2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA)

Secure and Efficient Mobile Personal Health Data Sharing in Resource Constrained Environments

Richard Ssembatya and Anne V.D.M. Kayem
Department of Computer Science University of Cape Town
Rondebosch, Cape Town, South Africa 7701
Email: richssembatya@gmail.com, akayem@cs.uct.ac.za

Abstract—**Personal health record (PHR) systems are widely used in the developed world, but little has been done to explore the utility of these PHR systems in the developing world. A key reason behind this is that a lot of areas in the developing world suffer from technological impediments resulting from poor infrastructure, low literacy, intermittent power connectivity, and unstable bandwidth connectivity. In technological resource constrained environments such as these, deploying standard PHR systems is challenging and so it makes sense to redesign systems to handle the environmental limitations in ways that offer users a usable and reliable platform. Furthermore, healthcare data is inherently privacy and security sensitive so, in re-designing the PHR system the security and privacy requirements need also be taken into consideration. The idea in this case, is to opt for security mechanisms that offer the same levels of security as is the case in the standard PHR systems that are used in the developed world, but that are also lightweight in terms of performance and storage overhead. In this paper, based on the observation that mobile phone use is widely proliferated in developing countries, we propose an access control framework supported by identity-based encryption for a secure Mobile-PHR system. Results from our prototype evaluation (laboratory and field studies) indicate that the proposed IBE scheme effectively secures PHRs beyond the healthcare provider's security domain and is efficient performance-wise.**

I. Introduction

Electronic health (E-health) systems emerged to introduce the use of electronic information and communication technology in the health sector [15]. While some definitions associate E-health strictly with computers, Harrison and Lee [15] define this to broadly refer to any electronic exchange of health related information, analyzed through electronic media to improve the efficiency and effectiveness of healthcare delivery. Thus, E-health is often used to describe anything related to computers and medicine [13]. Other definitions associate E-Health strictly with the Internet, focusing on the growing importance of the Internet in health transactions.

E-Health systems play an important role in improving the efficiency and effectiveness of healthcare service delivery by enabling healthcare providers and patients to monitor, control and provide health information as well as communicate more effectively across organizational boundaries [22]. Despite the many benefits of having E-health systems, the development of appropriate and scalable Electronic Health Record (EHR) and, Personal Health Record (PHR) systems in developing countries has proved difficult due to limitations that are inherent to the technological infrastructure. As such, the majority of current healthcare services and practices in developing countries are primarily paper-based [23]. Paper-based health record systems are prone to incorrect recording of diagnoses, unavailability and loss of patient information, delays in accessing the information and space limitations for record-keeping [4], [23]. Additionally, due to resource constraints, such as intermittent power and internet connectivity, automating these processes securely and in a privacy preserving manner is challenging.

Furthermore, the E-health systems implemented in developing countries do not adequately protect patients records. For instance, in a study we conducted at the Allan Galpin Health Centre (AGHC) Uganda, we discovered that all the clinical employees including doctors, nurses, receptionists and technicians have access to all the health records for all the patients in the E-Health system. This effectively means that there is no role-based access control hierarchy implemented and so no real way of controlling data access authorizations.

A. Motivation and Problem Statement

The increased proliferation of mobile-phone use in resource constrained environments [16], user demands for more patient-controlled access to healthcare data [18], [4], and the growth in wireless infrastructure to support communications has resulted in a plethora of mobile healthcare management systems. Rashid and Elder[18] identified several reasons why mobile phones are considered important for rural healthcare. First, beyond basic connectivity, mobile phones offer benefits such as mobility to users. Secondly, the base-stations can be powered using the healthcare providers generators in places where there is no electrical grid. In addition to voice communication, mobile phones allow for the transfer and exchange of health information, which can enable physicians to remotely monitor patients health, and enable a user to manage his/her healthcare data more easily[6]. These features have made mobile phones, as opposed to standard computers, a better suited device for rural developing world regions that are characterized by technological resource constraints.

While mobile phones are flexible and cost efficient communication and storage-wise, oftentimes mobile phones do not offer mechanisms for adequately protecting healthcare data from unauthorized disclosure, when this is stored on the mobile device. The problem becomes more challenging when the device is located outside of the healthcare provider's security domain because enforcing the healthcare provider's security policies on the data becomes a challenge. Some cellular phone operating systems provide sophisticated security

mechanisms such as application-oriented access control, but the architectural constraints of standard PHR systems result in security vulnerabilities that are centered around the fact that the stored data is insufficiently protected[10], [9]. The limited processing and memory capabilities of mobile phones make supporting security architectures a challenging problem. As a result, the healthcare data downloaded and stored on mobile phones remains unprotected, and potentially accessible by unauthorized parties. Therefore, a secure and efficient architecture, that takes into account the device's as well as the environment's constraints, is need to facilitate secure data sharing on a mobile PHR platform.

B. Contributions

In this paper, we propose a secure and efficient architecture for accessing Personal Health Records (PHRs) on mobile phones. Based on a contextual study and a participatory design study, we propose an Access Control Framework (ACOF) to protect patients' records on mobile devices and that ensures that the healthcare provider's security policies are enforced beyond the healthcare provider's trust boundaries. Our ACOF uses identity based encryption (IBE) together with 128-bit Advanced Encryption Standard (AES) keys to protect PHRs from unauthorized access. We implemented and evaluated a prototype mobile health (m-health) application and discuss the results of our usability experiments (field and laboratory). Our results indicate that the ACOF offers a viable approach to providing efficient and secure storage of PHRs on mobile phones. Furthermore, we note that IBE supported mobile phone-based PHR systems can be used effectively, efficiently, and securely in resource constrained environments that are typical of developing countries.

C. Outline

The rest of the paper is structured as follows. In Section 2, we discuss related work on E-health systems in general and the security of these systems. Section 3 presents our proposed architectural design for secure health data sharing and in Section 4, we discuss results from experiments we carried out both in a laboratory setting and on the field, using our prototype M-Health system. We offer concluding remarks and avenues for future work in Section 5.

II. Related Work

According to Glocal [1], developing countries are behind developed countries in E-health services due to the failure to develop E-health roadmaps by governments, frequent power outages and unstable bandwidth connections. Electronic health records (EHRs) enable the efficient communication of medical information and thus reduce operating costs and administrative workload [20]. Modern EHRs are accessed via stable Internet connections and support efficient sharing of health records among patients and healthcare providers.

A shortcoming of EHRs is that of data portability. An EHR can lose a great deal of utility if the patient chooses to change providers or moves to a remote area with no Internet connections. In cases where the patient has no access to his/her personal health record, it becomes practically infeasible to export the data from the previous provider to the new provider [20]. Personal Health Records (PHRs) evolved from EHRs. PHRs allow patients to add and annotate their own health records, which is typically not the case with EHRs. Unlike EHRs where healthcare providers control who adds or view patients records, PHRs allow a patient access to his/her records on demand.

There are two categories of PHRs. Paper-based PHR and electronic PHR. Paper-based PHRs are generally less portable between providers and in many cases, the cost of physically transporting the records is burdensome. 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. Thus, maintaining paper-based is a time-consuming and error prone process. A number of PHRs have emerged that provide patients with secure access to manage their health information. However, studies reveals that there is no standard framework for PHR [21]. 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. The majority of patient-centric PHR systems are Internet-based.

The issue of data portability is one of the major shortcomings of EHRs, particularly in developing countries. One promising type of PHR that can address the portability problem is the device-based PHR that can easily be carried by the patient from one location to another. A device-based PHR typically consist of a mobile device such as a mobile phone, preloaded with some software intended to download and organize health information on the mobile phone. It gives patients complete control over their health records, and provides much greater opportunity for portability [20]. The device-based PHR typically provides functionalities for automatically interfacing and synchronizing with the hospital server in order to provide up-to date health records [20].

Mobile phone-based PHRs can provide patients with a mechanism to communicate with their providers when the hospital servers are offline[6]. However, as in EHR systems, a mobile phone-based PHR also raises questions pertaining to security and privacy[6]. For example, a working group sponsored by the Markle Foundation conducted a consumer survey of PHR systems, and ninety-one percent of the respondents reported that they are very concerned about the privacy and security of their personal health records.

In addition to user identification and password methods, some PHR systems implement role-based access control (RBAC) scheme to manage users access rights [24]. The RBAC scheme usually places full trust at the server in order to protect patients records. The server runs an RBAC program that verifies the requests and determines the access rights. A user with appropriate permission(s) is able to access patients records. Two of the typical examples of authentication-based PHR system include: the Indivo and PCASSO platforms [3].

Therefore, an efficient, effective, and secure framework for supporting access to PHRs is essential if PHR systems are to train widespread usage popularity. We are now ready to describe our proposed ACOF design.

III. Access Control Framework

Although PHR systems promote communication between a patient and his/her healthcare provider, PHRs also generate security and privacy issues[6]. Furthermore, a key concern of the patients in every electronic healthcare application is the issue of security and privacy. In the following we present our adversary model and the proceed to describe how our Access Control Framework (ACOF) operates.

A. Adversarial Model

We consider a traditional healthcare scenario in which patients' electronic health records (EHRs) are stored on a local server of the healthcare provider, e.g., hospital. We assume that patients (users) are equipped with mobile devices such as mobile phones on which the patients can use to download and store their Personal Health Records (PHRs). Since patients health records are originally stored at the hospital server, mobile phones communicate with the server via wireless network connections through a mobile phone-application using standard web browsers on the mobile phone. Figure 1 depicts our adversarial scenario. Since a patients health records are

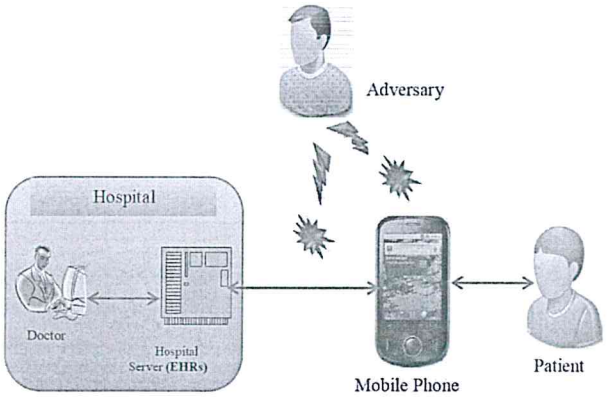

Fig. 1. Adversarial Model

inherently security and privacy sensitive, it is important to prevent unauthorized disclosure of this information. In Figure 1 we present a case in which an adversary may try to eavesdrop or manipulate patients records. In this case, the weak link in the security chain is at the mobile phone end or in the mobile phone's communication connection to the server. The adversary's goal in this situation is to gain unauthorized access the patients medical records.

B. Identity Based Encryption and Access Control

Similar to desktop-based PHR systems, mobile phone-based PHRs must provide the following functions to the user: confidentiality and integrity of data, user authentication, and none repudiation [6], [9]. We introduce an Identity-Based Encryption (IBE) inspired access control framework (ACOF) that supports secure sharing of PHRs on a mobile phone. To achieve this, the framework enables end-users to securely download and update their medical records onto the mobile phone, as well as selectively share the PHRs with the healthcare providers in an offline mode i.e. when hospital servers are offline due to unstable power connectivity and/or unreliable Internet connections. This reduces the need to rely on online access control in order to access the PHRs at the healthcare provider's end. Figure 2 presents the overall structure of the ACOF.

The ACOF is composed of four-modules that together provide secure sharing of personal health information beyond the healthcare providers security boundaries. The modules (registration module, authentication module, prescription module, and encryption module) interact with each other to ensure protection of the PHRs and secure offline access to the PHRs.

The registration module comprises a registration service that enables end-users such as healthcare providers to create an account for patients. A user receives a copy of his/her personal records on a mobile phone by registering on the registration service (RS). The RS is a web interface that captures users information such as identification number, date of birth, and email address in order to generate a personal identification number (PIN). The registered PIN is the corresponding identification information for each user. We use the Secure Socket Layer (SSL) protocol, for the submission of users information to the server. The information is encrypted with a private key that is generated based on the user's credentials and is protected using the user's PIN.

After signing up to the server, the registration service updates the list of the registered users with the new users credentials. A user listed with the RS can download and view the that handles calculating users private keys. A registered user can send a private key request to the TA in order to receive his/her private key. For security reasons, the transmitted key is encrypted using an IBE scheme. Besides, TA issues private keys after requesting the list of users IDs and the corresponding selection of system parameters.

The authentication module was designed on the assumption that the trust authority service is running on a secure and protected healthcare provider's server, accessible only by the authorized hospital administrators. This can be achieved by configuring the hospital server with the anti-virus software and a local firewall, which prevent illegitimate traffic traveling from the Internet to the hospital server.

When a new or modified record is submitted for storage to the hospital sever, the prescription module transfers the records to the encryption module where sensitive portions are selected for encryption with a 128-bit AES session key. For efficiency purposes, we use a standard hybrid approach where records are encrypted using a 128 bit AES session key and the session key is protected using an IBE scheme. The protected session key is then transferred to patients mobile phone. Once records have been encrypted, the encrypted records can then be stored at the hospital own server and/or exported to the patients mobile phone along with metadata, which includes the encrypted symmetric key and the associated disclosure policies. The hash value derived from these policies is encrypted along with the session key for an integrity check. The ACOF offers a form of public key encryption where the corresponding private keys are generated by the key server. The key server or the Trusted Authority (TA) uses the patients credentials (originally submitted to the RS) to generate the private key. For security reasons, private key is then used to protect the session key before it is delivered onto the patients mobile phone.

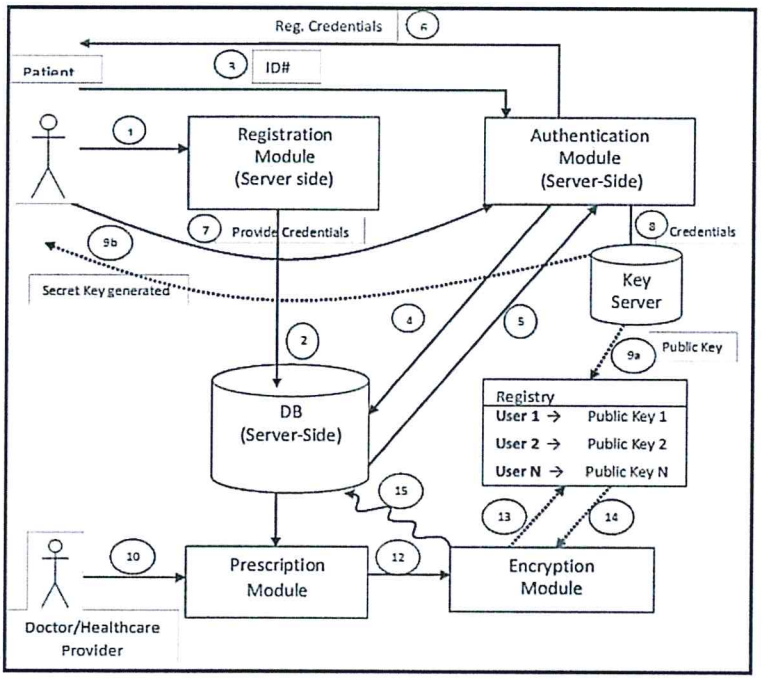

Fig. 2. Access Control Framework supported by Identity Based Encryption

To enable mobile access, the M-Health App system incorporates the push model where the healthcare provider's server takes the initiative to push the modified records to the intended patient, either on a regular basis via schedule or asynchronously by sending an update notification. Once the updated and encrypted records are downloaded to the mobile phone, the M-Health App then breaks down the records into an XML hierarchical structure such that records can be viewed/shared selectively. However, only users with a personal identification number (PIN) that satisfies the authorization policies are able to decrypt PHRs. Users are authenticated via a PIN in order to retrieve and download the encrypted records from the healthcare provider's server to the mobile phone. The M-Health App then uses an IBE private key stored in the registry to decrypt the records in order to support offline access.

The security model of our framework combines the theoretically proven Password-Based Key Derivation Function 2 (PBKDF2) that is based on the one that Kaliski[14]proposed, and Identity-Based Encryption scheme proposed by Shamir [25]. The PBKDF2 is a key derivation algorithm that was shown to be secure, and is part of the Rivest, Shamir and Adleman[19] laboratories and Public-Key Cryptography Standards (PKCS) series[14]. The PBKDF2 scheme was designed to provide users communicating over an unreliable channel with a secure session key even when the password or PIN is drawn from a small set of values [2]. The scheme applies a one way hash function to the input along with a cryptographic salt value to produce a derived key or private key (DK), which is used as the session key (sk) in our ACOF.

In order to store the DK securely on the mobile device, the user will on receiving the key from the key server, encrypt the DK using his/her PIN as follows:

$$DK \rightarrow_{Encrypt} E_{PIN}(DK)$$

The key server on the other hand will also encrypt the patients data with the session key (sk) as follows:

$$Data \rightarrow_{Encrypt} E_{sk}(Data)$$

One copy of the data is placed on the server while another is transferred to the patients mobile device. In order to access the data on the mobile device, a patient must first access his/her DK. This is done by requiring the patient to use his/her PIN to decrypt the DK as follows:

$$D_{PIN}(DK) \rightarrow_{PIN} (DK)$$

The session key (sk) is then obtained by using

$$sk \leftarrow Hash_{SHA\text{-}1}(DK,PRN)$$

where PRN is a pseudo-random number generated from a combination of the user's PIN number and in addition to some of the user's personal identification information. The sk is then used to decrypt the data as follows:

$$E_{sk}(Data) \rightarrow_{sk} Data$$

The security model of our framework rests on the security of the RSA scheme, which is a public/private key scheme based on the presumed difficulty of factoring large integers[19]. Additionally, for efficiency reasons, we do not use the IBE scheme to directly encrypt the record data. Instead, we use an AES key wherein each data object is encrypted using an AES session key that is derived from the users PIN using PBKDF2 algorithm, and the session key is protected using the IBE mechanism as described by Boneh and Franklin, and Cock[26], [8].

IV. System Implementation and Experimental Results

Our aim was to develop a user-friendly PHR system that protects and securely shares patients records on mobile phones using IBE infrastructure. To achieve this goal, we used an IBE library that supports Elliptic Curve Cryptographic (ECC) operations and bilinear pairing functions [27]. The IBE library implemented in our system is jpair. An advantage of using jpair library is that it was implemented using Java, and has no dependencies on external libraries. Four laboratory evaluation

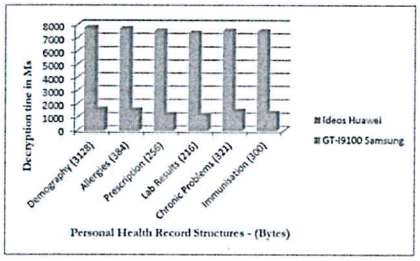

Fig. 3. Download Times per Record

sessions that included computational performance evaluation, Heuristic Evaluation, user experience evaluation and focus group evaluation were conducted in a controlled, laboratory setting to obtain feedback from users on the acceptability and functionality of the M-Health App system. For the first laboratory evaluation sessions, several experiments were conducted. First, we measured the efficiency (download time) required to download the records from the server to the mobile phone using four different 3G cellular networks in Uganda, as well as decryption performance on the mobile phone. To show that our architecture induce acceptable costs in terms of records storage, we also measured the cipher-text size overhead incurred by our encryption architecture. Our aim was to establish whether the M-Health App system can be usable on mobile phones. In order to better evaluate the performance of

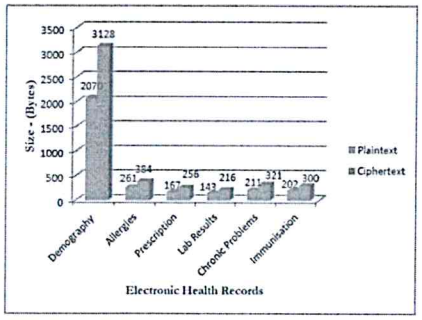

Fig. 4. Storage Overhead Created Due to Data Encryption

our crypto-based PHR system distributed on mobile devices, we measured the efficiency of IBE decryption on a mobile phone. We used a Huawei IDEOS phone, running Android OS, with 256MB of RAM and GT-I9100 Samsung, running Android OS with 1GB of RAM. Our motive was to show the abilities of different platforms. The IDEOS phones in particular were chosen as they were designed specifically for developing countries. We conducted this experiment using a small set of medical records that contained a representation of the PHRs from Allan Galpin Health Centre (AGHC). The records include demographic information, allergies, prescription, laboratory results, chronic problems and immunization. Figure 3 summarizes the measurements conducted on the two mobile devices. The x-axis represents the structure of PHRS (bytes) and y-axis shows the time required for decryption. The

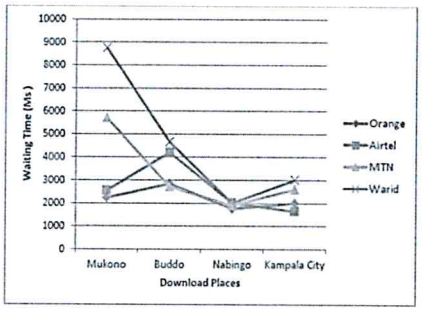

Fig. 5. Download Times between 8:30-11:30am

results from Figure 3 demonstrate that the average decryption time of Huawei IDEOS mobile phone is 7.5 seconds while the average decryption time for GT-I9100 is 1.4 seconds. The difference in decryption time is attributed to many factors including processor and memory capabilities[9]. Comparing the decryption time of PHRs on the two devices and the recommended waiting time [17], the decryption time of PHRs on the two platforms is acceptable performance-wise. While, our results indicate that the encrypted records vary in size we found no direct relationship between the records size and time taken to decrypt the records.

To determine the storage overhead incurred by our architecture, we conducted an experiment from a set of health records obtained from the Allan Galpin Health Centre. The records contained a representative of medical documents that includes demographic information, allergies, prescriptions, laboratory results, chronic problems and immunization. The size (in bytes) of each portion of the records described include: demography (2070), allergies (261), prescriptions (167), laboratory results (143), chronic problems (211) and immunization (202). To measure the storage overhead, we wrote a Java application that calculates the actual content/record size. Figure 4 describes our results. We note that the storage overhead of our architecture increased from 3054B to 4605B which is reasonable. According to Nielsen [17], download performance/speed

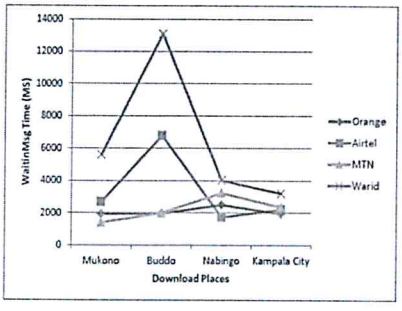

Fig. 6. Download Times between 12:30-16:00pm

is the single-most important design criterion on the Web. End-users are constantly demanding faster content downloads. The download time is affected by a number of factors: the performance of the browser, the speed of the Internet connection, the local network traffic, the load on the remote host, and the structure and format of the content requested (Nah, 2004). In this study, we are not addressing the issue of how these factors can be balanced to produce an acceptable download time but rather, we are interested in finding out whether our PHR system generates tolerable download time described by Nielsen, and, Hoxmeier and DiCesare [17], [12].

We measured the efficiency (download time) of downloading the records from the server to the mobile phone using 3G cellular networks and WLAN 802.11. Our experiments were done with Huawei IDEOS phone, running Android OS, with 256MB of RAM. The size of the encrypted records stored on MySQL database varied from 216 Bytes to 3128 Bytes. The mobile phone was connected via 3G cellular networks to the Internet and the download time measured. Figures 5, 6, and 7 describe a summary of our results. The mobile phone was also connected via WLAN, connected via ADSL connection to the Internet. Time taken to download the records from the server to the mobile phone was recorded and saved to the server.

Figures 5, 6 and 7 presents the average waiting time of a two-week experiment in which personal health records were downloaded from different places, at the same times, using the four 3G mobile networks in Uganda (MTN, Orange, Warid and Airtel). Although Uganda has more 3G mobile networks, the four were preferred because of the low barrier for setting up Internet access services on mobile phones. Three experiments were conducted each day at the same time in four different places: Kampala city, Mukono, Buddo and Nsangi and at different intervals: 8:30-11:30am, 12:30-4:00pm and 4:30-8:30pm. The differences in intervals were due to the fact that we wanted to establish the best time interval or range for patients to download their records efficiently. Figures 5, 6 and

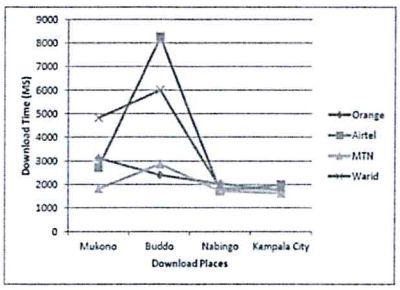

Fig. 7. Download Times between 16.30-20:30pm

7 show the distribution of time taken to download the records from the server to a mobile phone using 3G cellular networks (MTN, Orange, Warid and Airtel) in Uganda. The vertical axis represents the time taken to download the records and the horizontal axis represents the structured personal health records. As shown in Figures 5, 6 and 7, the average waiting/download time of personal health records of sizes (in bytes) between 216 and 3128 on 3G cellular network is 6.5 seconds. The prolonged waiting time was observed during the peak hours (12:30-4:00pm), which greatly improved after 4pm. Comparing M-Health App waiting time with Nielsens recommended time, we conclude that our system offers tolerable download time using 3G cellular networks. We further conducted a one-

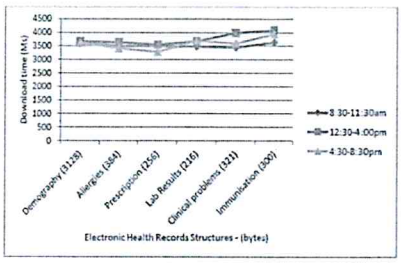

Fig. 8. Download Time with UCU Wireless network

day experiment using WLAN technology from the Uganda Christian University (UCU) network. We used the UCU wireless network because the University had extended its wireless connection to the Allan Galpin Health Centre. After obtaining approval from the University authorities, we connected the experimental mobile phones via an ADSL connection and the time taken to download the records was recorded by the server. Figure 8 describes our results. The results from Figure 8 above indicates that the average waiting time of our system to download the records from the server is 3.5 seconds in the morning, 3.8 seconds in the afternoon, and 3.4 seconds in the evening. Additionally, contrary to the 3G cellular networks, the waiting time of M-Health App system to download the records on WLAN environment is faster than that of 3G cellular networks. The higher bandwidth provided by WLAN technologies creates a performance gap between the 3G mobile networks and the WLAN technologies. The results in Figure 8 indicate that the waiting time for 3G cellular networks is twice that of the UCU WLAN assuming other factors constant. This means that WLAN should be the preferred choice for our ACOF, if available. However, the wider coverage of 3G cellular networks will allow downloads to proceed even if the patient is on the move.

V. Conclusion

We proposed an access control framework that protects patients health records on a mobile phone. In contrast to other architectures, the framework is designed to enable secure export of PHRs beyond the healthcare providers server security domain. To protect the mobile PHRs, our framework provides end-to-end encryption, and content-based access control. The experimental results demonstrate that mobile phones can be used to provide efficient and secure storage of PHRs in the developing countries.

Due to the small size of the field study sample, and the short duration of the trial it might be helpful to conduct a wider study to assess effectively the outcomes of the system. The benefits and usefulness reported by the users could potentially translate into improved medical and PHR outcomes. As mobile phone penetration in developing countries progresses, and initiatives to increase collaborative decision-making between patients and healthcare givers increase, we anticipate there will be more interest in providing patients accesses their medical records using mobile phones.

REFERENCES

[1] Glocal, eHealth Policy: From Silos to Systems. [Accessed: 02/08/2012], http://www.rockefellerfoundation.org/uploads/files/3af08a9f-a1a4-4fd5-9376-9b0bd498ceac-silos-to.pdf.

[2] M. Abdalla and D. Pointcheval, Simple password-based encrypted key exchange protocols., In Topics in cryptologyCT-RSA 2005 (pp. 191-208). Springer Berlin Heidelberg, 2005

[3] B. Adida and A. Sanyal and S. Zabak and I.S Kohane and K.D. Mandl (2010). Indivo x: developing a fully substitutable personally controlled health record platform. In AMIA Annual Symposium Proceedings (Vol. 2010, p. 6).0.4emAmerican Medical Informatics Association.

[4] Y. Anokwa, and N. Ribeka and T. Parikh and G. Borriello and M.C. Were (2012). Design of a phone-based clinical decision support system for resource-limited settings. In Proceedings of the Fifth International Conference on Information and Communication Technologies and Development (pp. 13-24).ACM.

[5] Y. Anokwa and C. Allen and T. Parikh (2008). Deploying a Medical Record System in Rural Rwanda. HCI for Community and International Development at CHI, 2008.

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

[7] J. Braa and B. Blobel (2003). Strategies for developing health information systems in developing countries. In D. Khakhar (Ed.), WITFOR 2003 White Book (pp. 175219). 0.4emLaxenburg, Austria, IFIP Press.

[8] C. Cocks (2001). An identity based encryption scheme based on quadratic residues. In IMA Int. Conf., pages 360-363.

[9] A. Dmitrienko and Z. Hadzic and H. Lhr, H. and A.R. Sadeghi and M. Winandy (2013). Securing the access to electronic health records on mobile phones. In Biomedical Engineering Systems and Technologies (pp. 365-379).Springer Berlin Heidelberg.

[10] A. Dmitrienko and Z. Hadzic and H. Lhr and M. Winandy and A.R. Sadeghi (2011). A Security Architecture for Accessing Health Records on Mobile Phones. In HEALTHINF (pp. 87-96).

[11] P. Ekler and J.K. Nurminen and A. Kiss (2008, January). Experiences of implementing BitTorrent on Java ME platform. In Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE (pp. 1154-1158).IEEE.

[12] J.A. Hoxmeier and C. DiCesare (2000, August). System response time and user satisfaction: An experimental study of browser-based applications. In Proceedings of the Association of Information Systems Americas Conference (pp. 140-145).

[13] S.Y. Kwankam (2004). What e-Health can offer. Bulletin of the World Health Organization, 82(10), 800-802.

[14] B. Kaliski (2000). PKCS# 5: Password-based cryptography specification version 2.0. [Accessed: 02/03/2012], from http://tools.ietf.org/html/rfc2898.

[15] J.P. Harrison and A. Lee (2006). The role of e-health in the changing health care environment. Nursing Economics, 24(6), 283.

[16] International Telecommunication Union 2013. Facts and figure. Accessed [March 12, 2013], from http://www.itu.int/ITU-D/ict/facts/material/ICTFactsFigures2013.pdf

[17] J. Nielsen (1999). User interface directions for the web. Communications of the ACM, 42(1), 65-72.

[18] A.T. Rashid and L. Elder (2009). Mobile phones and development: An Analysis of IDRC-supported projects. The Electronic Journal of Information Systems in Developing Countries, 36.

[19] R.L. Rivest and A. Shamir and L. Adleman (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[20] J. Robison and L. Bai and D.S. Mastrogiannis and C.C. Tan and J. Wu (2012, October). A survey on PHR technology. In e-Health Networking, Applications and Services (Healthcom), 2012 IEEE 14th International Conference on (pp. 184-189).IEEE.

[21] S.P. Sood and S.N. Nwabueze and V.W.A. Mbarika and N. Prakash and S. Chatterjee and P. Ray and S. Mishra (2008, January). Electronic medical records: a review comparing the challenges in developed and developing countries. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual (pp. 248-248).IEEE.

[22] World Health Organisation (WHO) 2005. Knowledge management strategy. Geneva. [Accessed:27/09/2012], from http://www.who.int/kms/about/strategy/kms_strategy.pdf

[23] R. Luk and M. Zaharia and M. Ho and B. Levine and P.M. Aoki (2009, April). ICTD for healthcare in Ghana: two parallel case studies. In Information and Communication Technologies and Development (ICTD), 2009 International Conference on (pp. 118-128). IEEE.

[24] Y. Zheng (2011). Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption (Doctoral dissertation, WORCESTER POLYTECHNIC INSTITUTE).

[25] A. Shamir (1984). Identity-based cryptosystems and signature schemes. Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7:47–53.

[26] D. Boneh and M.Franklin (2001, January). Identity-based encryption from the Weil pairing. In Advances in CryptologyCRYPTO 2001 (pp. 213-229). Springer Berlin Heidelberg.

[27] L.F. Blake and G. Seroussi and N. Smart, (1999). Elliptic curves in cryptography (Vol. 265). Cambridge University Press.