Enhanced e-Health Framework for Security and Privacy in Healthcare System

N. M. Shrestha[1], Abeer Alsadoon[1], P.W.C. Prasad[1], L. Hourany[1], A. Elchouemi[2]
[1]School of Computing and Mathematics, Charles Sturt University, Sydney, Australia
[2]Hewlett Packard Enterprise

***Abstract*—Patient health record (PHR) is a rising patient centric model which is frequently outsourced to store at third party. This addresses the issue in privacy such as hiding the sensitive health data of a patient which can be assessed by unauthorized users. In this paper, a new secured e-health framework has proposed. In this framework, patient centric personal data and access control scheme with enhanced encryption method has been considered. Security and privacy of personal health information have been identified by digital signature and patient pseudo identity as well as. This paper address the enhanced security model for more authentication and authorization functionality and expects to discover the new technique that can be utilized to build the efficiency in e-health care system based on security, privacy and user satisfaction. The survey has been conducted to test the proposed e-health framework. The data has been analyzed using SPSS tool.**

Keywords—Patient health record (PHR), e-health framework, authentication and authorization

I. Introduction

A new implementation of digital patient records, electronic management records, risk management, security tools, big data and all elements needed for better data security. Health Information is an information exchange which is linked and managed by the [1]. However, protecting information is not an easy job. Health care organizations are quickly confronting security dangers and vulnerabilities through the implementation of digitalization of patient records. However, the utilization of outdated and clinical applications that is not intended to safely work in the current organizational environment.

The goal of health care systems is to deliver the greatest health service for anyone at anytime from anywhere. Privacy is one of the major factors which has a sub factor in the form of confidentiality which is needed to prevent the disclosure of patients sensitive information [2]. In the health care sector, data security is a high priority, as it is essential to maintain access rights to data. Improving security in health care means maintaining privacy, and confidentiality of the patient and helps in preventing threats. It also helps to maintain secure communication between patients and doctor. The primary objective of the HIT is to meet three fundamental goals, confidential, integrity and availability with the overall aim of achieving security in Health Care.

The purpose of this research is to propose a secure Health care system from attacks by unauthorized users. In addition, this research aims to reduce the vulnerability and threats and increase user satisfaction based on security, performance and privacy. The paper is organized by contains the introduction in Section I, followed by literature review of current Health IT security in section II. The current and proposed frameworks are given in section III and section V. Discussion and conclusion are given in sections VI and VII respectively.

II. Literature Review

A. Impact of Security and Privacy in HIT

Cloud systems have been found to be problematic elsewhere in terms of security. The framework here is designed to facilitate sharing of electronic health records, for which [3] developed a model with the aim to maintain the growth, integration and large scale deployment of a wider variety of e health services. In addition, attribute based encryption cloud computing is used to store and share of personal health information securely. For achieving scalability extended attribute based encryption is labelled in a hierarchical structure [2].

According to Barua [2], combined hierarchical identity-based encryption and CP-ABE is to achieve fine-grained access control in cloud storage services. Barua [2] propose Efficient and Secure Patient-centric Access Control (ESPAC) scheme which permits data requesters to have various access benefits based on their roles.

Another study [4] proposed scheme smart card based e-health system which aims to secure a system by using smart card based authentication scheme. In addition, Mehndiratta [5] proposed a model for security and privacy in each reference layer, this model provides each layer security and privacy to achieve high flexibility and performance. Qian [6] proposed a model called pseudorandom function to make a privacy preserving multi authority CP-ABE scheme this model supports fine grained access control.

B. Negative Impact in Health IT security

The negative impact is on security issues in the health care system are on the data and storage on the system based environment. It's very hard to maintain and keep the data secure and ensure availability at any time. So, significant progress growth has been made in health service, but concern over service integration of sensitive medical information still require to focused [3]. In addition, Cloud storage can be vulnerable while storing large amount PHI in the sense as in it is in the hands of an outsider [7]. Moreover, Privacy of the patient having proper access control in cloud storage is a

ISBN: 978-1-4673-7503-0 ©2016 IEEE

rising fear in e-health care system because of involvement of human nature. Furthermore, security issue such as system lacking patient-centric access control is one of the major issue in HIT security ,Patient privacy is also the challenge in HIT security because in all level of communication, System cannot provide patient privacy and furthermore collision resident and efficiency are the issues that make system HIT security unsecured [8].

C. Positive Impact on Health IT security

Security in health care maximizes the health care quality and minimizes the health care cost. In our proposal, we have proposed a framework that provides security for health care and as well as privacy and performance in health care system [9]. Health IT security helps in securing Personal Health Information (PHI) at cloud and helps in mitigating the risk. Moreover, managing firewalls and other critical network resources helps in preventing from unauthorized access which helps in getting positive impact on HIT [10]. In addition, monitoring of data leakage and handling of security incidents helps in achieving positive impact on HIT [11]. Our proposal focuses on securing health care from attacks by unauthorized users and also identifies the threats and vulnerabilities in health care. The data that contains information are confidential and the integrity is preserved in HIT Barua [2] .

III. Current e-Health Framework

Figure 1 shows the Patient and Health service provider shared the key having public and private key. Patient sends encrypted information with digital signature to the health service provider. After receiving the message from the patient, Health Service provider decrypt the message and ensure by validating the signature, if it is verified then health service provider encrypt personal health information according to patient defined policy. After the transmission of personal health information to health service provider, PHI is stored at cloud. To get access to sensitive information data access requester sends access request to cloud service provider and then health service provider executes the access request Barua [2] .The current selected solution has different features. It ensures patient identity privacy, make sure PHI integrity and source authentication, simply revoke malicious user, resistant to collusion attack, and patient-centric access control. This solution has also some limitation. Collision resistant cannot completely be elevated in this encryption method. Fine gained access control is average in the CP-ABE method. Efficiency in this framework is not scalable. And Average authentication and authorization is the last limitation [1].

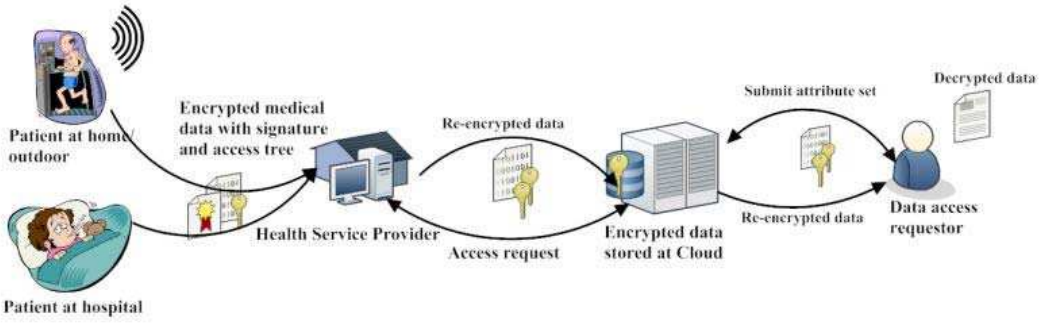


Fig. 1 Current Framework of Health IT security

IV. Proposed Mobile Cloud Framework in BFL

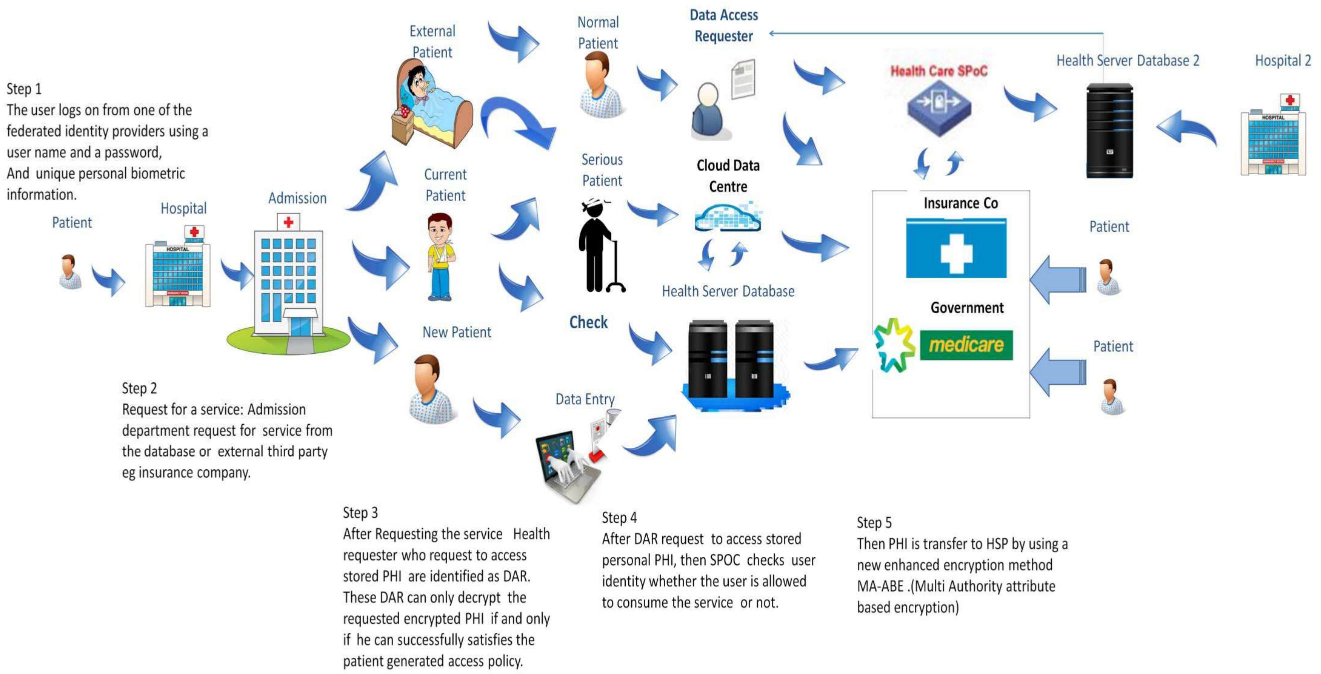
The proposed e-health care framework that is presented in figure 1 and the security process of it in figure 2. In this framework, firstly, the user logs on by using username, password and by providing unique biometric information to secure user identity. Secondly, Request for Service is generated by the admission department to get request from the database and external third parties. For instance, cloud computing. Thirdly, after administrator request for the service, health requester who asks for access to stored personal health information is known as Data Access Requester (DAR). If patient generate access policy satisfies, then only DAR can decrypt the encrypted Personal Health Information (PHI). Fourthly, after requesting to access the PHI , then Single point of contact checks whether the user is allowed to access the service or not. If the user gets allowed to access the service, administrator can easily access the patient coming from external hospital or referred by doctor. Then Personal Health Information is transfer to Health Service by using a new proposed framework MA-ABE (Multi Authority Attribute based encryption). In our current framework , the encryption technique CP-ABE(cipher policy Attribute based encryption)that were used to secure e-health system is average as new enhanced encryption technique can be used to overcome this technique which provides fined grained access control with excellent as compared to CP-ABE. In addition, its efficiency is scalable as compared to current solution and is collision resistant [1].

The proposed framework has different features as the following:

- Fined grained access control
- Patient centric access control

ISBN: 978-1-4673-7503-0 ©2016 IEEE

- Patient privacy
- Scalable efficiency
- Collision resistant elevated
- Single point of contact for more authentication and authorization.
- Prevents from Vulnerability and Threats



Step 1
The user logs on from one of the federated identity providers using a user name and a password,
And unique personal biometric information.

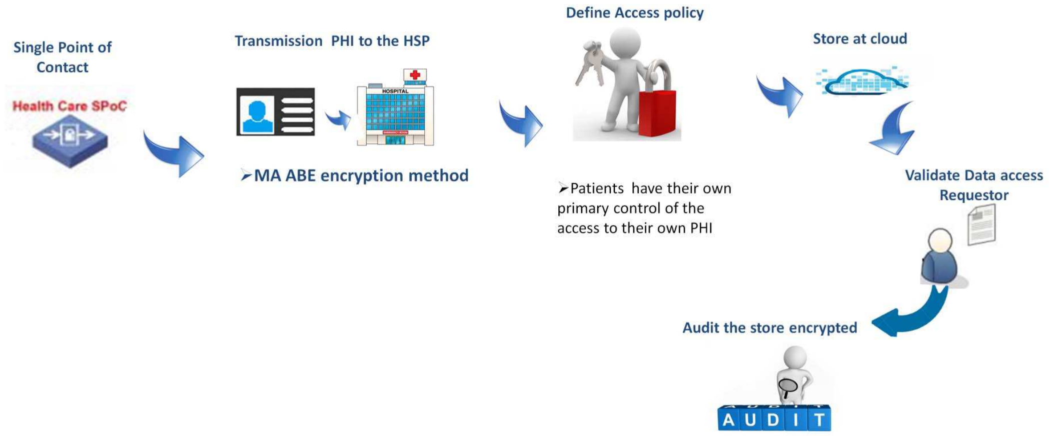
Step 2
Request for a service: Admission department request for service from the database or external third party eg insurance company.

Step 3
After Requesting the service Health requester who request to access stored PHI are identified as DAR. These DAR can only decrypt the requested encrypted PHI if and only if he can successfully satisfies the patient generated access policy.

Step 4
After DAR request to access stored personal PHI, then SPOC checks user identity whether the user is allowed to consume the service or not.

Step 5
Then PHI is transfer to HSP by using a new enhanced encryption method MA-ABE .(Multi Authority attribute based encryption)

Fig. 2 Proposed a Secure Framework for e-Health



Single Point of Contact
Health Care SPoC
Transmission PHI to the HSP
➢MA ABE encryption method
Define Access policy
➢Patients have their own primary control of the access to their own PHI
Store at cloud
Validate Data access Requestor
Audit the store encrypted
AUDIT

Fig. 3 Secure Process of the Proposed Framework

V. METHODOLOGY

It is a mixed method that combines a qualitative with a quantitative approach. In addition, we require for both method to discover the feature of Health IT security and to address the challenges faced in Health care IT system. This method provides a means to discover the impacts by high reliability as well as validity. Therefore, Conducting both methodology gives quality and the authenticity of the study.

A. Participants

The study was led through online survey taking into consideration distinctive respondents statistics that incorporates security, privacy and user satisfaction. 26 of the respondents are from Doctors and 25 from the IT support group.

B. Questionnaire design and Measurement Scale

Two different types of questionnaires were sent to the Doctor's and IT support. The survey questions were organized and find the impact of Doctor’s and IT support perception in security, privacy, user satisfaction and so on. Two parts of questionnaire were send via online to the Doctor's and IT support. First parts include demographic of the participants and second parts include participant’s response on the question working on Health system based on security, privacy, Threats. The perception of the survey questionnaire in Health IT Care System is to identify the threats, Vulnerability, privacy of the patient data and number of security breaches in every year.

C. Data Analysis

Evaluation and research are done by analyzing the health care security and the various methods collected in literature review. All the related and important articles, journals research papers and online resources for studying are implemented in this research. Gathering all these materials and information examined on literature review and answering all the questions which are mentioned in the purpose and aims. After working on literature review, information gathered were observed to bring good perspective and survey questionnaire were conducted for enhancing better framework which helps in enhancing security and privacy. The quantitative method was used to collect the data from number of respondents and analyzed through use of Statistical Package for the Social Sciences (SPSS) software.

VI. Results of Analysis

A. Correlations

Correlation for Doctor's perspective based on security, privacy, user satisfaction, Vulnerability and Threats are analyzed for showing the dependency of variable to each other. The correlation are measured from Doctor's perception (N= Doctor's total number) of Health system on Security, Privacy, User Satisfaction, Threats and Vulnerabilities.

From Table 5 "Security" is strongly correlated to "Privacy"(r=.530**) where p<0.01.From this analysis, we find that, on increase in security will strongly increase in user satisfaction or vice versa. Furthermore, " Security" is positively correlated to "vulnerability"(r= -.369) and" Threat"(r= -.134) which is correlated with each other. In addition, there is a weak relation between "Security" and "Privacy"(r=.158) as increase in security does not highly effect to privacy as it should be increase. So, it has less significant effect on privacy or vice versa.

VII. Discussion

The goal of this research is to make secure system in Health care where the main priority is security of patient health information. To secure health care from attacks by unauthorized users, a new enhanced framework has been proposed called MA-ABE encryption technique. This technique helps in achieving fine grained access control, in addition, using MA-ABE enhances system scalability. In addition, outsiders attack like Man-in-middle attack, eavesdropping, denial of service(DOS) attack are managed efficiently in this encryption technique. After doing analysis through SPSS, there is a positive impact as well as negative impact. In negative impact, we have encountered that there is a weak relationship between privacy, for instance, administrator can access patient information for stealing data. So, to overcome this, administrator can only access the patient information by patient consent or by doctor consent. There is also weak relation in cloud computing, as it is third party so any one can access the data .So, while storing data in the cloud, Advance Encryption Standard is used in enhanced proposed work. AES is the latest encryption technique which improves the privacy and security of Personal Health Information. Therefore, we have used Multi Authority Attribute Based Encryption (MA-ABE) techniques for securing PHR data with Advance encryption standard(AES) and explore how SPOC(single point of contact) helps in getting benefit in Health IT(HIT) security.

VIII. Conclusion and Recommendations

Security in health care should maximize the health care quality and minimize the health care cost. In our research, we have proposed a framework that provides security for health care. Our research focuses on securing health care from attacks by unauthorized users and also identifies the threats and vulnerabilities in health care. It highlights the approach and technique that are equally used in security Health IT and also reflect cyber security threats. In this research, we conducted a survey on Health IT security based on security, privacy and performance. This proposed research describe in securing health records in the efficient and scalable by using Multi Authority Attribute Based Encryption (MA-ABE) techniques for securing PHR data with Advance encryption standard(AES) and explore how SPOC(single point of contact) helps in getting benefit in HIT(Health IT) security.

Table I Correlations based on Doctor satisfaction by security, privacy, Threats and Vulnerability of E-health System

		Security	Privacy	User Satisfaction	Vulnerability	Threat
Security	Pearson Correlation	1	.158	.530**	-.369	-.134
	Sig. (2-tailed)		.431	.004	.059	.505
	N	27	27	27	27	27
Privacy	Pearson Correlation	.158	1	.042	.438*	-.209
	Sig. (2-tailed)	.431		.835	.022	.296
	N	27	27	27	27	27
User Satisfaction	Pearson Correlation	.530**	.042	1	-.225	-.270
	Sig. (2-tailed)	.004	.835		.260	.173
	N	27	27	27	27	27
Vulnerability	Pearson Correlation	-.369	.438*	-.225	1	.030
	Sig. (2-tailed)	.059	.022	.260		.880
	N	27	27	27	27	27
Threat	Pearson Correlation	-.134	-.209	-.270	.030	1
	Sig. (2-tailed)	.505	.296	.173	.880	
	N	27	27	27	27	27
**. Correlation is significant at the 0.01 level (2-tailed).						
*. Correlation is significant at the 0.05 level (2-tailed).						

References

[1] A. Samydurai, K. Revathi , P. Prema, D. Arulmozhiarasi, J. Jency, & S. Hemapriya, "Secured Health Care Information exchange on cloud using attribute based encryption," *3rd International* of *Communication and Networking (ICSCN)* , pp. 1-5, 2015.

[2] L. Barua, & Shen, "Secure Personal Health Information Sharing," *Symposium* of *Communication and Information System Security,* pp. 201-205, 2013.

[3] L. Fan, W. Buchanan, C. Thummler, O. Lo, A. Khedim, & O. Uthmani, "DACAR Platform for eHealth Services Cloud," *in IEEE International Conference on Cloud Computing (CLOUD).* , pp.219-226, 2011.

[4] K. Yeh, - N. Lo , T. Wu, T. Yang, & H. Liaw, "Analysis of an eHealth Care System with Smart Card Based Authentication, " *in Information Security (Asia JCIS)* , 59-61, 2012.

[5] P. Mehndiratta, " A Model of Privacy and Security for Electronic Health Records," A Model of Privacy and Security for Electronic Health Records," *In Bhalla Springer International Conference*, pp. 202-213, 2014.

[6] H. Qian, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," *International Journal of Information Security* , pp. 487-497, 2015.

[7] N. Thiranant, M. Sain, L. Hoon , "A design of security framework for data privacy in e-health system using web service," 16th *International Conference on Advanced Communication Technology (ICACT),* pp.40-43, 2014

[8] S. Satheesh, D. Sangeetha, V. Vaidehi, , "EPSSHIC-enabling privacy and security of smart health care system in cloud," *International Conference on Recent Trends in Information Technology (ICRTIT),* pp.79-83, 2013

[9] H. Abie & I. Balasingham, "Risk-based a daptive security for smart ToTin eHealth," *7th International Conference on Body Area Networks*, P. 269-275, 2012.

[10] A. Lounis, A. Hadjidj, A. Bouabdallah, & Y. Challal, "Secure and Scalable Cloud-Based Architecture for e-Health Wireless Sensor Networks," *21st International Conference on Computer Communications and Networks (ICCCN),* pp.1-7, 2012.

[11] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, & G. Muller, "Aspects of Privacy for electronic Health Records", International Jornal of Medical Informatics, 80(2), e26-e31, 2011.