Impact of Data Privacy and Confidentiality on Developing Telemedicine Applications: A Review Participates Opinion and Expert Concerns

1,2,3B.B. Zaidan, 1,2,3A.A. Zaidan and 3,4M.L. Mat Kiah
1Faculty of Engineering, Multimedia University, 63100, Selangor Darul Ehsan Cyberjaya, Malaysia
2Predictive Intelligence Research Cluster, Sunway University, No 5, Jalan Universiti, Bandar Sunway, 46150 Petaling Jaya, Selangor, Malaysia
3Network and Communication Security Research Group, ICT and Computational Science Research Cluster, University of Malaya, 50603 Kuala Lumpur, Malaysia
4Faculty of Computer Science and Information Technology, University Malaysia, 50603, Kuala Lumpur, Malaysia

Abstract: Telemedicine referred to any health care delivery application using an active media such as internet, mobile platforms, or satellites to communicate the parties. Telemedicine can be as simple as patient-doctors phone call, or as complex as the remote surgeries (telesurgery). Telemedicine applications required highly secured systems. In this study we will review the impact of data privacy and confidentiality on developing telemedicine applications. Moreover, we will support this review by short survey on 130 participants to support the literature evidence.

Key words: Telemedicine, patient records, privacy, m-health, e-health, security, health informatics

INTRODUCTION

Websites are now a major vehicle through which health care agencies deliver information to the public, also known as e-health. When mobile platform deliver the medical information it become m-health. Through Information Communication Technology (ICT), particularly the Internet, e-health and m-health can deliver public services in a much convenient, cost-effective and altogether different and better way. Realizing the potential benefits of ICT, health care delivery agencies began actively posting information on the websites and other communication tools. In ensuring the success of e-health initiative, a level of trust is required from all transaction such as patients-doctors, doctors-public within health delivery agencies and between agencies itself. The issue of trust involves two special concerns to any online service, these are privacy and security (Jun and Hua, 2010; Toorani and Beheshti Shirazi, 2009; Kimou et al., 2010). In the telemedicine applications privacy is refers as a protecting personal information by the health agencies that collect about individuals whereas, security is refers as protecting e-health sites from attack and misuse. While e-health is working in an open environment (internet), the issues of privacy and security are of great concern especially to decision makers and designers of e-health systems (Alanazi et al., 2010b; Chen et al., 2010; Mirza et al., 2009). Government around the world has invested a huge amount of money and time to ensure the security of electronic transactions by constantly enhancing the information security infrastructure (Abomhara et al., 2010; Alam et al., 2010; Zaidan et al., 2010a,d,f). But, unfortunately many security breaches over health website still exist and the continuing emergence of attack and misuse can affect users’ trust and confidence towards the e-health services and hinder them from using e-health services. Thompson et al. (2011) made a study on document and describe online portrayals of potential patient privacy violations in the social networks, in particular, Facebook profiles of medical students and residents. They found that (49.8%) of all eligible students and residents had Facebook profiles. There were 12 cases of potential patient violations, in which residents and students are posted photographs of care they provided to the individuals. Jones et al. (2011) stated researchers whom are using forums, blogs and online groups-based, they need to make sure they are safe and need tools to make best use of the data. Though it is about time to develop a security system than can truly effective in protecting the e-health sites and efficient in protecting individuals personal information.

THE IMPACT OF SECURITY ON TELEMEDICINE APPLICATIONS

Recently, Researchers have paid direct attention to the area of telemedicine applications (Jayashree and Marthandan, 2010). Telemedicine is a broad word for any
application of clinical medicine where medical information is transferred through interactive media for the purpose of consulting and sometimes remote medical procedures. Telemedicine may be as simple as two health professionals discussing a case over the telephone. Recently, several telemedicine examples available such as e-health (Seetharaman et al., 2010), m-health (Viswacheda et al., 2007), medical records (Bhuvaneswari et al., 2007), transfer medical records, diagnosis systems (Khanale and Ambilwade, 2011), tele-emergency (Jawahitha et al., 2007) and health information systems Farahbakhsh et al. (2007). Due to the development of internet technology, many transactions are carried out through the internet. Recently, most of transactions cannot be done by face-to-face based approaches. The key problems of these applications are on how to secure the applications and how to authenticate the identities of the involved parties. Therefore, many security mechanisms and authentication methods have been presented during the past few years. Authentication protocol based on cryptographic technologies, biometrics, graphic passwords and smart cards are used to confirm the identities of parties in the communication (Meng and Shao, 2010; Meng, 2009a,b; Abu Ali et al., 2010). Telemedicine is a rapidly growing area, however, services provided by telemedicine is yet to be trusted. One of the most important factors to ensure the successful implementation of telemedicine is the data privacy (Fig. 1). According to Wicks et al. (2010), Among respondents in the center for health information technology study, 75% who were not using a PHR; they reported their worries about the privacy of their information as one of the most important reasons for not using PHRs, compared with 51% of respondents who had concerns about cost, 38% who were concerned with how much time it would take and 26% who did not like computers or the Internet. Weitzman et al. (2010) said “subjects linked the tight security controls as factor that would increase willingness to share their medical data for health research”. According to Fernandez-Laque et al. (2011), several social network users tend to fake information to protect their privacy. For instance, in a study of Facebook profiles, it was found that 8% of the users had fake names. In the security, control over user accessing to the system is known as authentication. The most well-known authentication controls mechanisms are passwords and biometrics. Biometrics refers to the measurement of specific features for human body, such as the fingerprints, irises and even the voice, with the purpose to distinguish the person (Ilyas et al., 2010; Luo et al., 2010). These characteristics are unique to each individual thus the developers implement it to be an access password to the user. Password is a regular type of first layer defends strategy to determine that a computer user requesting access to a computer system. Password is very vulnerable to interception especially when transmitted over a network to authentication machine. Once the password is compromised, the intruders can cause a great harm and significant financial losses. According to El-Emam et al. (2011), passwords

Fig. 1: Security concerns of telemedicine applications
are not recommended to secure the electronic medical records; moreover, they provided an experiment on which they were able to crack the passwords for 93% of the files (14/15). Biometric systems are now becoming an alternative solution to access the electronic health records. Biometric widely used by many organizations to provide greatest level of security because it more reliable than password and it represent the user.

INFORMATION SECURITY

Information security is defined as the field of science that concerns about protecting the information and data from attackers or security threats (Wang, 2011; Al-Azawi and Fadhil, 2010). Numbers of method are available to secure data such as encryption methods or to ensure secure access (i.e., authentication) using biometrics (Luo et al., 2011). Data privacy refers to the relationship between technology and the legal right to public expectation of privacy in the collection and sharing of data about one's self (Haque et al., 2009).

Survey conducted by telemedicine and health informatics associations: Telemedicine and Health Informatics Associations (THIA) is an association focus on the development of e-health and m-health systems. THIA support the research and gathering the data on the related topics to the health informatics. Moreover, THIA interest on the knowledge sharing for health care applications.

Ethical statement: Consent of the participant was obtained with detailed information given before commencement of the study. Data protection and confidentiality were maintained all through the study.

Data collection: The primary data used in the research is composed of data gathered through questionnaires, a short questionnaire has been distributed through a survey form; this form was designed and distributed to targeted highly educated people and medium educated people. Besides the basic demographic questions, four other questions were asked pertaining to their concerns on using e-health systems. A total of 130 respondents participated in the questionnaire survey.

Demography of the respondents: The questionnaire has been randomly distributed to cover a wide range of age and gender, the respondents have not been asked for their nationality, however, they have been asked about the level of education and been classified into two groups, highly educated people (i.e., who hold master or above) and medium educated people (i.e., people who hold degree or less) (Fig. 2).

Fig. 2: Demography of the respondents

Part two: Part two of the questionnaire consists of four questions which are:

- **Question one:** Have you subscribed to any telemedicine applications?

As shown in Fig. 3, People who have highly education level, they subscribe mostly in the telemedicine applications. While people from medium education level had less subscriptions.

- **Question two:** If you want to subscribe in telemedicine application, what will be the considered factors? (Security, cost or Management)

As depicted in Fig. 4, people are mostly consider the security more than other factors to subscribe on telemedicine applications, 50% of the participates considered the security comparing with 32% considered the cost and 18% for management.

- **Question three:** Would you mind if your health data is being available for others?

One twenty eight out of 130 said, No and 2 said they don’t mind, this ratio depicted the important of the privacy on telemedicine applications.

- **Question four:** If someone publishes your pictures and your health records in the internet, would you submit the case to courts?

384
implementation (Nabi et al., 2010; Alanazi et al., 2010a) both have done their research on electronic medical records security. Nabi et al. (2010) stated the important using strong security tools can increase the number of users in the e-health and m-health.

The present study made the following recommendations:

- Several algorithms are available to secure the telemmedicine applications such as AES, NTRU, ECC, RSA and etc. (Zaidan et al., 2010b, c; Ahmed et al., 2010) However, using symmetric algorithms cannot stand alone due to the challenges of the non-repudiation, authorization and authentication (Alanazi et al., 2010a, Zaidan et al., 2010c). Therefore, we recommend either using asymmetric algorithms or implement hybrid approaches consist of symmetric and asymmetric

- Design and implement secure algorithms for authentication purposes; these algorithms can be developed using biometrics, hybrid passwords with tokens or graphic passwords to ensure the authorize access (Alsaaed, 2010; Sayeed et al., 2010; Liao et al., 2009)

- Create a clear global law to protect the patient rights under the cyber crime umbrella (Eneh, 2010)

ACKNOWLEDGMENTS

This research has been funded from Telemedicine and Health Informatics Associations under grant number THIA-11-001. Authors would like to acknowledge Multimedia University and Sunway University for providing several researches facilities, important recourses and providing experts’ consultations to improve this study.

REFERENCES


