An Access Control Framework for Protecting Personal Electronic Health Records

Ambrose Atuheire Izaara
Department of Information Technology, Faculty of Computing and Informatics Mbarara University of Science and Technology
Mbarara, Uganda
aturose@must.ac.ug

Richard Ssembatya
Department of Computer Science, Faculty of Science and Technology Uganda Christian University
Kampala, Uganda
richssembatya@gmail.com

Fred Kaggwa
Department of Computer Science, Faculty of Computing and Informatics Mbarara University of Science and Technology
Mbarara, Uganda
kaggwa_fred@must.ac.ug

***Abstract*—The increasing expansion of wireless systems and the extensive popularity and usage of mobile devices such as mobile phones and wireless tablets represents a great opportunity to use mobile devices as widespread health data access tools. Unfortunately, some problems impeding the general acceptance of mhealth such as privacy protection, limitation of wireless networks and handheld devices are still common. Challenges such as unreliable data repositories and limited connection speeds in resource limited environments are also evident. The inadequate capabilities of hand-held devices and wireless systems make these Public Key Cryptography based frameworks unsuitable for mobile networks. Moreover, these protocols were designed to preserve customary flow of health data, which is vulnerable to attack and increase the user's risk. This research drew its foundations from literature and theoretical review and used qualitative approaches. 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 provides identity protection for a patient from all forms of unathorised data access. The framework not only reduces the computational operations between the engaging parties, but also achieves 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.**

Keywords—mhealth, security, framework, electronic health records

I. INTRODUCTION

The healthcare industry has received an explosion in innovation in the last decade aimed at improving 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 a significant role in improving the efficiency of healthcare service delivery by enabling patients to monitor, control and provide vital information to healthcare givers. [3], [4]. Despite the many benefits of having PHR systems, the development of suitable and scalable PHR systems in emerging economies is still difficult due to limitations that are inherent to the technological and social issues [3]. As such, the mainstream of existing PHR practices in emerging economies are primarily paper-based [3]. Paper-based PHR systems are prone to loss and unavailability of patient information, delays in retrieving 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 shows a number of studies demonstrating that PHR systems implemented in emerging economies do not sufficiently protect patients' records [3], [5]. These findings were also in agreement with our study conducted at Mbarara University Teaching Hospital (Uganda). Most of the hospital personnel 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.

II. RESEARCH MOTIVATION

There is an increase in the use of hand-held devices in developing countries [3], [6], and user demands for more patient controlled access to healthcare data [5], [6,] [16]. Additionally, the growth of wireless infrastructure in developing countries has increased demand for mobile PHR systems [6], [16]. 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 mechanisms for adequately protecting personal data from unauthorized disclosure, especially when patient's data is stored on the mobile device [3]. This is mostly due to the architectural deficiencies of their design [18]. The limited processing and memory capabilities of mobile phones to support resource intensive security architectures is still a major challenge. When personal data is transacted, downloaded and stored on mobile phones, it remains prone to being accessed by unauthorized parties. Therefore, an access control framework that securely protects mobile phone-based PHR is needed to facilitate secure sharing of Personal Health records.

978-1-5386-6477-3/18/$31.00 ©2018 IEEE

Authorized licensed use limited to: Mbarara University of Science and Technology. Downloaded on April 21,2021 at 14:35:36 UTC from IEEE Xplore. Restrictions apply.

III. RELATED WORK

A. Personal Health Records (PHRs)

In the current century, trends have favored PHRs to the customary Electronic Health Records (EHRs). PHRs allow users to be fully in charge of their own health records [3]. Unlike EHRs where providers have higher control, PHRs endow users to become the overseers, and have complete control of their health records.

Literature reveals two sorts of PHRs. These are paper-based PHR and electronic PHR. Paper-based PHRs are generally hard to share between healthcare givers and in many cases costly to transport [21]. Moreover, according to the medical record ethics, patient records should be kept for a definite number of years and should be readily available in order to improve patient care [11]. Keeping paper-based records for a number of years incurs high storage costs in addition to difficulty in interpretation of standard medical terms and jargon. This could result in deficiencies in terms of accuracy, availability and legibility of the stored documents [12].

A good way to overcome such deficiencies is to adopt the use of Electronic Personal Health Records (EPHRs). An EPHR is created by gathering health information of a person from a single or multiple source such that information can be shared through electronic networks with authorized healthcare professionals [3]. EPHR systems have been developed that offer patients with safe access to manage their own health information. However, recent studies reveal that there is no standard framework for EPHR [3], [13]. In the patient-centric EPHR model, patients manage their entire EPHR through web portals or hand-held computing devices such as mobile phones in order to access, read and update their records.

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

B. National Institute of Standards and Technology (NIST) Framework 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 Health Insurance Portability and Accountability Act (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.

C. 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 present privacy challenges.

D. Public Key Infrastructure (PKI) based Access control framework

PKI 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]. PKI 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. PKI 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 would not suit best.

E. Attribute Based Access Control (ABAC)

Similar to the above approach, the ABAC 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 protect the user's privacy if data is intercepted on a network.

F. Surrogate Trust Negotiation (STN)

STN 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.

Authorized licensed use limited to: Mbarara University of Science and Technology. Downloaded on April 21,2021 at 14:35:36 UTC from IEEE Xplore. Restrictions apply.

G. Medical Information System (MEDIS)

MEDIS was developed in Serbia aiming 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 Health Level 7 (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 E-PHR.

IV. 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 [3] [22]. The consumer survey of PHR systems conducted by Markle Foundation working group found that ninety-one percent of the respondents are worried about the confidentiality of their PHR's. In the following section, an adversary model is presented and then a description on how the Framework operates is given.

A. Adversary Model

The framework design puts into consideration an adversary setting that defines the capabilities of possible actions of an attacker. Consideration of a probabilistic man in the middle attacker that has access to the communication links or the communication devices is made.

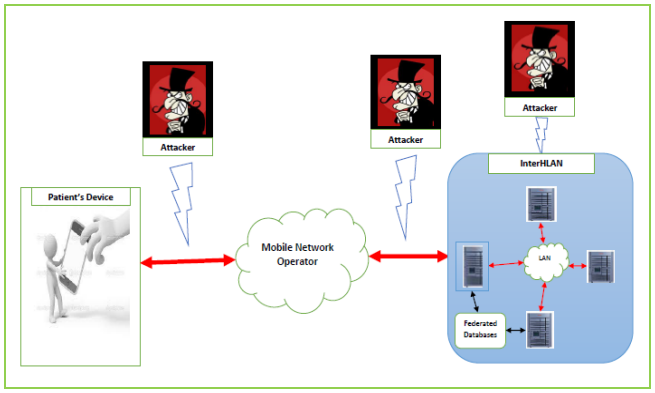


Fig. 1. Adversary Model

The attacker can listen to all transmitted messages or view transmitted messages on the communication device, change the EHR or inject their own generated messages. The Framework considers 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, the framework guarantees 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 centered on a patient centric model. The Patients Data Server (P_{DS}) does not communicate with the Patient's Mobile Network Operator (MNO) directly. The framework is composed of four parties including Patients Device, Patients Data Server, Patient's MNO, and InterHLAN. The Framework works with the assertion that secrete Xi, where i=1...,n is only shared between Patients Device and Patient's MNO, and secrete Yi is only known 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	Password Identification Number for Patient
ID_p	Identity of Patient which Identifies Patient to NO; computed as $ID_p=PN_p + H(PN_p, PIN_p)$
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 + Timestamp generated by P_D to avoid replay attack from a completed communication.
R	Random Number and Timestamp generated by P_{DS} to act as a P_{DS} ID which uniquely identifies 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

Authorized licensed use limited to: Mbarara University of Science and Technology. Downloaded on April 21,2021 at 14:35:36 UTC from IEEE Xplore. Restrictions apply.

	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

B. The Framework

The proposed Framework consists of two procedures, which are registration procedure and data transaction procedure. P_D and P_{DS} are required to register with their Network System before any data transaction can take place. P_D and P_{NO} create session key, X_i by running Diffie-Hellman Key Agreement protocol. P_D then sends registration details like 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 procedure, a 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 procedure uses two factor authentication which is an vital principle for physical and mobile devices access control [21]. The two-factor authentication applies two methods to authenticate users to access the mobile based personal health information system. It uses the mobile device with the Application (something he/she has) and the Password (Something he/she knows only). Then the ID_P is calculated 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 data. P_{NO} stores required data into their database. If registration procedure 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 $X = \{X_1, X_2 \ldots Xn\}$ 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 $Y = \{Y_1, Y_2 \ldots Y_n\}$ 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.

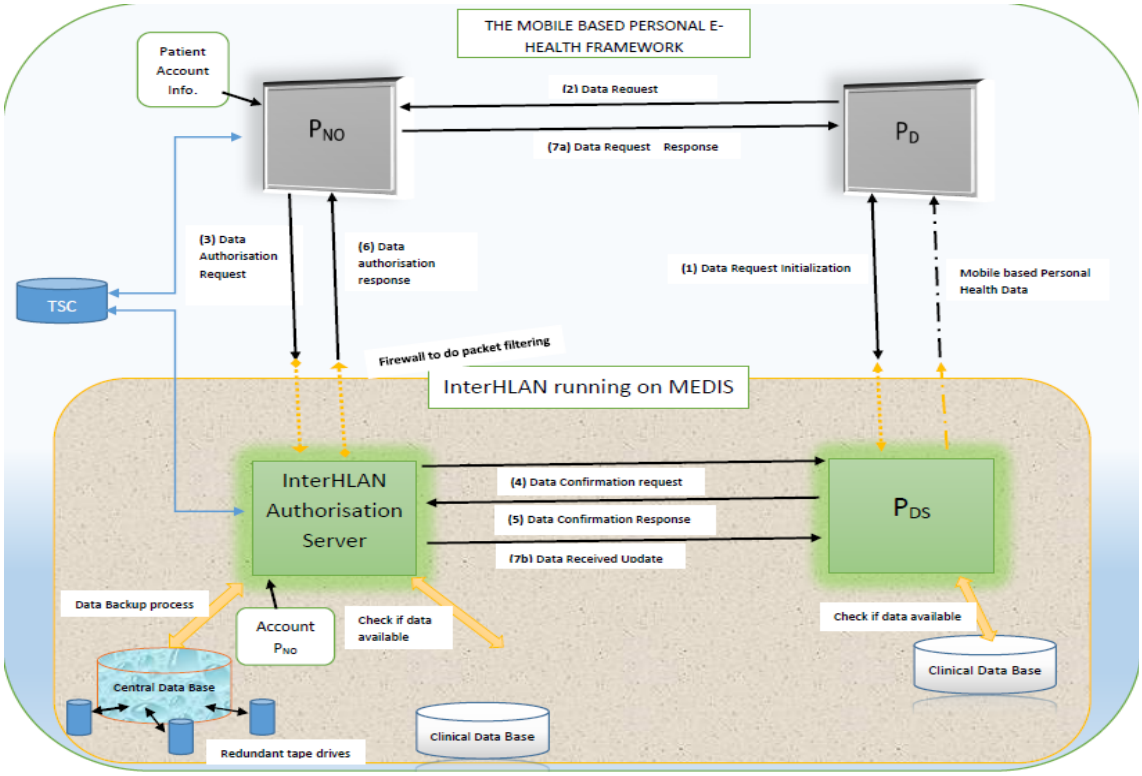


Fig. 2. The Framework

Authorized licensed use limited to: Mbarara University of Science and Technology. Downloaded on April 21,2021 at 14:35:36 UTC from IEEE Xplore. Restrictions apply.

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*

C. 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 may result in loss of life. The override to access a patients' data is made 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 [22] to protect patient data integrity and privacy.

Phase 1 Data request Initiation:
InterHLAN → P_{DS}: *R, TID_{req}, $P_{DS}ID_{req}$*
P_{DS} → InterHLAN: *{TID, ID_{NO}} K_3*

Phase 2 Data Request:
InterHLAN → P_{DS}: *{ 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:
P_{DS} → 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}*

V. 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.

Patient's privacy protection is the most significant security achievement of the designed framework. The framework protects patient's identity by sending a random generated number (R) to patients federated data server (P_{DS}) when requesting the identity from the server InterHLAN. R symbolizes one-time patient's identity while the 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.

VI. 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

Authorized licensed use limited to: Mbarara University of Science and Technology. Downloaded on April 21,2021 at 14:35:36 UTC from IEEE Xplore. Restrictions apply.

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

[2] U. C. Commission, "The Uganda Communications Commission Act," 17 September 2000. [Online]. Available: http://www.ucc.co.ug/ucaCap106LawsOfUganda.pdf. [Accessed 25 January 2017].

[3] R. Ssembatya (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, 2014.

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

[5] R. Ssembatya, A. V. Kayem, (2015, March). "Secure and Efficient Mobile Personal Health Data Sharing in Resource Constrained Environments". *In Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 17th International Conference*, 411-416.

[6] M. N. K. Boulos, S. Wheeler, C Tavares, & R. Jones (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] R. Ssembatya,, A. Kayem, & G. Marsden, (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).

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

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

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

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

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

[13] World Health Organisation (WHO). "Knowledge management strategy. Geneva", (2005) [Online]. Available: http://www.who.int/kms/about/strategy/kms strategy.pdf. [Accessed:15 August 2016].

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

[15] D. D. Bell, and L.J. La Padula (1976). "Secure Computer System: Unified Exposition and Multics Interpretation". No. MTR-2997-REV-1. MITRE CORP BEDFORD MA.

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

[17] I. Mavridis, C. Georgiadis, G. Pangalos, and M. Khair (2001). "Access Control Based on Attribute Certificates for Medical Intranet Applications". *JMIR***3**(1), 9.

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

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

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

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

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

Authorized licensed use limited to: Mbarara University of Science and Technology. Downloaded on April 21,2021 at 14:35:36 UTC from IEEE Xplore. Restrictions apply.