Security and Quality Privacy in a Remote Medical System for Internet of Things

K. Sakthi
M. Phil Scholar
Department of Computer Science & Engineering
Bharathidasan University, Tiruchirappalli, Tamil Nadu, India.

Abstract— With the continuous evolution of Internet of Things (IoT) different kind of aspects of life will improvement. IoT based healthcare system has probable to provide error free medical data and alerting system in serious conditions with continuous observation. The system will reduce the need of faithful medical personnel for patient observation and help the patients to lead a usual life besides providing them with high quality medical service. Privacy problems commonly discussed between researchers in healthcare. Healthcare systems are applications that can support patient's essential anytime and anywhere. However, healthcare increases privacy concerns since it can lead to situations where patients may not be alert that their private information is being common and becomes vulnerable users. The different problems recognized are medical information misuse, prescription leakage, medical data's eavesdropping, social consequences for the patient, patient difficulties in handling privacy settings, and lack of support in scheming privacy-sensitive applications. We slight down the problems and choose to focus on the problem of 'huge number of support in manipulative privacy aware applications' by proposing privacy - aware architecture specifically designed for pervasive healthcare observation systems.

Key words: IoT, Human Factors, Quality Healthcare, Privacy Problems

I. INTRODUCTION

Internet of Things (IoT) is allowing and revolutionizing the way in which physical objects are connecting with each other. IoT can be utilized in a number of application domains such as: smart homes and cities, food safety and security and healthcare. The possibilities that IoT delivers will modernize novel applications and devices whose communication capability will create new markets and a new economy Ubiquitous computing developments are growing rapidly as wireless technology becomes more reliable and capable to sustain various types of applications. From ubiquitous computing is born another field, omnipresent healthcare that combines ubiquitous computing and healthcare to develop applications that can assist patients in their daily life routines [1]. Varshney [2] defines Healthcare as "healthcare to anyone, anytime and anywhere by eliminating location, time and other restraints while cumulative both the coverage and the quality of healthcare". This means, for instance, that a patient with heart problems can stay in the comfort of their own home while being checked by healthcare services, instead of staying at the hospital.

On the other hand, there are numerous problems and challenges in recognizing healthcare in daily life. These include the privacy characteristic that has been known based on the literature reviews conducted in this study. Most of the papers designated that there is a need to address privacy in a healthcare system. Examples of Healthcare applications include pervasive healthcare observation systems, intelligent emergency systems, pervasive healthcare data access and worldwide mobile tele-medicine. However, this paper can specialize in exclusively pervasive healthcare observation systems since they create additional potential problems regarding patient privacy than other applications.

Confidentiality law normally defines an individual's privacy as personal information about a separate that can represent that individual as a complete that consequently describes a private. To shield their privacy, patients have the right to offer permission on that knowledge ought to be collected, used or connected. Without approval from the individual, his or her information ought to stay private; if any unauthorized person takes it, it is illegal action. Observation systems were preferred for this investigation; as a result they deal more with data communication, such as audio, video, or medical data (blood pressure, heartbeat and electrocardiography (ECG/EKG). "ECG is the process of recording the electrical activity of the heart and is used in the investigation of heart disease" [3,4]. An observation system could be a system which will monitor patient daily while not interrupting on patient's daily routine. It might involve multiple parameters simultaneously; as an example; the parameter can be reading the patient's electrocardiogram every few minutes or taking their vital sign and causation it to their healthcare providers. An observation system might also involve, as an example, transmitting live video and audio of a patient to observe their activity to know her current condition. As it is pervasive, it implies that most of the system parts are wireless, thus vulnerable to potential threats like eavesdropping and data theft; this raises privacy problems. The next section discusses in detail the privacy problems in pervasive healthcare observation systems based on analysis of the research papers.

II. THE MOTIVATIONS

Increasing range of analysis and development comes in pervasive healthcare, many privacy problems and challenges arise; for that reason, we would like to understand the current problems and challenges. Patients have the right to choose whether or not to reveal their information and more individuals are becoming aware of privacy problems. Stronger security of a system would promise higher privacy protection for the patients.

We selected analysis papers that relate to universal computing, pervasive healthcare in overall and pervasive healthcare observation systems. The principles for selected credentials are that they confer security and privacy problems within the whole paper or at least in the introduction thus discussing the reasons overdue the development of the system, architecture or model.

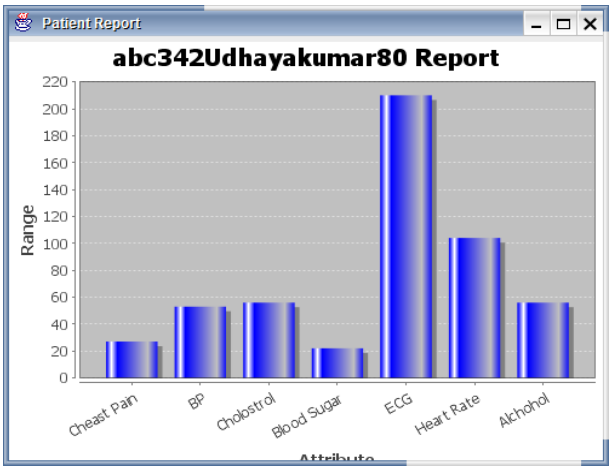

Fig. 1: Patient Report Analysis

Figure 1 depicts the outline of the accumulated papers for the related topics.

A. Healthcare Observation System

A healthcare observation system will monitor numerous varieties of information and measurements having a bet on the patient's health issues. A healthcare observation treatment system is a system that monitors the patient's treatment and evaluates their clinical state. This kind of observation is vital to ensure a patient's treatment is accurately recorded hence making it easier for healthcare professionals to offer follow up treatment. If the patient has a problem in future, all the stored data can be easily accessed to hurry up the treatment decision. However, from the privacy perception, storage of a patient's healthcare data is vulnerable to data leakage or theft by information hackers and may lead to abuse of the patient's data.

The system monitors two types of vital signs, oxygen diffusion and heart rate, via electrocardiography (ECG) of a psychiatric patient exhausting two types of devices. The signal is sent from the gadget to healthcare providers via Bluetooth connection. If any strange vital signs are detected, aid is immediately sent. The wireless connection could open additional privacy problems as it has the potential security defect of permitting unauthorized persons to steal the data hence forward patient's privacy data. To shield the patient's privacy, the system should have powerful privacy data management controls to minimize the privacy risk.

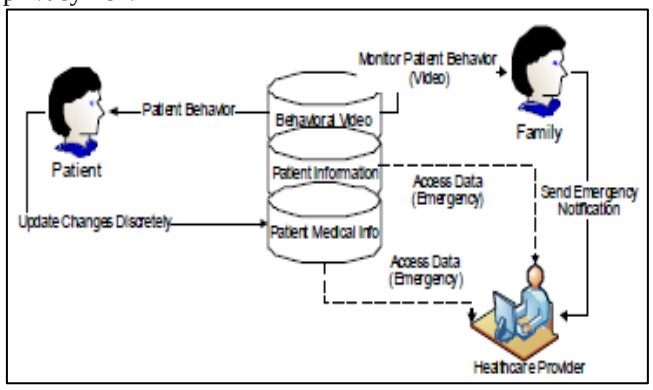

Fig. 2: Healthcare Observation System Overview

Fig.2 Depicts the general overview of a healthcare observation system used in this research. There are three main stakeholders that have privacy concerns in a healthcare observation system: the patient, the family and the healthcare providers. To illustrate how a healthcare observation system works, consider the following scenario. The patient is an elderly woman and the mother of a working daughter. The mother wants to live alone in the house; the daughter would like to be able to monitor the mother from her office. The observation system provides cameras in the house at a few possibly dangerous locations such as the kitchen and the living hall to monitor the patient's movement. The daughter can watch the video. The system is also connected to the mother's healthcare providers but they are not allowed to watch the video except in case of emergency. In order to protect the patient's data privacy, the healthcare provider also does not have any access to the patient's information unless there is an emergency. If there is an emergency with the patient, the daughter can send an emergency notification to the healthcare provider. Only then can the healthcare provider can retrieve all related patient information (such as name, address, medical history, prescription information, etc.) to send an ambulance and to provide adequate treatment [5-8]. This type of restriction on observation of data can ensure the patient's privacy is protected and can decrease the possibility of data leakage.

III. PRIVACY PROBLEMS

Privacy problems obtained from multidisciplinary fields such as computer science, bioinformatics, the social sciences and medical science. These days some pervasive healthcare applications are in development while patients have put other applications into use, therefore users and researchers are also starting to raise privacy problems. For example, before dementia patients agree to use the application, they and their relatives often ask about the privacy policies. This is because they want to ensure that their use either health is taken care of by the healthcare service providers while the privacy of their life is insured.

Based on the collected and analyzed privacy problems, we have summarized and grouped similar and related problems into six major privacy problems. The six problems identified are medical data misuse, prescription leakage, medical data eavesdropping, social involvement for the patient, patient difficulties in administration privacy settings, and lack of support in designing privacy-sensitive applications. By doing this grouping, it would be easier for future research to know current problems in pervasive healthcare and embark upon the interested privacy problem.

A. Misuse of Patient Medical Information by Unauthorized Individual

In a pervasive healthcare observation system, patients are more exposed to privacy risks. A comprehensive observation system can be applied at the hospital, home or nursing home. The system can transmit signals from the patient to the healthcare provider when unusual signs are detected to get immediate help. When there is pervasive healthcare, the technology usually involves wireless communication; therefore it is open to all of the wireless threats such as eavesdropping and information theft. Thus one privacy problem would be the possible misuse of patient medical information by unauthorized person who can intercept and control the information [12]. Without proper authentication and encryption unauthorized person can take

patient data without any difficulty. Every pervasive system should incorporate basic encryption to protect the patient's information.

B. Eavesdropping of Patient's Medical Information

A third potentially dangerous problem when applying observation technology is eavesdropping. Observation means that the system will record some patient data (such as blood pressure) to be transmitted to the healthcare providers. With these observation systems, it is easy for unscrupulous developers to make a system that can easily spy on the patient's data during the data transaction through wireless technology [6]. Therefore developers need to consider applying controlling authority whenever they develop a system. This can at least protect the patient's information from eavesdroppers or reduce the number of people that can easily take the information.

C. Lack of Support in Designing Privacy Sensitive Applications

Most of the above listed security and privacy problems are based on the user's perspective. From the developer's perspective, the problems would be a little bit different. Developers have little support in designing applications that are supportive in serving users manage their privacy policies in applications [19]. Developers are keen to build up a pervasive healthcare observation system that applies the latest wireless technology and that can progress on preceding applications. However, the privacy part of a system is somehow overlooked. Although developers have considered some privacy aspects, they only cover a narrow aspect of privacy; therefore developers tend to develop systems that fail to fulfill this user requirement. Because of this, users feel that the system is intrusive and end up refusing to use the system. As a result, Hong [19] has come out with Confab, a toolkit for facilitating the development of privacy sensitive applications. However, Confab is a toolkit for general application. We would like to develop a toolkit specifically targeted to pervasive healthcare observation applications that can assist developers in designing such applications. The resulting system could work enhanced in assisting patients in managing their confidentiality policies and therefore provide a better healthcare application in future.

We have collected security and privacy problems in ubiquitous computing in general and in pervasive healthcare observation systems in particular that are focused on the human factors from the analysis of selected research papers [9-15, 18-19]. Based on these problems, in the remainder of this paper we address privacy framework and propose a methodology for producing a privacy architecture that can be used by system developers to include a enhanced design for privacy settings in their system requirements. Thus users, healthcare providers and developers can all benefit from the architecture. The next section will discuss the proposed work and the methodology in order to achieve the goal.

IV. PROPOSED WORK

The contribution of this research would be creating privacy sensitive architecture that can help behavioral psychiatric observation system ensuring patient's privacy. This research is going to be interesting, as psychiatric patients would have different privacy perspective and different concerns compared to other patients. Different type of psychiatric problems would define different level of disclosure. Furthermore their family has authority to define patient's privacy on behalf of them. Therefore we are going to analyze their privacy preferences based on their needs to help them protecting their privacy. Figure 3 depicts the proposed framework for a privacy sensitive behavioral observation system. There are four stakeholders in this system: patient, family, application developer and healthcare provider. Patient and family will be informed of their privacy policy first as a guideline, before they define their privacy management [20, 22-23].

Patient and family defined as end users in the system as they have authority to define their privacy preferences through the user interface. Their privacy setting will go through End- Users Privacy Management Module. The privacy preferences will be combined with privacy management in the system, which contains privacy policies that are collected during the initial phase of this research. The combination of these two privacy managements will define the multiple data storage in this system. in other words, users automatically have control on their privacy such as who can view their video and how long the data could be saved on the database. The application developer's role is to develop an observation system that has a privacy architecture that will guarantee the system will work well with patient's privacy preferences. The healthcare provider has access to vital signs data and certain additional data as permitted by patients and family.

A. Data Encryption Standard 2

The Data Encryption Standard 2 is a symmetric-key algorithm for the encryption of electronic data. DES2 is the standard block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complex operations into a different cipher text bit string of the same length. In the case of DES2, the block size is 64 bits. DES2 moreover uses a key to adapt the transformation, so that decryption can evidently only be performed by those who know the exacting key used to encrypt. The key apparently consists of 64 bits; however, only 56 of these are really used by the algorithm. Eight bits are used exclusively for checking parity, and are thereafter discarded. Hence the successful key length is 56 bits.

The key is technically stored or transmitted as 8 bytes, each with odd parity. According in the direction of ANSI X3.92-1981 (Now, known as ANSI INCITS 92-1981). One bit in each 8-bit byte of the key may be used for error detection in key generation, distribution, and storage. Bits 8, 16... 64 are for use in ensuring that every byte is of odd parity.

B. DES2 Analysis

The DES2 satisfies both the desired properties of block cipher. These two properties make cipher extremely strong.

- Avalanche effect − A little modify in plaintext results in the very grate change in the cipher text.
- Completeness − each bit of cipher text depends on many bits of plaintext.

C. Key Encryption

The aim of Key Encryption (KE) is to make sure that the communication being sent is kept confidential during transit. To send a message using KE, the sender of the message uses the public key of the receiver to encrypt the contents of the message. The encrypted message is then conveyed electronically to the receiver and the receiver can then utilize their own matching private key to decrypt the message.

The encryption process of using the receivers' key is useful for preserving the privacy of the message as only the receiver has the matching private key to decrypt the message. As a result, the sender of the message cannot decrypt the message once it has been encrypted using the receivers public key. However, KE does not address the difficulty of non- denial, as the message could have been sent by anyone that has access to the receivers key. Key encryption is the major part in this work. Through which admin also cannot able to view the original details but he can see encrypted messages.

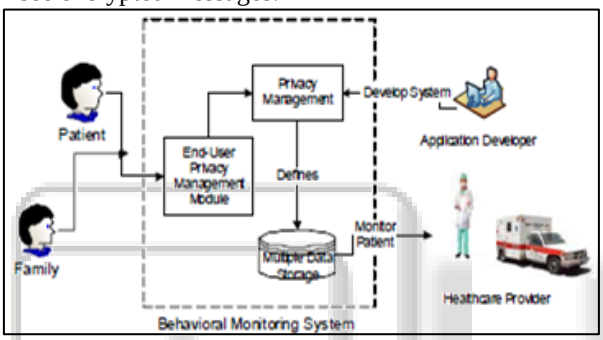

Fig. 3: Proposed Framework for Privacy-Sensitive Observation System

V. Result and Discussion

To achieve the goal of this work, we are going to gather privacy policy requirements by doing document analysis. The document analysis would specify type of hospital polices, obtain related documents on privacy, interview few experts and as for the outcome is the comprehensive privacy guidelines. After the first phase, we proceed by developing privacy management module. This is going to be the gathering of user requirements through survey and interview that involve the stakeholders mentioned in previous section. Next phase is the design of privacy module prototype to check the interface design and develop the privacy management module and evaluate the design. We will then later evaluate the design then finally implement the design.

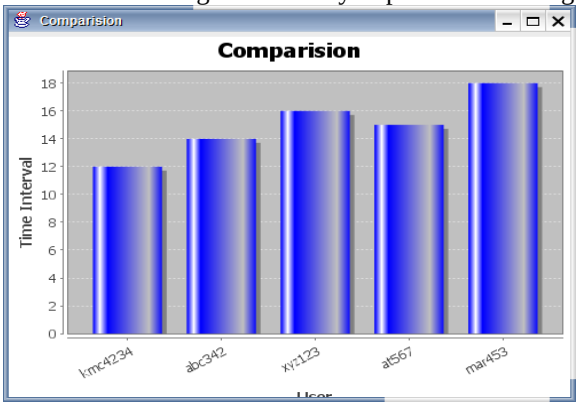

Fig. 4: Comparison Chart

The experimental setup to compare both the architectures is shown in Figure 4. The scenario consists of a hospital room with twenty patient nodes reading patient's medical data from various data [24-25].

Every patient node transmits about 8.7 kbits (payload) of data per second. Figure 5 summarizes the average power consumption (mW) by the patient (client) data.

Fig. 5: Quality Analysis

VI. Conclusions

In this paper, we offered wireless systems for remote observation of bio-medical data's to alleviate problems in traditional health observation systems and to improve the quality of medical care. Two variants of the wireless health observation systems are implemented to remotely monitor patients. Each of the problems listed have been discussed in detail and we have proposed suggestions to address each of them. From the problems, we chose one to be addressed in our subsequent research that is the privacy policy management difficulties faced by end users of a pervasive healthcare observation system. To address these difficulties, we plan to propose architecture for a privacy-sensitive pervasive observation system. The requirements will be gathered from end users and application developers. The architecture will provide a framework that can be used by application developers to develop a privacy-sensitive application for the end users.

Reference

[1] Istepanian. R. S. H, Jara. A. J, Sungoor. A, Philips. N, "Internet of Things for M-health applications (IoMT)", in Proc. AMA IEEE Medical Tech. Conf. Individualized Healthcare, 2010.
[2] Varshney. U, "Pervasive healthcare and wireless health observation. Mob.Netw. Appl", 12, 113-127, 2007.
[3] Kosseim. P, Emam. K.E, "Privacy Interests in Prescription Data, Part I: Prescriber Privacy. IEEE Security and Privacy 7", 72-76, 2009.
[4] Jenkins. D, Gerred. S, "Electrocardiogram (ECG, RKG) library", Vol. 2009.
[5] Schilit. B, Hong, J., Gruteser, M. "Wireless Location Privacy Protection. Computer 36", 135-137, 2003.
[6] Beckwith. R, "Designing for Ubiquity: The Perception of Privacy. IEEE Pervasive Computing 2", 40-46, 2003.
[7] Kai. W, Yan. S, Xukai. Z, Durresi. A, Shiaofen. F, "Pervasive and Trustworthy Healthcare. Advanced

Information Networking and Applications", 750-755, 2008.

[8] Goethe. J.W, Bronzino. J.D, "An expert system for observation psychiatric treatment. Engineering in Medicine and Biology Magazine, IEEE 14", 776-780, 1995.

[9] A.J. R, "Wireless physiological observation for psychiatric patients. Mechanical and Mechatronic Engineering" Vol. MScEng. University of Stellenbosch, 2008.

[10] Varshney. U, "Managing Comprehensive Wireless Patient Observation Pervasive Health Conference and Workshops, 2006 (2006) 1-4

[11] Sadeh. N, Hong. J, Cranor. L, Fette. I, Kelley. P, Prabaker. M, Rao. J, "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application. Journal of Personal and Ubiquitous Computing", 14, 2008.

[12] Hong. J.I, Landay. J.A, "An architecture for privacy-sensitive ubiquitous computing. Proceedings of the 2nd international conference on Mobile systems, applications, and services. ACM, Boston, MA, USA", 2004.

[13] Hong. J, Satyanarayanan. M, Cybenko. G, "Security & Privacy. Pervasive Computing, IEEE", 2007.

[14] Kara. A, "Protecting Privacy in Remote-Patient Observation. Computer 34", 24-27, 2001.

[15] Kelley. P.G, Drielsma. P.H, Sadeh. N, Cranor. L.F, "User-Controllable Learning of Security and Privacy Policies. ACM CCS", 2008.

[16] Kim. J, Beresford. A, Stajano. F, "Towards a Security Policy for Ubiquitous Healthcare Systems (Position Paper). Ubiquitous Convergence Technology", 263-272, 2007.

[17] Martino. L.D, Qun. N, Dan. L, Bertino. E, "Multi-domain and privacy aware role based access control in eHealth. Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference", 131-134, 2008.

[18] Puzar, M., Plagemann, T., Roudier, Y.: Security and privacy problems in middleware for emergency and rescue applications. Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference (2008) 89-92

[19] Sadeh. N, Hong. J, Cranor. L, Fette. I, Kelley. P, Prabaker. M, Rao. J, "Understanding and capturing people's privacy policies in a mobile social networking application. Personal Ubiquitous Comput. 13", 401-412, 2009.

[20] Weerasinghe. D, Elmufti. K, Rajarajan. M, Rakocevic. V, "Patient's privacy protection with anonymous access to medical services. Pervasive Computing Technologies for Healthcare", 127-130, 2008.

[21] Adlam. T.D, Evans. N, Gibbs. C, Orpwood. R, "User Evaluation of Smart Flats for People with Dementia. Pervasive Health Conference and Workshops", 1-4, 2006.

[22] Butz. A, Kruger. A, "User-centered development of a pervasive healthcare application. Pervasive Health Conference and Workshops ", 1-8, 2006.

[23] Dong. C, Dulay N, "Privacy Preserving Trust Negotiation for Pervasive Healthcare. Pervasive Health Conference and Workshops", 1-9, 2006.

[24] Elmufti. K, Weerasinghe. D, Rajarajan. M, Rakocevic. V, Khan. S, "Privacy in Mobile Web Services eHealth. Pervasive Health Conference and Workshops", 1-6, 2006.

[25] Jasemian. Y, "Security and privacy in a wireless remote medical system for home healthcare purpose. Pervasive Health Conference and Workshops", 1-7, 2006.

