International Journal of Pharmacology, 2011
ISSN 1811-7775 / DOI: 10.3923/ijp.2011.

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

[1,2,3]B.B. Zaidan and [1,2,3]A.A. Zaidan
[1]Faculty of Engineering, Multimedia University, 63100, Selangor Darul Ehsan Cyberjaya, Malaysia
[2]Predictive Intelligence Research Cluster, Sunway University, No 5, Jalan Universiti,
Bandar Sunway, 46150 Petaling Jaya, Selangor, Malaysia
[3]Network and Communication Security Research Group, ICT and Computational Science Research Cluster,
University of Malaya, 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 participates 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 collects about individuals whereas, security is refers as protecting e-heath sites from attack and misuse. While e-health is working in an open environment (internet), the issues of privacy and security are of great concerns 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

Corresponding Author: B.B. Zaidan, Faculty of Engineering, Multimedia University, 63100, Selangor, Darul Ehsan, Cyberjaya, Malaysia Tel: 0060104204377

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-Luque *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

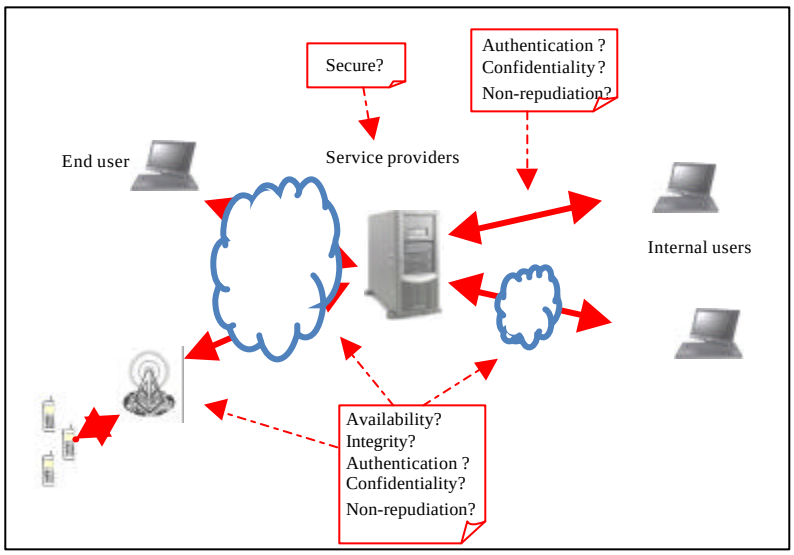

Fig. 1: Security concerns of telemedicine applications

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).

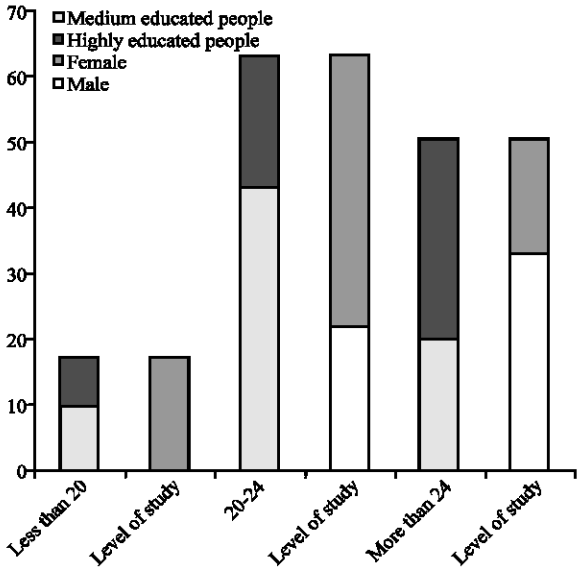

Fig. 2: Demography of the respondents

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 subscript 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?

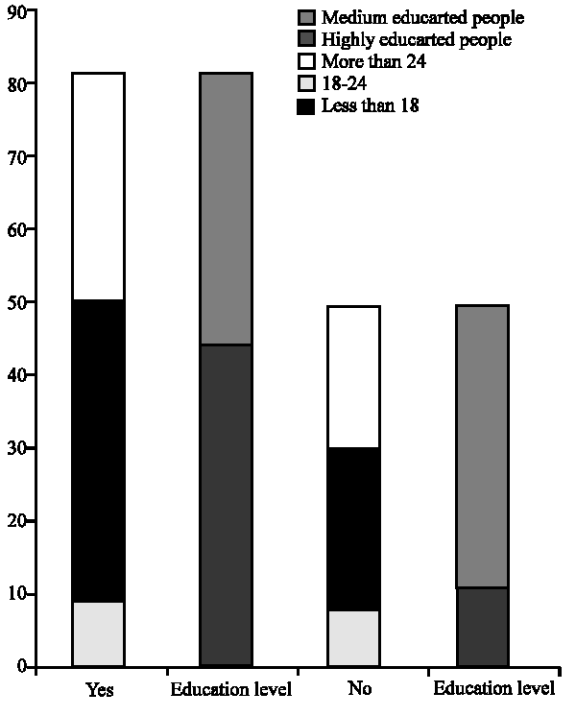

Fig. 3: Subscriptions on telemedicine applications

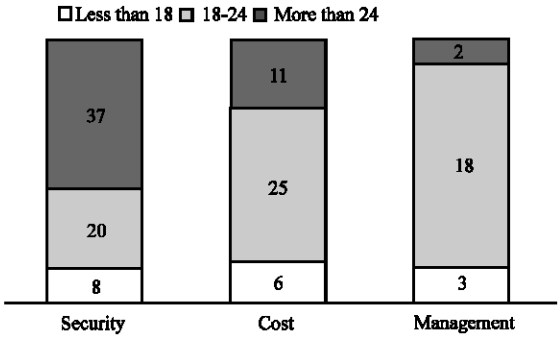

Fig. 4: The considered factors for the participate to apply

As in question three 128 out of 130 said definitely Yes, while 2 said No. The two who said No explained why they don't want to submit the case to the court, they said such cases take longtime and yet there is no clear protocol in the law to support these cases.

DISCUSSION AND RECOMMENDATION

According to Judi *et al.* (2009) Successful implementation of telemedicine is related to the availability of three factors: strong fundamental knowledge and infrastructure, planning and management of health information and technology and fulfillment of legal and ethical issues and constant evaluation of telemedicine 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 telemedicine 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*., 2010e). 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 (Alsaade, 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

Abomhara, M., O. Zakaria, O.O. Khalifa, A.A. Zaidan, B.B. Zaidan and O.A. Hamdan, 2010. Overview: Suitability of using symmetric key to secure multimedia data. J. Applied Sci., 10: 1656-1661.

Abu Ali, A.N., A.K. Alnaimat and H.Y. Abu-Addose, 2010. Evaluating the vulnerability and the security of public organizations websites in Jordan. J. Applied Sci., 10: 2447-2453.

Ahmed, M.A., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2010. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Applied Sci., 10: 59-64.

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Alam, G.M., M.L.M. Kiah, B.B. Zaidan, A.A. Zaidan and H.O. Alanazi, 2010. Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. Sci. Res. Essays, 5: 3254-3260.

Alanazi, H.O., M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan and G.M. Alam, 2010a. Secure topology for electronic medical record transmissions. Int. J. Pharmacol., 6: 954-958.

Alanazi, H.O., H.A. Jalab, G.M. Alam, B.B. Zaidan and A.A. Zaidan, 2010b. Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. J. Med. Plants Res., 4: 2059-2074.

Alsaade, F., 2010. A study of neural network and its properties of training and adaptability in enhancing accuracy in a multimodal biometrics scenario. Inform. Technol. J., 9: 188-191.

Bhuvaneswari, T., N. Dutta and S.K. Srivatsa, 2007. Distributed virtual patient record system. Inform. Technol. J., 6: 766-770.

Chen, T.S., J. Chen and Y.H. Kao, 2010. A novel hybrid protection technique of privacy-preserving data mining and anti-data mining. Inform. Technol. J., 9: 500-505.

El-Emam, K., K. Moreau and E. Jonker, 2011. How strong are passwords used to protect personal health information in clinical trials. J. Med. Internet Res., 13: e18-e18.

Eneh, O.C., 2010. Technoscience in crime detection and control: A review. J. Applied Sci., 10: 1873-1884.

Farahbakhsh, M., S. Fozounkhah, H. Sadeghi-Bazargani, A. Zakeri, N. Houshiyan, N. Asmani and A. Naghili, 2007. The study of health information system performance from managers and expert's viewpoints. Inform. Technol. J., 6: 227-231.

Fernandez-Luque, L., R. Karlsen and J. Bonander, 2011. Review of extracting information from the social web for health personalization. J. Med. Internet Res., 13: e15-e15.

Haque, A., A. Zaki-Hj-Ismail and A.H. Daraz, 2009. Issues of E-banking transaction: An empirical investigation on malaysian customers perception. J. Applied Sci., 10: 1870-1879.

Ilyas, M.Z., S.A. Samad, A. Hussain and K.A. Ishak, 2010. Improving speaker verification in noisy environments using adaptive filtering and hybrid classification technique. Inform. Technol. J., 9: 107-115.

Jawahitha, S., M. Ishak and M. Mazahir, 2007. E-data privacy and the personal data protection bill of Malaysia. J. Applied Sci., 7: 732-742.

Jayashree, S. and G. Marthandan, 2010. Government to E-government to E-society. J. Applied Sci., 10: 2205-2210.

Jones, R., S. Sharkey, J. Smithson, T. Ford and T. Emmens *et al*., 2011. Using metrics to describe the participative stances of members within discussion forums. J. Med. Internet Res., 13: e3-e3.

Judi, H.M., A.A. Razak, N. Shaari and H. Mohamed, 2009. Feasibility and critical success factors in implementing telemedicine. Inform. Technol. J., 8: 326-332.

Jun, D. and L.W. Hua, 2010. A security routing optimization scheme for multi-hop wireless networks. Inform. Technol. J., 9: 506-511.

Khanale, P.B. and R.P. Ambilwade, 2011. A fuzzy inference system for diagnosis of hypothyroidism. J. Artificial Intel., 4: 45-54.

Kimou, K.P., B. Barry, M. Babri, S. Oumtanaga and T.L. Kadjo, 2010. An efficient analysis of honeypot data based on markov chain. J. Applied Sciences, 10: 196-202.

Liao, H.C., C.H. Hsieh, C.W. Chen and W.C. Chen, 2009. The security snalysis and enhancement of photographic authentication. Inform. Technol. J., 8: 1170-1179.

Luo, H., F.X. Yu, J.S. Pan, S.C. Chu and P.W. Tsai, 2010. A survey of vein recognition techniques. Inform. Technol. J., 9: 1142-1149.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Meng, B., 2009a. A secure non-interactive deniable authentication protocol with strong deniability based on discrete logarithm problem and its application on Internet voting protocol. Inform. Technol. J., 8: 302-309.

Meng, B., 2009b. Formalizing deniability. Inform. Technol. J., 8: 625-642.

Mirza, A.P., A. Wallstrom, M.T.H. Beheshti and O.P. Mirza, 2009. Internet banking service adoption: Private bank versus governmental bank. J. Applied Sci., 9: 4206-4214.

Meng, B. and F. Shao, 2010. Computationally sound mechanized proofs for deniable authentication protocols with a probabilistic polynomial calculus in computational model. Inform. Technol. J., 10: 611-625.

Nabi, M.S.A., M.L.M. Kiah, B.B. Zaidan, A.A. Zaidan and G.M. Alam, 2010. Suitability of SOAP protocol in securing transmissions of EMR database. Int. J. Pharmacol., 6: 959-964.

Sayeed, S., A. Samraj, R. Besar and J. Hossen, 2010. Online hand signature verification: A review. J. Applied Sci., 10: 1632-1643.

Seetharaman, A., J.R. Raj and A.S. Saravanan, 2010. The changing role of accounting in the health care industry. Res. J. Bus. Manage., 4: 91-102.

Thompson, L.A., E. Black, W.P. Duff, N.P. Black, H. Saliba and K. Dawson, 2011. Protected health information on social networking sites: Ethical and legal considerations. J. Med. Internet Res., 13: e8-e8.

Toorani, M. and A.A. Beheshti Shirazi, 2009. An elliptic curve-based signcryption scheme with forward secrecy. J. Applied Sci., 9: 1025-1035.

Viswacheda, D.V., L. Barukang, M.Y. Hamid and M.S. Arifianto, 2007. Performance evaluation of mobile ad hoc network based communications for future mobile tele-emergency system. J. Applied Sci., 7: 2111-2119.

Wang, Y., 2011. Unconditional security of cryptosystem: A review and outlook. Trends Applied Sci. Res., 6: 554-562.

Weitzman, E.R., L. Kaci and K.D. Mandl, 2010. Sharing medical data for health research: The early personal health record experience. J. Med. Internet Res., 12: e14-e14.

Wicks, P., M. Massagli, J. Frost, C. Brownstein and S. Okun *et al*., 2010. Sharing health data for better outcomes on PatientsLikeMe. J. Med. Internet Res., 12: e19-e19.

Zaidan, A.A., B.B. Zaidan, A.K. Al-Fraja and H.A. Jalab, 2010a. Investigate the capability of applying hidden data in text file: An overview. J. Applied Sci., 10: 1916-1922.

Zaidan, A.A., B.B. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010b. An overview: Theoretical and mathematical perspectives for advance encryption standard/rijndael. J. Applied Sci., 10: 2161-2167.

Zaidan, A.A., B.B. Zaidan, A.Y. Taqa, K.M.S. Mustafa, G.M. Alam and H.A. Jalab, 2010c. Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. Int. J. Phys. Sci., 5: 1992-2000.

Zaidan, A.A., B.B. Zaidan, H.O. Alanazi, A. Gani, O. Zakaria and G.M. Alam, 2010d. Novel approach for high (Secure and rate) data hidden within triplex space for non multimedia file. Sci. Res. Essays, 5: 1965-1977.

Zaidan, B.B., A.A. Zaidan, A. Taqa, G.M. Alam, M.L.M. Kiah and H.A. Jalab, 2010e. StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem. Int. J. Phys. Sci., 5: 1796-1806.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010f. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.