workshop on ubiquitous computing for pervasive healthcare applications, Nottingham, England*. 2004.

[13] Belsis, Petros, Dimitris Vassis, and Christos Skourlas. "Identifying and utilizing secure paths in ad hoc assistive medical environments." *Security and Communication Networks* 4.11 (2011): 1231-1242.

[14] Grammati Pantziou, Fillia Makedon, Petros Belsis "Special Issue on Privacy and Security on Pervasivee-Health and Assistive Environments." Published online 20 April 2011 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.318