Biometric Access Control for e-Health Records in Pre-hospital Care

José R. Díaz-Palacios Víctor J. Romo-Aledo Amir H. Chinaei

University Of Puerto Rico at Mayagüez
Department of Electrical and Computer Engineering
Call Box 9000, Mayagüez, PR 00681, USA
+1 (787) 832- 4040 x. 3086
jose.diaz30@upr.edu, victor.romo@upr.edu, ahchinaei@ece.uprm.edu

ABSTRACT

Efficient and privacy-preserved access to the health record of patients is necessary to correctly practice medicine. This research addresses two concerns in emerging health software systems. First, electronic health records are not yet remotely accessible without using a token (e.g. health card). Second, patients' privacy must be preserved even in special situations such as emergency cases. This paper proposes to exploit *biometric identification* to access a central health record database featured by *privacy policies*. The experiments implement a real world scenario in which an ambulance reaches an unconscious patient who needs pre-hospital medical care for which their health record is retrieved from the database and is modified to meet privacy policies. The results demonstrate an average response time of 19.8 seconds when over 200K patients are registered in the database.

Categories and Subject Descriptors

J.3. [**LIFE AND MEDICAL SCIENCES**]: Medical information systems

General Terms

Security, Verification

Keywords

Biometrics, emergency, health record.

1. INTRODUCTION

Modern medical centers use electronic health records (EHR) for storing and retrieving patient's information. Medical centers provide a relatively easy access to EHR for authorized personnel on site, but this is not the case in the pre-hospital environment. Patients outside a medical center enjoy no benefit from having their information stored in an EHR when emergency medical technicians or private house doctors have no immediate access to such information.

Access to patient information must be done discreetly and must comply with some corporate policies—such as the rules stipulated in the health insurance portability and accountability act (HIPAA) [5]—conditions that must be met for **"proper access"**. Granting any health professional full access to a patients' EHR may pose potential law violation and create privacy and security risks. A study analyzing whether or not different health professionals will comply with the information assurance policy of their respective health clinic reveals that as many as fifteen compliance factors are involved in such a decision [7]. Therefore, granting *full access* to any health professional is simply not wise. Instead, a limited and/or partial access is the solution. Granting partial or limited access to a patient's EHR outside of hospital grounds has been an area of interest [8], but it has been limited to close contact or carried on solutions. In this paper, we focus on granting proper access to a patient's EHR remotely with the use of a biometric identification system.

EDBT/ICDT '13 , March 18 - 22 2013, Genoa, Italy

Biometrics as a means of access control has been previously studied and found to be a popular choice for guaranteeing authentication and authorization [18]. This includes: iris, voice, face, fingerprint, and hand geometry recognition [17]. Biometric features possess an if-and-only-if relationship discussed in details in Section 3.2. This makes biometric features the ideal basis for any identification system. In particular, fingerprint extraction is relatively easy in comparison with other biometric features. Fingerprints also possess great hardware and software support in industry [1]. Hence, we choose fingerprints as an adequate biometric identification feature for the environment in mind. Note that biometric identification not only can be used for the health data privacy preservation, it can also contribute in preserving the privacy of the token data (e.g. social security number) itself.

We propose a solution that enables emergency medical technicians to have simple and fast, remote and token-free, as well as privacy-preserved and reliable access to patients' medical information. The idea is to provide the technicians with a mobile system through which they gain access to necessary attributes of patients' EHR using the patient's fingerprint. Reliability is employed by exploiting the uniqueness of a person's fingerprint as a means of access control as well as by precision of fingerprint scanners. Privacy of patients is preserved by enforcing an *arbitrary* privacy policy, which we discuss in Section 3.5. Furthermore, the system requires patients to provide only their fingerprint; they need not to carry with them an additional token—such as a health card, driving license, etc.—to receive the service. Simplicity and efficiency of the system is justified through the course of implementation and experiments.

2. LITERATURE REVIEW

There are several approaches to access electronic health records (EHR) in emergency situations. This section reviews them as follows.

Web services such as Microsoft Health Vault and former Google Health provide space to store medical information for any registered user [3]. This type of service is effective at storing information, but it depends on the patient's credentials, e.g. username and password. It lacks the ability to access information in real world situations where

patients may forget such credentials or may simply be unable to provide such information in a given circumstance.

Another approach for storing and sharing medical information is via a *flash drive* [4]. The Health Key is a USB flash drive sold by MedicAlert. It provides storage for medical records. However, when it is inserted into a computer it automatically prompts the user with its contents. Thus, the device is meant to be inserted only into physicians' computer in order to not violate privacy of is content. This is a high risk to a patient's privacy because of possible misuse by strangers. Robbery and theft may result in identity theft. Also, it is difficult to keep such information up to date.

Some approaches suggest a carried-on token—e.g. wearing a *smart band*—such as the one proposed by Hinkamp in which patent suggests a health system built around the smart band, which stores patients' health data [9]. The data can then be retrieved by a server network and displayed on a screen. While this proposition provides a good solution for real time access on an emergency situation, it is dependent on the assumption that a patient will be carrying one; thus, it deemed unfeasible for the basis of a health system.

Another carried-on token approach is called *rendezvous-based* access control [8]. It rejects using the Internet to access patients' EHR. Instead, the data is replicated inside global **s**ystem for mobile communication (GSM) servers stationed at every emergency environment, e.g. placing one inside an ambulance. Emergency medical technician gain access to the patients' EHR file through the use of a token, which contains the encrypted key, provided by the patient. This approach is efficient at decentralizing patient information because each GSM server stores its data independent from others. However, it is not effective in practice due to its dependency on a carried-on token.

Other approaches require the use of smartphones' Internet capability for accessing web services [3]. Kulkarnim and Agrawal propose a healthcare system for developing countries based on using smartphones as tokens [10]. Smartphones act as a beacon for health information with the use of external hardware sensors. The system basically consists of smartphone handlers or facilitators in each community to which one can go for medical guidance. Although this is not targeted for emergency access, it serves as a precursor to a modernized healthcare system which employs mobile technology. Yet, it is still token-based.

Another example of relying on a smartphone token is described in an approach by Gardner et al. [6]. In their approach, patients must carry their medical record inside their phone. Privacy is preserved with the division of access capabilities, so called *secret sharing*. Secret sharing refers to the case that privileges of granting access to an object are divided into different layers. For example, when a user wants to access their own health record, they must enter the right combination of password and biometrics to gain the access.

The need for a *token-less* option is in place. Our solution is based on the approaches introduced by Gardner et al. [6] and Paik et al. [16]. The former proposes using of biometrics for authentication and authorization. The latter proposes to apply biometrics to register and identify people and their attendance. Their approach is tailored for registrar methods in India, as their growing population is overwhelming. The idea is to create a biometric attendance terminal that eliminates the need for keys by using fingerprints: once registered, a visitor can log her attendance by scanning her chosen finger once. None of the approaches focus on accessing EHR's in emergency care or privacy preservation in such cases. Yet, the biometric terminal serves as a good example of how biometrics is effective in such problems.

3. SOLUTION MODEL

This section clarifies assumptions and the scope of our solution. The granular details and specifications will be explained in the subsequent Sections 3.1 to 3.5.

3.1 Adversarial Model

We do not address an attack to the central database with the use of external resources, such as software, hardware, or knowledge; neither do we provide a framework for health policy to regulate the use of such system. We assume that such a system will be regulated and deployed by corresponding agencies in charge. Theft and social engineering methods of unauthorized access are not considered. Traditional physical appropriation of data, however, is assumed in the design and nature of the system.

System adversaries—we are addressing—are described as internal snoopers, such as a misbehaving healthcare worker who might seek to profit, for instance, by selling the medical history of a patient.

3.2 Access Control Method

Proper access control security relays on identification, authentication, and authorization in order to enforce security and maintain the integrity of data [14]. These components are closely related to one another. They represent a closely linked chain, where each node is one of the three components of access control. Each node of the chain is a pre-requisite for the next.

3.2.1 Non Biometric Techniques

As an example of non-biometric access technique, assume a person wants to view an old email account for which the email host has no recollection of their password. How do they manage to retrieve access of their customer? The email host most likely provides an alternate access control method for this situation. It could consist of providing answers to some security questions usually combined with some CAPTCHA techniques [13].

3.2.2 Using Biometrics

Biometrics techniques play an important role in our system. We focus on the use of fingerprints among various categories—such as iris, voice recognition, etc.—by which biometrics can be utilized [15]. Fingerprints are individual unique identifiers of any person. They provide an if-and-only-if (*iff*) relationship between a patient and their fingerprint. Our system follows the *iff* relation of Dilema and Lupetti's model [8], where access to patient information is granted *iff* the patient met in person with the physician. Similarly, our design grants access to the patient health record *iff* the patient's fingerprint is matched with one stored in the database. Of course, given the system architecture, explained in Section 3.4, the fingerprint should have been previously enrolled in the electronic health record database in order to find it in future queries.

3.3 System Assumptions

Because access to the pre-hospital environment has been mostly limited to carried-on devices [4][6][8][9], we strive away from such proposals; instead, we favor the remote accessibility of patient information. Yet, illustrated in Figure 1, a couple of preparatory events must take place to ensure the full functionality of the system—as follows:

- First, legislation adopts the privacy-preservation policy discussed in Section 3.5, or defines one as it is arbitrary.
- Second, patients must visit their respective general practitioner office to be added to the EHR database together with an image of their chosen fingerprint.

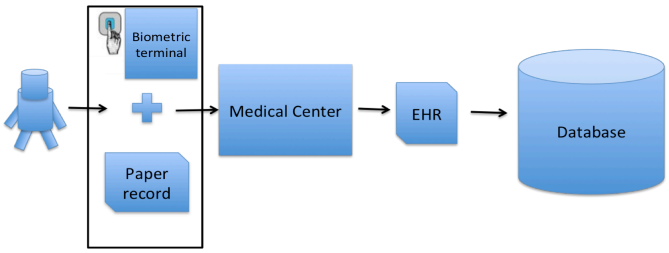

Figure 1. System preparatory events

3.4 System Architecture

The system architecture is defined as a unimodal biometric system that uses a singular biometric feature. Sharma and Kumar state that unimodal biometric systems suffer from noisy sensor data, non-universality, and unacceptable error rates [12]. However, the empirical data presented in this paper contradicts their statement at least for our particular application. Due to real world implementation feasibility, the unimodal system is favored in our particular scenario even though multimodal systems have been proven more accurate for complicated identification purposes [12].

3.4.1 System Component Description

System components consist of both hardware and software elements. Hardware components include a fingerprint scanner, a mobile broadband internet capable tablet PC, and a hosting server computer. Figure 2 depicts our system components architecture linked in functional sequence in order to demonstrate the sequence of events.

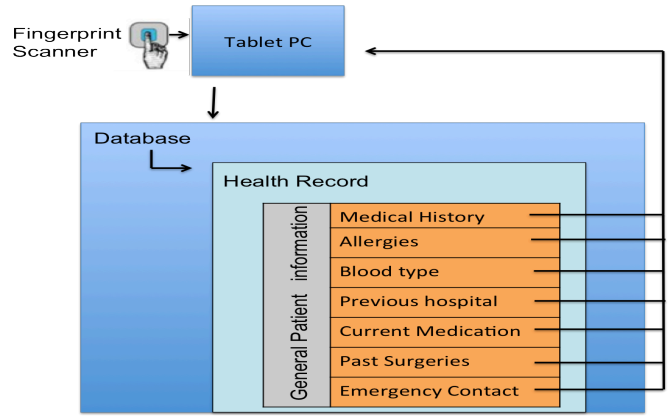

Figure 2: Health record retrieval with privacy-preserved policies

3.4.2 Using the system

There are two hardware components, two software components, and a set of privacy-preservation policies in our system architecture. First, the biometric terminal user collects the patients fingerprint image. Then, they select the *identify command* from the system user interface. It is important to note that collecting a patient's fingerprint during this scenario study is feasible even if the patient is found unconscious. The fingerprint image is then sent as a SQL query to the central database through the biometric terminal's mobile broadband connection for matching. After this process, the result is either the set of privacy preserved values from a record or a not found message.

3.5 Privacy Preservation

By Health Insurance Portability Accountability Act Privacy Rule [5] (HIPAA), it is learned that access to a patient's health record should be highly regulated. Among many restrictions, it prohibits unauthorized access to a person's health information without consent. Thus, one cannot provide full access to such information to any health personnel unless the policies allow. This is known as *the principle of least privilege* [11]—also required by minimum necessary provision of HIPAA. The principle of least privilege is at the core of our system privacy-preservation policies. We have conducted extensive research and consultation to identify attributes that are essential in emergency and pre-hospital care. (This also includes consultations with the Ponce School of Medicine as well as New Orleans Medical Center.) Figure 2 shows—under given circumstance and privacy policies—exposure of the following attributes are allowed: *medical history*, *current medication*, *allergies to medication*, *past surgeries*, *blood type*, *emergency contact*, and *medical center* in which patient is normally treated. Fields colored in orange in Figure 2 are used in our client software to filter data found inside a patient's EHR (cf. Section 5). As emphasized in Section 4.1, the assumption is that legislation has taken place to define legitimate privacy policies. However, such policies can simply be replaced by any arbitrary policies that other privacy acts instruct or by any arbitrary decentralized policies that also take into account each patient's preference—as long as complies with corporation policies (here HIPAA) .

4. IMPLEMENTATION

As stated in Section 3.4, our approach is a junction of four components: fingerprint scanner, remote capable device (Tablet PC), the matching algorithm, and an electronic health record database. The system has been implemented with the products listed in Table I.

Table I. Implementation components

Component	Implementation Choice
Mobile Device	Hp Slate 500
Fingerprint Scanner	Futronic FS88
Fingerprint Matching Algorithm Software	Griaule Biometrics Java fingerprint 2009 SDK

The mobile broadband capable tablet PC runs on windows 7 (full version) OS platform. It has Internet capability for WiFi and 4G mobile broadband. Hence, it is able to send and receive information independent from Wi-Fi hotspots. Also, it has one USB port that is needed for most fingerprint scanners currently on the market. In addition, it has 2GB DDR2 SDRAM and an HD 64GB. Choosing a tablet PC running on Windows operating system made it more convenient due to compatibility with other components. The Futronic FS88 USB fingerprint scanner [1] was chosen as due to its size (~ 2" by 2"), simplicity, compatibility, and support. The core component of this system is the client and server software utilities utilizing the fingerprint-matching algorithm provided in the software development kit. This component is called client and server software. This process is implemented using Java and Griaule's fingerprint-matching software development kit [2]. The SDK provides malleable software to utilize the proprietary matching context and template extraction. The matching algorithm for a tolerance degree of 180 is guaranteed to have a false acceptance rate of 0% and a false rejection rate of 1%. It is also capable of conducting one-to-many comparisons of fingerprint, for more efficient performance.

4.1 Database Design & Population

The database is designed in first normal form and created by PostgreSQL open source software. Relations are populated by fingerprints and notional electronic health records (EHR) for a more realistic scenario in experiments. Each EHR has an ID number, binary data column (fingerprint image), and several attributes specifying different medical information or history of patients.

Fingerprint images are represented as a hexadecimal coded string. Therefore, manipulating such a string generates a different fingerprint based on its numeric values. A Java program was written to generate more fingerprint images. The program requires a fingerprint string input, and then modifies ten characters of the string with randomly generated characters. Using this tool, we created and populated individual databases starting from 20k fingerprints and increasing to 200k in 20k intervals. The fingerprint-matching algorithm interprets them as authentic fingerprints. Section 5 illustrates our experiments.

4.2 Client & Server Software

The system is implemented in two versions. One version is *server-matching*, while the other is a converse approach: *client-matching*. Both versions yield valuable results. However, the former is more effective than the latter. This can be appreciated in Section 5. The details of each version are as follows.

The *Server-matching* version has a client and a server software utility. The client software extracts the image taken from the scanner and creates a template of a hexadecimal coded string based on the finger's attributes. This template is the key component used throughout the whole process. It is used as the primary identifier for each record and as the key parameter in the matching process.

The server runs in an infinite loop waiting for the requests sent by the client. In the client side, once a finger is scanned, the resulting template is sent to the server as a request to look up the respective EHR. The request triggers an event in the server to look up the received template in the database. The matching process runs locally in the server. This reduces the response time enormously (cf. Section 5). It only takes a few seconds to return a result. When the server finishes processing, it lets the client know which information to display. While this is happening in the server, the client is also inside a loop waiting for that information to be received so the patient's crucial information can be displayed in the screen. Letting the server handle the matching process locally instead of sending the result set to the tablet makes the process run almost instantly.

Using the converse approach, *client-matching* version, the tablet would need to download gigabytes of information from the server and then process the result set locally. This approach takes much longer as shown in Section 5. However, it inspires a solution in which the client tablet can download the most up-to-date instance of the database prior to departure the hospital towards remote rural places where the Internet connection is not guaranteed.

5. EXPERIMENTS

In order to evaluate the feasibility of our solution in real world, we have experimented extensively both the fingerprint matching time and the system response time. We created ten EHR relations: starting from 20K fingerprint images to 200K images with 20K intervals. Each experiment for measuring the fingerprint matching time and the system response time were conducted five times and, for each case, the average time was calculated. The experiments were conducted through the tablet PC and the following server: Intel Core i5 2.67 GHz processor, 3GB RAM, and 30GB HDD. Also, both versions of implementations were evaluated through our experiments to measure their respective matching and response time.

5.1 Response Time Testing

Measuring the total system response time is essential for testing real world applicability. We define response time of the system as the sum of fingerprint matching time and the time it takes to produce the on-screen result. It can also be defined as the time elapsed from the moment the user of the biometric terminal presses the identify button on the client software to the moment a result shows up on the screen.

Figure 3 shows the result of this experiment. Furthermore, based on Figure 3, one can conclude that using server-matching approach for such a task is highly effective. Probing the data for the largest amount in the dataset shows that, for database populated with 200k records, one can expect an average result of 19.88 seconds. Fingerprint match time can be defined as the time the fingerprint-matching algorithm takes to find a match against a particular database. Testing against locally stored fingerprint databases on the tablet PC yielded an average match time of 17.8 for 200k fingerprints. By taking into account our first sample, one can predict a rough estimate of future behavior: the response time increases one second per every ten thousand fingerprints (1:10,000). Thus, if we were to extrapolate this ratio to a larger population of fingerprints, we could predict the response time for any population. However, it is important to note that this research has implemented the simplest approach of a central database just to show the feasibility of token-free identification and privacy preservation. It sounds promising that decentralized databases and optimization techniques can further improve this performance, as a follow up to this research.

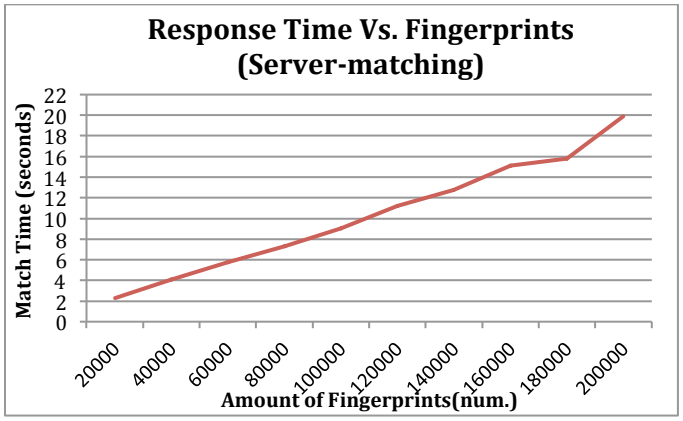

Figure 3: Displays response time for server-matching version of the system.

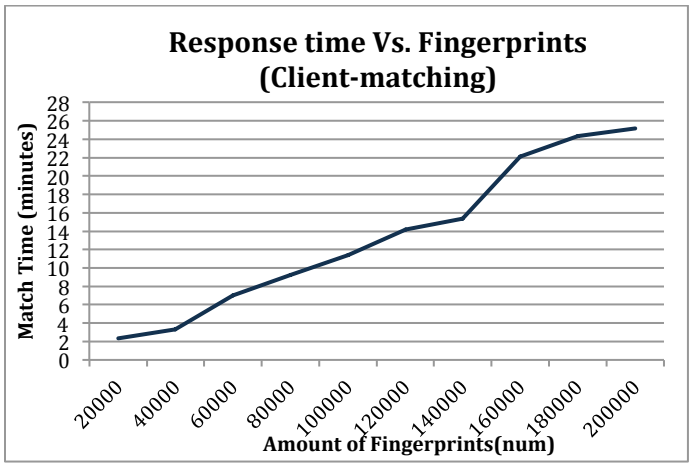

Figure 4: Response time displayed as a function of the amount of fingerprints inside the database.

Figure 4 depicts the response time for the client-matching approach, where the time scale for matching is in minutes not seconds. This difference is due to downloading the whole database each time through the Internet. Although this approach is not feasible for frequent scenarios, it inspires a solution through which the most recent version of the database instance can be downloaded to the client machine prior to departure the hospital grounds towards a

remote rural place where the Internet connection is not guaranteed or reliable. This observation suggests another research topic, which is still token-free, and privacy preserved but it is based on using replicas and distributed databases.

6. CONCLUSION & FUTURE WORK

This paper provides insight on how use of biometrics together with new hardware and software technologies can be of significant advances in the combination of privacy preservation concerns and pre-hospital emergency cases. The proposed system describes a biometric terminal that exploits mobile technology to send fingerprint of patients from an emergency scene to a central database, and receive the health information of the patient to provide proper care to them in pre-hospital environment while patients' privacy is preserved with respect to an *arbitrary* privacy policy. Another contribution of this work is its token independence: while other solutions impose patients to carry a token, such as official identification cards or smart bands [9], our approach is token free and it only depends on the patient's fingerprint.

During our extensive experiments, we found that a server-matching solution yields a response time acceptable for realistic situations. In particular, the experiments reveal a one second overhead for every ten thousand EHRs (1:10,000), efficient enough for many real world applications. In particular, when there are 200,000 EHRs in the database, the response time is 19.8 seconds. This is despite the naive centralized database implementation. Thus, the response time can definitely be improved when optimization techniques and decentralized databases are employed for larger populations.

An immediate direction to follow this research is to incorporate a wireless Bluetooth fingerprint scanner into the proposed architecture. This feature would improve the mobility and would facilitate the process of scanning a patient's fingerprint.

Concerning privacy preservation, the current model does not provide a flexible mechanism to change the privacy policies. Furthermore, all patients are enforced to comply with the same policy. However, this work can be improved by exploring a system that can opt for a decentralized privacy preservation policy. This would enable each patient to choose how each field of their EHR should be treated in terms of privacy concerns. Furthermore, policy conflict resolution is a follow up extension to decentralization.

7. ACKNOWLEDGMENTS

We would like to acknowledge the University of Puerto Rico at Mayagüez and the Industrial Affiliates Program for partially funding this research. In addition, we would like to thank medical experts, Dr. Ihdaliz Flores, from the School of Medicine at Ponce Puerto Rico, as well as Mr. Juan G. Medina and Dr. Enrique Segura from the Culicchia Neurological Clinic for their valuable consultations. We also greatly thank Hiva Samadian as well as one of PAIS reviewers (anonymous) for their constructive feedback to this work.

8. REFERENCES

[1] Futronic, FS88 FIPS201/PIV Compliant USB2.0 Fingerprint Scanner http://www.futronic-tech.com/product_fs88.html

[2] Griaule Java Software Development Kit 2009 http://www.griaulebiometrics.com/ page/en-us/fingerprint_sdk

[3] Microsoft Health Vault http://www.healthvault.com/Personal/index.html.

[4] The MedicalAlert Key http://www.healthcentral.com/migraine/reviews-202629-5.html

[5] U.S. Department of Health & Human Services, *HIPAA Privacy Rule Summary,* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

[6] Akinyele, J., Pagano M., Green, M., Lehmann, C., Peterson, Z., and Rubin, A. 2009. Securing electronic medical records on smart phone. *SPIMACS '09 Proceedings of the 1st ACM workshop on Security and privacy in medical and home-care systems*, (Hyatt Regency Chicago, IL, November 9- 13I, 2009), ACM New York, NY.

[7] Cannoy, S. D. and Salam, A. F. A framework for health care information assurance policy and compliance. *Communications of the ACM, vol. 53 Issue 3, March 2010*. 126-131.

[8] Dillema, F., and Lupetti, S. 2007. Rendezvous-based access control for medical records in the pre hospital environment. In *HealthNet 07' Proceedings of the first ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments*, (San Juan, Puerto Rico), ACM New York, NY.

[9] Hinkamp T. System providing medical personnel with immediate critical data for emergency treatments. Patent Application Publication 11/510,317, 2007.

[10] Kulkarni, S. and Agrawal, R. 2008. Smarphone driven healthcare system for rural communities in developing countries. *HealthNet '08 Proceedings of the 2nd International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments*, (Breckenridge, Colorado, June 17, 2008), ACM New York, NY.

[11] Salter, J. and Schroeder M. The Protection of Information in Computer Systems. *Proceedings of the IEEE*, 63(9), 278-1308 (1975).

[12] Sharma, D. and Kumar, A. Multi-Modal Biometric Recognition System: Fusion of Face and Iris Features using Local Gabor Patters. *International Journal of Advanced Research in Computer Science*; *vol 2, No. 6, Nov-Dec 2011. 166-175.*

[13] Shrili-Shahreza, S. New Anti Spam Protocol Using CAPTCHA. *Networking Sensing and Control IEEE International 15-17, April 2007.*

[14] Sukhai, N. 2004. Access Control & Biometrics. *InfoSecCD '04 Proceedings of the 1st annual conference on Information security curriculum development*, ACM New York NY.

[15] Maltoni, D., Maio, D., Jain, A.K and Prabhakar, S. *Handbook of Fingerprint Recognition 2nd.* Springer Publishing Company, 2003.

[16] Paik, M., Samdaria, N., Gupta, A., Weber, J., Bhatnagar, N., Batra, S., Bhardwaj, M., and Thies, W. 2010. A biometric attendance terminal and its application to health programs in India. *NSDR '10 Proceedings 4th ACM Workshop on Networked Systems for Developing Regions*, (San Francisco, CA, 15-18 June, 2010), ACM New York, NY.

[17] Pankanti, S., Prabhakar S., and Jain, A. On the individuality of Fingerprints*. IEEE Transactions on pattern analysis and machine intelligence, vol. 24, No. 8. August 2002*.

[18] Prabhakar S., Pankanti, S., Jain, A. Biometrics Recognition: Security and Privacy Concerns. *IEEE Security & Privacy, IEEE Computer Society, March- April 2003.* 33-42.