2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)

An Access Control Framework for Protecting Personal Electronic Health Records

Ambrose Atuheire Izaara[1], Richard Ssembatya[2] and Fed Kaggwa[1]
[1] Faculty of Computing and Informatics, Mbarara University of Science and Technology
[2] Faculty of Science and Technology, Uganda Christian University

Abstract - The increasing development of wireless networks and the widespread popularity and usage of handheld devices such as mobile phones and wireless tablets represents an incredible opportunity to enable mobile devices as a universal health data access tools. Unfortunately, some issues hampering the widespread acceptance of mhealth such as accountability properties, privacy protection, limitation of wireless network and mobile device. Challenges such as unreliable data repositories and limited connection speeds in resource limited environments are evident. Recently, many public-key cryptography based mobile health data access protocols have been proposed. However, limited capabilities of mobile devices and wireless networks make these protocols unsuitable for mobile network. Moreover, these protocols were designed to preserve traditional flow of health data, which is vulnerable to attack and increase the user's risk. In this paper, the researchers build on existing concepts of *MEDical* Information Systems and use of Symmetric Key Infrastructure to design a framework for secure access to personal electronic health records. The framework not only minimizes the computational operations and communication passes between the engaging parties, but also achieves complete privacy protection for the user. Validation results from ICT experts demonstrate that the designed framework is applicable for secure access to personal medical health records in resource limited settings.

Key Terms: – mhealth, mobile device, Security, framework, Mobile Network Operator.

I. INTRODUCTION

The last century has produced a proliferation of innovations in the health care industry aimed at enhancing life expectancy, quality of life, diagnostic and treatment options, as well as the efficiency and cost effectiveness of the healthcare system [1]. Opportunities of using mobile technology have improved in the last few years with the growing population of smart phones in Uganda [2]. A combination of wireless mobile technology and medical health innovation can revolutionarise the use of medical technologies to improve service delivery in the health sector. Personal Health record (PHR) systems play an important role in improving the efficiency of healthcare service delivery by enabling patients monitoring, control and providing health information to healthcare givers. [3], [4]. Despite the many benefits of having PHR systems, the development of appropriate and scalable Personal Health Record systems in developing countries has proved difficult due to limitations that are inherent to the technological and social issues [3]. As such, the majority of current PHR practices in developing countries are primarily paper-based [3]. Paper-based PHR systems are prone to loss and unavailability of patient information, delays in accessing the information and space limitations for record-keeping [3]. Similarly, due to limited resources, such as intermittent power and Internet connectivity, computerizing these processes securely is challenging.

Furthermore, literature reveals a number of studies demonstrating that PHR systems implemented in developing countries do not adequately protect patients' records [5], [3]. These findings were also in agreement with our study conducted at Mbarara University Teaching Hospital (Uganda). Most of the hospital employees including doctors, nurses, lab technicians and messengers have access to all the personal health records for all the patients. This demonstrates that there is no role-based access control hierarchy implemented at the hospital, and therefore no mechanism of controlling authorizations of data access. Patients expressed fear of their health data confidentiality and showed a need to access their health data using personal mobile devices.

Motivation and Problem Statement

There has been an increase in the proliferation of mobile-phone use in developing countries [6], [3], and user demands for more patient controlled access to healthcare data [16], [6,] [5]. Additionally, the growth of wireless infrastructure in developing countries have increased demand for mobile PHR systems [16], [6].

While mobile phones and the increasing availability of wireless infrastructure can support and improve patients' access to their personal Health Records, they generally do not provide sufficient security mechanism for adequately protecting personal data from unauthorized disclosure, especially when patient's data is stored on the mobile device [3]. This is mainly due to the architectural shortcomings of their design [18]. The limited processing and memory capabilities of the mobile phones to support the security architectures is still a challenging problem. When personal data is downloaded and stored on mobile phones, it remains unprotected and potentially accessible by unauthorized users. Therefore, an access control framework that securely protects mobile phone-based PHR is needed to facilitate secure sharing of Personal Health records.

Contributions

In this paper, we propose an access control framework that protects personal health data in transit between a federated Data server and a mobile phone. The study was based on the findings from the contextual study covering four months of fieldwork with patients and healthcare givers at Mbarara University Teaching Hospital. The framework makes use of public key infrastructure, privilege management infrastructure, SSL and web service security and pluggable XML based access control policies to protect PHRs from unauthorized access.

Outline

The rest of the paper is structured as follows. In Section 2, we discuss related work on PHR systems in general and the security of these systems. Section 3 presents our proposed access control framework that supports protection and sharing of Personal Health Records. Section 4 discusses the strengths of the designed framework and finally section 5 concludes the research.

II. RELATED WORK

Personal Health Records (PHRs)

In the current century, a new development of Personal Health Records (PHRs) has evolved from EHRs. PHRs allow patients to add and annotate their own health records [3]. Unlike EHRs where providers control who adds or views patients' records, PHRs empower patients to become the custodians, and have full control of their health records.

The literature reveals two categories of PHRs. Paper-based PHR and electronic PHR. Paper-based PHRs are generally less portable between healthcare givers and in many cases, the cost of physically transporting the records is burdensome [21]. Additionally, according to the medical record standards, patient records should be kept for a certain number of years, and should be available at all times in order to support continuity of patient care [11]. Thus, keeping paper-based records for certain number of years incurs overwhelming storage costs, in addition to difficulty in interpretation of standard medical jargon, and abbreviations of medical terms. The outcome is usually shortcomings in documentation in terms of accuracy, availability and legibility [12].

One way to overcome such shortcomings is to make use of Electronic Personal Health Records (PHRs). An electronic PHR is initiated by gathering health information of an individual from a single, or multiple sources such that information can be shared via the Internet with the authorised healthcare professional (s) [3].

A number of PHR systems have emerged that provide patients with secure access to manage their health information. However, studies reveal that there is no standard framework for PHR [13], [3]. In the patient-centric PHR model, patients control their entire PHR via web portals or portable computing devices such as mobile phones in order to import, read and update their records.

Mobile phone-based PHR systems, due to their offline nature provide patients with a mechanism to communicate with their healthcare givers when the hospital servers are offline, in addition to the provision of up-to date health records [3], [6], [16]. This makes a mobile phone-based PHR more valuable in healthcare delivery [3].

PHR Authentication Frameworks

A. The NIST Model for role Based Access Control

RBAC has four elements: users, roles, permissions and sessions; NIST RBAC elaborates permissions by introducing operations and objects sub entities [14]. In flat RBAC, users are assigned to roles, permissions are assigned to roles so users inherit permissions from being members of these roles. RBAC has default rights for users based on their roles. This implies that a doctor for example inherits rights that the doctors' role is defined. This access approach by itself does not satisfy requirements for HIPAA. Therefore, basing on the framework that shall be designed, this approach will not be favourable as every patient needs to have only one role towards his data and a doctor who inherits another doctor's role may compromise the confidentiality of a patient.

B. Multi-Level Security Framework

MLS defines that every data has a classification and every user possesses a clearance. The security levels are unclassified, confidential, secret and top secret which are hierarchical. Multi-level security leverages on Bell La Padula security model [6]. Based on the Bell La Padula model, MLS permits users or processes to read only information classified at only or below their clearance. The fact that MLS is based on classification of information and clearance of the users prior to authorization limits its use in situations where the information sharing parties do not have prior knowledge of each other. In cases where a user is visiting a new medical practitioner, this would be very limiting hence not favourable.

C. PKI-based Access control framework

Public Key Infrastructure is a security architecture that uses the concept of a trusted third party to ensure confidentiality, integrity, non-repudiation and accountability during information sharing [16]. Public Key Infrastructure is based on asymmetric cryptography where a pair of keys; public and private keys are used. What one key encrypts, only the other

key can decrypt. The public key is published to the public while the private key is kept secret by a user. A sender uses the receiver's public key to encrypt data that can only be decrypted by using the receiver's private key. This provides for data confidentiality. Public Key Infrastructure operations are very resource intensive and pose a challenge in resource limited environments. Therefore, with the environment for the proposed architecture to function well, PKI will not suit best.

D. Attribute Based Access Control (ABAC)

Similar to the above approach, the attribute based access control uses attribute certificates only that these certificates do not contain a public key [17]. An attribute certificate contains the account holder's specific attributes similar to policies that specify his or her access control information such as role, security clearance or group membership [17]. ABAC is effective at authorization of users from different security domains using a trusted third party even in environments where the parties do not have any prior knowledge of each other. ABAC does not use public keys and therefore does not cater for security during transmission. For the kind of data transmitted between health center and patients, the structural arrangement may not fit this approach so will not suit the proposed framework.

E. Surrogate Trust Negotiation (STN)

Trust negotiation allows two parties that are previously unknown to each other outside a local security domain to transact securely through a handshake like process of requesting and providing digital credentials and policies [18]. "Trust agents are autonomous software modules on secure, offsite computers that act as surrogates for mobile devices, performing cryptographic operations and managing credentials, policies, secret keys for use in trust negotiation." [18] STN allows resource limited devices to participate in trust negotiation using trust agents.

F. MEDIS

MEDIS is a *MEDical* Information System developed in Serbia aimed at building an integrated patient centric electronic health record right from the beginning and not integrating existing heterogeneous ones [19]. It is designed to meet international health system standards such as HL7.

MEDIS has been implemented as a federated system where the central server hosts basic electronic medical records about the patient and the distributed clinical servers contain their own part of the patient's record [19]. MEDIS combines the strengths of the previous approaches to bring forward a federated system where the records are stored where they are collected but are accessible globally. It ensures security on the network using certificates, security from the client device using applets and conforms to public standards such as HIPAA. The research builds on this existing MEDIS literature for secure sharing and accessing Personal Electronic Health records architecture.

III. PROPOSED FRAMEWORK

Although PHR systems promote the sharing of personal information between a patient and his/her healthcare provider, they also generate security and privacy issues [22] [3]. The consumer survey of PHR systems conducted by Markle Foundation working group demonstrates that ninety-one percent of the respondents are very concerned about the privacy and security of their personal health records. In the following section, we present our adversary model and then proceed to describe how our Access Control Framework operates.

Adversary Model

We define an adversary setting that determines the capabilities of possible actions of an attacker. We consider a probabilistic man in the middle attacker that has access to the communication links or the communication devices.

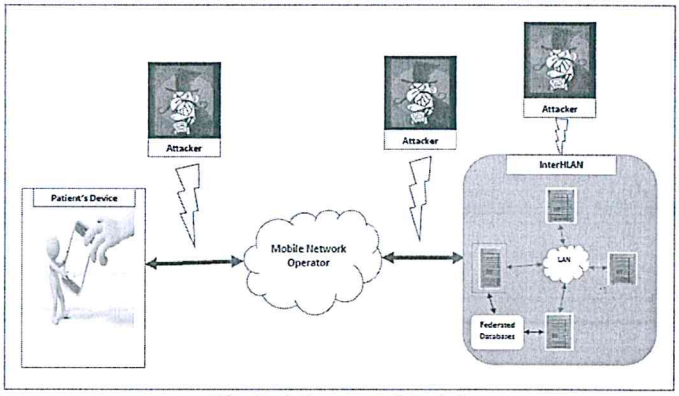

Fig 1. Adversary Model

We assume the attacker can listen to all transmitted messages or view transmitted messages on the communication device, change these EHR or inject their own generated messages. We consider that all secrete information stored on a federated database or received on a mobile device is potentially vulnerable to break-ins or other forms of leakage. However, we want to guarantee that information leaked in one specific data transaction will have minimal effect on the security of other data transactions. The patient's identity is protected by use of random generated numbers sent to the federated data server during data transaction in case of a replay attack. Use of shared session keys between the Patients device and the federated data server verses a shared session key between the Mobile network operator and InterHealth Institution Local Area (InterHLAN) Network protects patient identity from a Trusted Third-Party attack. These keys are first exchanged during the registration protocol which only takes place on the InterHLAN to protect against eavesdroppers on public Mobile Networks.

To protect the privacy of the patient and resolve the problem of data flow between the user and the data repository, the framework is designed based on a client centric model where

the Patients Data Server (P_{DS}) does not have direct communications with the Patient's MNO. The framework is composed of four parties including Patients Device, Patients Data Server, Patient's MNO, and InterHLAN. The Framework works with the assurance that secrete Xi, where i=1,...,n is only shared between Patients Device and Patient's MNO, and secrete Yi is only shared between the Patients Data Server and InterHLAN. The following symbols are used in the Framework.

TABLE I
NOTATIONS

SYMBOL	DESCRIPTION
{P_D P_{NO}, P_{DS}, InterHLAN}	A set of engaging parties which are The Patient's Device, Patient Device Network Operator, Patients Data Server and Inter Health Institutions LAN respectively.
TSC	Time Stamp Center
PN_p	SIM Number of Patients Device
PIN_p	Selected Password Identification Number for Patient
ID_p	Identity of Patient which Identifies Patient to NO; computed as $\mathbf{ID_P=PN_P + H(PN_P, PIN_P)}$
Bio_P	A set of the Patient's finger print scans to uniquely identify the Patient in emergency cases
AI_p	Account Information for Patient such as account status, age, names, address etc.
Rand	Random Number and Timestamp generated by $\mathbf{P_D}$ to protect against replay attack that ensure old communication cannot be reused in replay attack.
R	Random Number and Timestamp generated by P_{DS} to act as a $\mathbf{P_{DS}}$ Pseudo ID which uniquely identifies $\mathbf{P_{DS}}$ to **InterHLAN**.
DATE	Date of Data Retrieval
ehr	Data to be retrieved
DESC	Description of data retrieved which may include delivery address. Patient will only disclose information they wish to disclose for privacy purposes.
TID	Identification of Data Transaction Process
TID_{req}	The request for TID
PID_{req}	Request for Patient Device Identity
{D}X	Data D symmetrically encrypted with shared key X
H(D)	The one-way hash function for Data D
I	Used to Identify the current session Key of Xi and Yi
K_{p_p}	The secrete key shared between Patients Device and Inter Health Institution LAN on registration
Success/Failed	The status of registration whether success or Failed
Yes/No	The status of Data transaction whether approved or rejected
Received	Information Receivable update status, which may include the description of data received

The proposed Framework consists of two sub protocols, which are registration and data transaction protocol. Both P_D and P_{DS} are required to register with their own Network Service provider before any data transaction can take place. P_D and P_{NO} generate session key, X_i by running Diffie-Hellman Key Agreement protocol. Then P_D sends registration details such as Patient Names Phone Number and Patient Address encrypted with session key K_i to P_{NO}.

$P_D \rightarrow P_{NO}$: *{PNp, IDp, AIp}* K_1

A patient's details will be captured during first registration at a health center connected on the Inter Health Institution Local Area Network. This takes place ONLY on the InterHLAN network for accurate authentication, verification and integrity of patient data. The patient reports at the hospital or clinic reception and their initial bio data is captured by trained personnel, their health data is entered by a doctor and stored in a federated database as the first electronic health record.

During the Registration process, Patient is required to set his/her Personal Identification Number, PIN_P for later access to his/her personal Medical data. The registration process also captures a patient's biometric finger print that shall be used on the InterHLAN in emergency cases or special cases such as a patient who forgets his Password. This implementation uses two factor authentication and that is an important principle for physical and mobile devices access control [21]. The two-factor authentication applies two measures to authenticate users to access the mobile based personal health information system, that is the mobile device with the Application (something he/she has) and the Password (Something he/she knows only). Then the ID_P is computed by hashing the PN_P and PIN_P.

$ID_P = PN_P + H(PN_P\ PIN_P)$

P_{NO} decrypts data with shared session key, K_1 to retrieve patient's health information. P_{NO} stores required information into their database. If registration process is successful, P_{NO} sends confirmation message to P_D to inform Patient. The confirmation message is encrypted with the session key K_1

$P_{NO} \rightarrow P_D$:{ Success/Failed} K_1

After registration process, Patient receives a mobile API access code from P_{NO}. The application contains symmetric key generation and mhealth software. After it has been installed successfully, a set of symmetric keys $X = \{X_1, X_2.....Xn\}$ is generated and stored into P_D and sent to the P_{NO}. The P_D will also in the same process exchange a secrete key K_{P_P} with the Inter Health LAN authentication server during the registration process. Similarly, P_{DS} MUST go through similar registration process with the InterHLAN server to enable it to receive data from P_D. The P_{DS} generates a set of symmetric keys $Y = \{Y_1, Y_2....Y_n\}$ with the InterHLAN server and store them into the InterHLAN Database Server. The figure below shows the framework design. The various components of the framework are illustrated and their interaction shown.

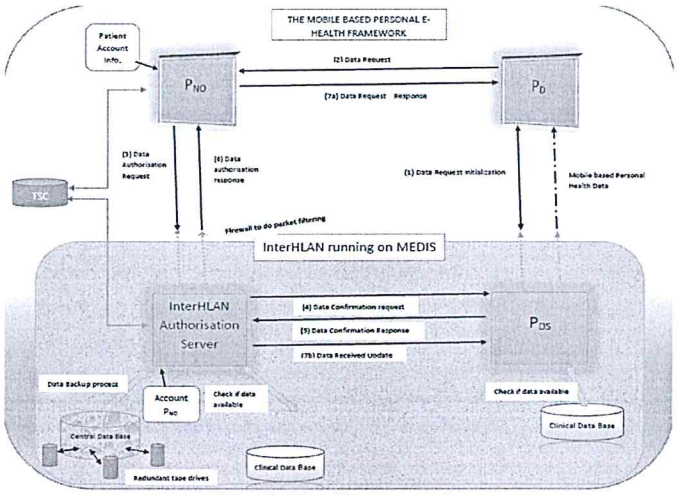

Fig. 2 The Framework

Phase 1 Data request Initialisation

PD → PDS: *R, TIDreq, PDSIDreq*

PDS → PD: *{IDP, TID, PDSID} K2*

Phase 2 Data Request:

PD → PNO: *{IDP, PDSID, R, TID, ehr, DATE, Rand, H(IDPNO, R, TID, ehr, DATE, Rand), {R, DESC }K2 }Xi, i, IDP*

PNO → TSC: *H[{PDSID, PNOID, R, TID, ehr, DATE, Rand, H(PDSID, PDSID, R, TID, ehr, DATE, Rand)}, { R, DESC } K2 }Xi, i, IDP]*

TSC → PNO: *TimeStamp1*

Phase 3 Data Authorisation Request:

PNO → InterHLAN: *R, IDP, TID, ehr, DATE, {R, DESC} K2*

Phase 4 Data Confirmation Request:

InterHLAN → PDS: *{R, TID, ehr, DATE, {R, DESC} K2, Rand, H(R, TID, ehr, DATE {R, DESC} K2, Rand) H(KP_P) }Yi, i*

Phase 5 Data Confirmation Response

PDS → InterHLAN: *{Yes/No, Rand, H(KP_P), H(R, TID, ehr, DATE, {R, DESC}K2, Rand), {Yes/No, TID, ehr, DATE}K2}Yi+1*

Phase 6 Data Authorisation Response:

InterHLAN → TSC: *H({Yes/No, Rand, H(KP_P), H(R, TID, ehr, DATE, {R, DESC}K2, Rand), {Yes/No, TID, ehr, DATE}K2}Yi+1)*

TSC → PNO: TimeStamp2

InterHLAN → PNO: *Yes/No, TID, ehr, DATE, {Yes/No, TID, ehr, DATE} K2*

Phase 7 Data Request Response:

PNO → PD: *{Yes/No, Rand, H(KP_P), H(PDSID, IDNO, R, TID, ehr, DATE, Rand){Yes/No, TID, ehr, DATE}K2}Xi+1*

InterHLAN → PDS: *{Received, Rand, H(KP_P), H(R, TID, ehr, DATE, {R, DESC}K2, Rand)}Yi+1*

Emergency Cases Data flow:

Emergency cases are considered when a patient is unconscious, mentally unable to use the application on their mobile device, involved in a case with law enforcement agencies or has succumbed to fatal injury that results in loss of life. The override to access a patients' data shall be only possible with presentation of the patients' biometric finger print which was captured during the registration protocol using Gabor filter-based multiple enrolment fingerprint recognition [23] to protect patient data integrity and privacy.

Phase One: Data request Initiation:

InterHLAN → PDS: *R, TID_{req}, $P_{DS}ID_{req}$*

PDS → InterHLAN: *{TID, ID_{NO}} K_3*

Phase 2 Data Request:

InterHLAN → PDS: *{ Bio_P, ID_{NO}, R, TID, ehr, DATE, Rand, $H(ID_{NO}$, R, TID, ehr, DATE, Rand), {R, DESC }K_3 }Yi, i*

Phase 3 Data Request Response:

PDS → InterHLAN: *{Yes/No, Rand, $H(P_{DS}ID$, ID_{NO}, ID_P, Bio_P, R, TID, ehr, DATE, Rand){Yes/No, TID, ehr, DATE}K_3}Y_{i+1}*

IV. STRENGTHS OF THE FRAMEWORK

The framework achieves a lot of strength in identity protection of the patient device (P_D) from the Patients federated data server (P_{DS}), identity protection from eavesdroppers or Man in the Middle attack, data transaction protection from eavesdroppers and transaction protection from trusted third party.

Achievement of patient's privacy protection is one of the most significant security properties of the proposed framework. The proposed framework protects patient's identity by sending a random generated number (R) to patients federated data server (P_{DS}) when requesting the transaction identity from the server

InterHLAN. R represents one-time patient's identity while transaction identity (TID) uniquely identifies Patients Device (P_D) to Federated Data Server (P_{DS}). This avoids revealing the real patient's identity (ID_P) to Patients Data Server (P_{DS}). The framework also provides transaction privacy from trusted third party (TTP) or Man in the Middle (MiM) attackers. The Data request that is sent from patient Device (PD) to patient's MNO consist the transaction details, which is $\{R, DESC\}K_2$. Note that, the data transaction details such as which data the patient wants or data from a number of visits is protected from both patient's MNO and Inter Health Institution Authentication server by encrypting it with the Patients Device (P_D) and Patients Data Server (P_{DS}) shared session key, K_2. Hence, only the corresponding Patients Data Server can decrypt and retrieve the data transaction details.

Besides that, both Data request message and Data confirmation response message are applied a hash function before sending it to Time Stamp Center (TSC). This prevents revealing of any data transaction details to TSC. To this end therefore, the proposed Framework comprehensively satisfies all privacy protection requirements for the patient.

The framework leverages on the pervasive computing concept to extend patient centered access control to resource limited environments. This concept is generic and does not meet electronic health systems requirements. The complements of certified access lists, message digests and secrete keys on the InterHLAN are integrated with pervasive computing to achieve the requirements of electronic health systems in resource limited environments.

V. CONCLUSION

This research produced an access control framework for secure access to personal medical health records using mobile technology in resource constrained environments. Future work will involve building an actual system to implement the requirements gathered in this research and implementing it in the real world.

Other information security domains such as business continuity and disaster recovery, application and system development security and physical security are outside the scope of this research but future research can look into integrating them into this framework.

This research acknowledges that some patients may not be able to use mobile devices or computers. This does not negate their rights to privacy. There is need for future research on how to enable such patients to be able to manage access to their electronic health records.

REFERENCES

[1] Varkey, P., Horne, A., & Bennet, K. E. (2008). Innovation in health care: a primer. *American Journal of Medical Quality*, *11*(5), 382-388.

[2] Uganda Communications Commission, 2000. *The Uganda Communication Act, September 2000*. Online: http://www.ucc.co.ug/ucaCap106LawsOfUganda.pdf

[3] Ssembatya, R (2014). Designing an architecture for secure sharing of personal health records: a case of developing countries. PhD thesis, University of Cape Town, Cape Town, South Africa, December, 2014.

[4] Kim, M. I., & Johnson, K. B. (2002). Personal health records evaluation of functionality and utilAity. *Journal of the American Medical Informatics Association*, *9*(2), 171-180.

[5] Ssembatya, R., & Kayem, A. V. (2015, March). Secure and Efficient Mobile Personal Health Data Sharing in Resource Constrained

[6] Boulos, M. N. K., Wheeler, S., Tavares, C., & Jones, R. (2011). How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. *Biomedical engineering online*, *10*(1), 12.

[7] Ssembatya, R., Kayem, A., & Marsden, G. (2013, January). On the challenge of adopting standard EHR systems in developing countries. In *Proceedings of the 3rd ACM Symposium on Computing for Development* (p. 11). ACM.

[8] Ssembatya, R., & Zawedde, S. (2014). Issues of Adoption: Can Health Services Designed for Developed Countries be adopted in Developing Countries?. In *INC* (pp. 115-137)

[9] Dmitrienko, A., Hadzic, Z., Löhr, H., Winandy, M., & Sadeghi, A. R. (2011). A Security Architecture for Accessing Health Records on Mobile Phones. In *HEALTHINF* (pp. 87-96).

[10] Halamka, J. D., Mandl, K. D., & Tang, P. C. (2008). Early experiences with personal health records. *Journal of the American Medical Informatics Association*, *15*(1), 1-7.

[11] Carpenter, I., Ram, M. B., Croft, G. P., & Williams, J. G. (2007). Medical records and record-keeping standards. *Clinical Medicine*, *7*(4), 196-319.

[12] Garrido, T., Jamieson, L., Zhou, Y., Wiesenthal, A., & Liang, L. (2005). Effect of electronic health records in ambulatory care: retrospective, serial, cross sectional study. *Bmj*, *198*(7491), 581.

[13] World Health Organisation (WHO) 2005. Knowledge management strategy. Geneva. [Accessed:15/09/2012], from http://www.who.int/kms/about/strategy/kms strategy.pdf

[14] Sandhu, R.; Ferraiolo, D. and Kuhn, R. (2001). The NIST Model for Role-Based Access Control: Towards a Unified Standard. *ACM Transactions on Information and System Security (TISSEC).*

[15] Bell, D.D. and La Padula L.J. (1974). Secure Computer System: Unified Exposition and Multics Interpretation.

[16] Bourka, A.; Kaliontzoglou, A. and Polemi, D. (2003). PKI-based Security of Electronic Healthcare Documents. *Proc SSGRR.*

[17] Mavridis, I.; Georgiadis, C.; Pangalos, G and Khair, M. (2001). Access Control Based on Attribute Certificates for Medical Intranet Applications. *JMIR***3**(1):e9.

[18] Vawdrey, D.K.; Sundelin, T.L.; Seamons K.E.and Knutson C.D. (2003). Trust Negotiation for Authentication and Authorization in Healthcare Information Systems. *Proc Annual International Conference of IEEE.***2**:1406-1409

[19] Snezana, S. (2007). Implementing Security in a Distributed Web-Based EHCR. *International Journal of Medical Informatics.* :491-496.

[20] Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR)*, *45*(1), 3.

[21] Panko R. R, *Corporate Computer and Network Security*, *Prentice Hall*, Upper Saddle River, New Jersey, 2004.

[22] Environments. In Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 17th International Conference on (pp. 411-416). IEEE

[23] Fred Kaggwa, J. N. (2016, April). Gabor Filter-based Multiple Enrollment Fingerprint Recognition. *International Journal of Computer Applications, 139*(7), 32-38.