World Applied Sciences Journal 32 (4): 688-692, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.32.04.907

Privacy and Security Problems in Using Health Information Application in Smart National Identity Card (SNIC)

Ismail Bile Hassan and Masrah Azrifah Azmi Murad

Department of Information System, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Malaysia

Abstract: This study discovers privacy and security problems in using health information application in SNIC. Many countries introduced smart national identity card with various applications such as health information application embedded inside it. The need for avoiding a long queue at hospitals, airports and shopping mall etc. has led to the introduction of smart cards. These smart national identity cards are resulting uncontrollable troubles with confidentiality attack, illegal accessing of database, fraud, planned crime and untrustworthiness of biometric identification. Studies on the general acceptability of the various SNIC's applications have been conducted but the privacy and security problems in using them have yet to be investigated. Hence, this research investigates the privacy and security problems in using health information application in SNIC and extends better understanding on the relevant factors that the government and the application providers would need to consider in predicting citizens' technology usage in the future. Survey questionnaires on the privacy and security problems in using health information application were distributed to public and private hospitals. The study discovered that there are privacy and security problems in using health information application in SNIC.

Key words: Smart National Identity Card · Health Information application · Health Data · Privacy and Security problems

INTRODUCTION

Smart card can be defined as a normal plastic card that has processor and memory chip integrated inside it in order to operate certain functions [1]. In case of smart national identity card, it is a portable plastic card with digitally embedded information that citizens are encouraged or required to carry as a means of confirming their identity [2]. The earliest smart card application was established by [3] in 1974 and then thousands of smart card applications have appeared and it is one of the greatest achievements in the world of information technology [4]. The need for avoiding a long queue at hospitals, airports and shopping mall has led to the introduction of smart cards [5]. The smart national identity cards are also resulting uncontrollable troubles with confidentiality attack, illegal accessing of database, fraud, planned crime; untrustworthiness of biometric identification, etc. and the adoption of such innovations has yet to be studied [6].

Smart national identity card is a bit of plastic card with sizes of a typical credit card and a built in microchip. It utilizes biometric technology with thumbprints being encrypted in its chip [7]. There are many applications that can be included in SNIC for instance, some of the embedded applications in the Malaysian multipurpose smart national identity card (MyKad) are: driving license, national identity card (NIC), health information, automated teller machine (ATM) access, passport information, electronic purse, public key infrastructure, travel application known as frequent teller card and Touch 'n Go [8]. However, many studies on the general acceptability of the various SNIC's applications have been conducted by [9-11] but the security and privacy problems in using them have yet to be studied [12].

Moreover, many countries are following the Malaysian multipurpose smart national identity card model. The privacy and security problems in using health information application embedded SNIC remains unknown to many governments and the application providers as

Corresponding Author: Ismail Bile Hassan, Department of Information System, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Malaysia.

well. There is no research on the privacy and security problems in using health information application in SNIC. As such, the aim of this study is to investigate on the privacy and security problems in using SNIC's health information application in the Malaysian context.

Related Works: Privacy can be defined as the implication that individuals make an assessment of their ability to protect their information in order to determine what level of protection of their data is possible. That is, they assess whether, under given circumstances, the information someone gives to another is, as it were, safe in their hands [13]. Considering the use of e-government technologies such as smart national identity card applications, citizens have limited choices and them to feel confident and use e-Government; they must be reassured about the systems' security and privacy [14, 15]. A recent study on the views of 490 patients and their physicians (46 in total) undertaken in Canada regarding health information and privacy [16] found that although 48% of the patients and 63% of doctors think that patient data must be limited to the family physician, more than 90% endorsed the usefulness of computers to facilitate the distribution of health data with other healthcare staff.

Furthermore, Security and Privacy are also major concerns among healthcare professionals and patients [17-19]. Patients worry that their health information may be used without permission. Some worry that their mental and sexual health issues will be made known to healthcare providers not directly involved in their care, thus compromising patient confidentiality and doctor-patient relationships. Thus, access to certain aspects of a patient's medical record should be restricted to certain healthcare providers. Patients also worry that their family may access their health records by pretending to be the patient. Cost and reluctant to use the system by the healthcare professionals might be a barrier to the implementation of the health information application in SNIC as well [18].

According to the privacy law of medical records in Malaysia, the Code of Medical Ethics asserts that patients are entitled to receive a copy of their medical records and doctors are obliged to provide this report without unreasonable delay [20]. The identification number of a multipurpose smart national card(MyKad) holder can be applied to read and view all types of data about the citizens if the user of the card reader has access privilege to such data [21]. However, The implications of not meeting patients' trust expectations could have serious consequences, such as a reluctance on behalf of the patient to go to a doctor, patients may provide misleading, or incomplete information about their condition since they don't have any other choice rather than themselves to the doctor, the doctor or the patient may be reluctance to use ICT mediated services, less patient self-management and less growth in knowledge and expertise for patients regarding their own health or their health conditions [22].

Therefore, a study on the privacy and security problems in using health information application in SNIC is required in order to introduce proper policies and initiatives to increase its acceptance since the use of this application may result increased productivity, improved patient care, reductions in medical error that affect patient safety[18].

MATERIALS AND METHODS

The survey was limited to public and private hospitals in the Multimedia Super Corridor(MSC) area because (1) the National Registration Department (NRD) offices load with complete applications in MyKads issued at these areas while there are less applications loaded with those issued by other NRD branches, (2) the government has chosen this area for the MyKad pilot project and (3) the necessary infrastructure needed for MyKad implementation is currently available at MSC area since it is regarded as the "Silicon Valley "of Malaysia. Hence, the respondents in this area are assumed to have sufficient awareness and technical knowledge of the technological developments such as MyKad and are expected to be able to provide satisfactory responses to the topic surveyed.

The survey questionnaire papers were submitted to six hospitals in order to first get permission from the hospital management as to conduct the survey. However, three out six hospitals only permitted to distribute the survey questionnaire to their hospitals. The survey questionnaire papers were distributed equally among the male and female respondents. Table 1 and 2 present gender and occupation of the respondents, Table 3 shows the overall frequency distribution and test statistics for health information application in SNIC questionnaire items.

Table 1: Gender of the respondents

	Frequency	Percent(%)
Male	7	21.2
Female	26	78.8
Total	33	100.0

Table 2: Occupation of the respondents

	Frequency	Percent (100%)
Registration Officer	15	45.5
Doctor	11	33.3
Nurses	1	3.0
Patients	3	9.1
Others	3	9.1
Total	33	100.0

RESULTS AND DISCUSSION

The questions consist of (1) the respondent's demographic information; (2) questions about the privacy and security problems in using health information application in SNIC. The study consists of 9 questionnaire items measuring privacy and security problems in using SNIC's health information application.

Eighty (80) copies of the survey questionnaire papers were distributed among the three hospitals but 52 questions were received from them. The respondents completed 33 questionnaire papers while the remaining 19 were incomplete. The Statistical Package for Social Science (SPSS) software is utilized to analyze the data whereas frequency and Chi-Square test are applied.

Table 3 shows the frequency distribution and test statics of the items. The responses are coded as 1=yes which means the respondents agree with the question and 0=no that means the respondents don't agree with it. As usual, frequency and chi square tests are used to present the results. The first five items in Table 3 are about privacy problems in using health information application in SNIC. For example, 69.7% of the respondents enlighten that patients worry that their family may access their health records by pretending to be the patient and 72.7% of them concluded that using health information application in SNIC would erode their privacies. However, the respondents did not state other privacy problems in using health information application in SNIC.

The items from no. 6 to 9 in table 3 are related with security problems in using health information application in SNIC from the literature. It can be concluded that there are security problems in using health information application in SNIC as more than 66% of the respondents agreed on the security problems. But respondents did not highlight other security problems. For instance, 87.9% agreed that health information application in SNIC is vulnerable to loss and theft.

In addition to that, Table 3 shows the Chi-Square, degree of freedom (df) and significance of the dichotomous scale questionnaire items. However, there will be null hypothesis that specifies the expected frequency of each category (i.e. yes or no). The null hypothesis assumes that half of the respondents will say yes and the other half will say no to each questionnaire item. The observed frequency may be different than that expected by the null hypothesis. In table 3, zero cells have expected frequency less than 5 and which is a good indication; the larger chi square the more likely to reject the null hypothesis. The degree of freedom (df) is 1 as shown in the above table 3 (i.e. 2 categories - 1 = 1). P value is the probability that the null hypothesis is correct. It is statistically significant if the p value is less than 0.05 and the null hypothesis will be rejected while accepting the testing hypothesis as valid. If the p value is greater than 0.05 than the null hypothesis is retained.

Table 3: Overall Frequency Distributions and test statistics for health information application in SNIC questionnaire items

	Test Statistics				Distribution of Respondents	
					1	0
Item	N[b]	Chi-Square	df	Asymp. Sig.	Yes N[b]%	No N[b]%
i. Privacy Problems in using Health Information Application in SNIC						
1. Health information may be used or edited without permission.	33	16.030[a]	1	.001	28 (84.8)	5 (15.2)
2. Patients worry that their organ implants and chronic diseases will be made known to healthcare providers not directly involved in their care.	33	8.758[a]	1	.003	25 (75.8)	8 (24.2)
3. Patients worry that their family may access their health records by pretending to be the patient.	33	5.121[a]	1	.024	23 (69.7)	10 (30.3)
4. Using e-health application in SNIC would erode my privacy.	33	6.818[a]	1	.009	24 (72.7)	9 (27.3)
5. Others	33		1		0	100
ii. Security Problems in using Health Information in SNIC						
6. It is not secure to load health information into my SNIC.	33	3.667[a]	1	.056	22 (66.7)	11 (33.3)
7. E-health card in SNIC is easily to be forged.	33	3.667[a]	1	.056	22 (66.7)	11 (33.3)
8. Health information in SNIC is vulnerable to loss and theft.	33	18.939[a]	1	.001	29 (87.9)	4 (12.1)
9. Others	33	29.121[a]	1	.001	1 (97)	32 (3)

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 16.5.

b. N=Total number of respondents

The data in the tables 3 is analyzed using chi square goodness of fit. The p values of 5 items in table 3 are less than 0.05 and therefore are statistically significant, for example, out of 33 respondents in total, we evaluated if the number of respondents agreed that health information may be used or edited without permission (28) is equal to the number of respondents who did not agree that health information may be used or edited without permission (5). The null hypothesis is rejected as $p<0.05$ for this item. 84.8% of the respondents agreed that their health information may be used or edited without permission which is a strong validation that there is privacy problem in using health information application in SNIC. Moreover, 87.9% of the respondent agreed that Health information in SNIC is vulnerable to loss and theft and this testifies that there is security problem in using health information application in SNIC as $P<0.05$. The same explanation goes to the other remaining items in table 3. We can conclude that there are privacy and security problems in using health information in SNIC since p value is statistically significant for most of the items in table 3.

CONCLUSION

Privacy and security are of fundamental importance to health information application in smart national identity card especially as it pertains to the confidentiality of personal health data. The analysis of the study provides a root for the researcher to validate the identified privacy and security problems in using health information application in SNIC from the literature in the context of this study. The researcher discussed and analyzed the data using quantitative method. Most of the respondents agreed to that there are privacy and security problems in using health information application in SNIC. Therefore, the governments and application providers need to ensure the privacy and security features of this application as to gain citizens' trust. Moreover, further study can be done on trust and risks factors related with health information application in SNIC.

REFERENCES

1. Mahmut, T., 2011. Identifying Factors that facilitate the use of Multi-Purpose Smart Cards by University Students: An empirical investigation. Informatics institute. Ankara, Middle East Technical University Master, pp: 99.
2. Anneshwa, 2007. National Identity Card in India : Still a dream. Retrieved May 18, 2010, from http://creative.sulekha.com/national-identity-card-in-india-still-a-dream_309276_blog.
3. Moreno, R., 1974. "Smart Card : Invented here."
4. Danielle, C.F., M.C.S. Paula, *et al*. 2007. "Issues Affecting the Implementation of Multiple Application Smart Card Systems."
5. 1Kamrul, I.M., 2012. Effective use of smart cards A case study of smart cards in Sweden http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-66300, Umeå University, Faculty of Social Sciences, Department of Informatics. Master
6. Nathan, A., 2009. Identity Cards : A global Perspective Global Research, Centre for Research on Globalization Montreal, Canada.
7. Yeow, P.H., P. Loo, Wee Hong Chong and Siong Choy, 2007. "Accepting Multipurpose "Smart" Identity Cards in a Developing Country." Journal of Urban Technology, 14(1): 23-50.
8. Yeow, P.H.P. and W.H. Loo, 2009. "Acceptability of ATM and transit applications embedded in multipurpose smart identity card: An exploratory study in Malaysia." International Journal of Electronic Government Research, 5(2): 37-56 (IGI Publishing; Scopus journal).
9. Yeow, P.H.P.F.M., 2005. "The Attitude of Malaysians Towards MyKad." Proceedings of the 4th International Conference on Information Technology in Asia 2005 (CITA '05).
10. Loo, W.H., P.H.P. Yeow and S.C. Chong, 2011. "Acceptability of Multipurpose Smart National Identity Card: An Empirical Study." Journal of Global Information Technology Management 14(1): 35-58. (Thomson ISI journal).
11. Yeow, P.H.P., *et al*., 2012. "Ergonomics issues in national identity card for homeland security, Applied Ergonomics." http://dx.doi.org/10.1016/j. apergo. 2012.04.017.
12. Mathews, T., 2004. "Is Malaysia's MyKad the 'One Card to Rule Them All'? The Urgent Need to Develop a Proper Legal Framework for the Protection of Personal Information in Malaysia," Melbourne University Law Review.
13. Goldbergm, I.W.D. and E. Brewer, 1997. Privacy-Enhancing Technologies for the Internet. IEEECOMPCON'97: pp: 103-109.

14. Sullivan, K.C.J., 2010. Balancing security and privacy in eGovernment services. In. Cunningham P, Cunninham M (eds) Proceedings IST-Africa 2010. IIMC International Information Management Corporation, Durban.
15. Ismail, H.A.A., 2008. Citizens' readiness for e-government in developing countries. PhD thesis, Middlesex University. (See: http://eprints.mdx.ac.uk/view/creators/Ismail=3AHany_A=2E_Abdelghaffar=3A=3A.html).
16. Perera, G.H.A., L. Thabane, G. Foster and D.J. Willison, (February 2011). "Views on health information sharing and privacy from primary care practices using electronic medical records." Int. J. Med. Informat, 80(2): 90-101.
17. McGinn, C.A.G.S., J. Duplantie, N. Shaw, C. Sicotte and L. Mathieu, 2011. " Comparison of user groups' perspectives of barriers and facilitators to implementing electronic health records." A systematic review. BMC Med., 9: 46.
18. Sellappans, R., S.S. Chua, *et al*., 2013. "Health innovation for patient safety improvement." Australasian Medical Journal, 6(1): 60-63.
19. Win, K.T.S.W. and Y. Mu, 2006. " Personal health record systems and their security protection.. " J Med. Syst., 30(4): 309-15..
20. Cieh, E., 2013. Limitations of the Personal Data Protection Act 2010 and Personal Data Protection in Selected Sectors. Beyond Data Protection. N. Ismail and E. L. Yong Cieh, Springer Berlin Heidelberg. pp: 65-98.
21. Yap Ai Kee, Y.C.N., Leau Yu Beng and Tan Soo Fun, 2012. "Security Issues on Identity Card in Malaysia." IA CSIT International Journal of Engineering and Technology, 4(5).
22. Duquenoy, P., N. Mekawie, *et al*., 2013. Patients, Trust and Ethics in Information Privacy in eHealth. eHealth: Legal, Ethical and Governance Challenges. C. George, D. Whitehouse and P. Duquenoy, Springer Berlin Heidelberg, pp: 275-295.