Designing an Electronic Health Security System Framework for Authentication with Wi-Fi, Smartphone and 3D Face Recognition Technology

Lesole Kalake(✉) and Chika Yoshida

Graduate School of Technology, Kobe Institute of Computing,
Kano-cho 2-7-7, Chuo-ku, Kobe 6500001, Japan
Lesole.kalake@gmail.com, cyoshida@kic.ac.jp

Abstract. Information technology for development is the tool that has been around for ages and it is now mainly focusing on making people lives easy including of those in a health sector. However, health practitioners and patients are somehow had not fully experienced this benefits due to sensitive information distribution and security concerns around the distribution of electronic health records. There have been various issues and challenges on security breaches, leakage of confidential patient records and computer attacks which have been raised on security and privacy concerns in electronic health records. The unauthorized access, denial of services, lack of standardization of the system increases mistrust on electronic health record system and makes it very difficult for the parties involved in handling and transmission of patients' record. Therefore the aim of this paper is to propose an efficient and cost-effective face recognition security framework through Wi-Fi to enable the monitoring and access control on patient record in developing countries.

Keywords: 3D face recognition · Biometric · Mobile device encryption · Patient electronic health record · Wi-Fi · Mac address · Serial number · International mobile station equipment identity · Authentication and security

1 Introduction

Healthcare process in developing countries is hierarchy structured based on the type of service, specialization and location. This means a patient have to carry a paper file or card with sensitive information and move from one place to a referral practitioner at the another side of a Health Institution or region [1]. This poses a huge risk for files been easily accessed by unauthorized persons or fall into the wrong hands and deprive patient privacy rights. The electronic patient health record is the ideal system that healthcare professionals around the globe believe it will offload work and help in making work and patient health record distribution easy by enabling information sharing over the network. However, electronic patient health record is faced with security threats and challenges as to how to secure the patient record and who should have what rights on which section of the electronic health record [2, 6].

F. Belqasmi et al. (Eds.): AFRICATEK 2017, LNICST 206, pp. 226–232, 2018.
https://doi.org/10.1007/978-3-319-67837-5_22

There have been lots of security protocol and framework proposals for e-health authentications and security improvement but most of them sound time consuming, expensive and exposes negative impact on the practitioner's daily work coverage. They also seem to contribute to health record distribution path error and have a huge potential on information management risk. The patients are very much worried about their information control access and risks such as information leakage and disclosure. They do not want everybody at Health Institutions to have access to their information without their consent [3]. Therefore, they want a full control, tight security and activity log on their health records of the authorized individuals. On the other hands, both health professionals and patients don't like to spend too much time waiting for system authentication or have to go through lots of hectic authentication processes. Therefore, there is a need for a more secure, quick, hygienic and accurate authentication technology method. Hence, this paper proposes a cost-effective and efficient facial recognition technology method through Wi-Fi for e-health security system to enable the system administrators to have easy access control on authorized individuals. It is also intended to improve the distribution of patient record in a securely and efficiently technological environment.

1.1 Objectives and Scope

Electronic patient health record system is the place where everybody wants to go but the limitation is the best security technologies. Hence, sharing sensitive information over the network needs tight security. Nowadays smart phones have cameras and this is the boost for face recognition authentication procedures and can be used to scan the face on live and authenticate the user within less than five seconds. The proposed e-health system in this paper will use the mobile device, biometric and network technologies to strengthen authentication and eliminate security threats.

1.1.1 User Login Credentials

User shall register to creating a profile over the internet using work computers and notebooks. Use a 3D face recognition application installed on a smartphone to scan a face.

1.1.2 Device Information Storage

The Smartphone's information retrieval and verification shall be done by the system through a request sent via an email or SMS to the user for the account activation. During a user profile creation process the system solution will link the user, personal computer and smartphone device information that has been retrieved from Wi-Fi, and then encrypt and store it on the Web server for future authentication process and auditing.

2 Related Work

Biometric technologies have been used in the different fields but mostly where the confidentiality matters most such as in army, hospital, finance and intelligence agencies.

The facial recognition is one of the biometrics that is mostly used in the market today. The United Services Automobile Association has deployed the face recognition authentication technology for its members to login to mobile banking with the blink of an eye literally [4]. ZoOm™ has developed the 3D facial authentication smartphone application which use the front-facing camera on any smartphone to capture a selfie video and instantly process frames on the device and compare against previously stored biometric data [5] (Table 1).

Table 1. Biometric technologies comparisons

Facial recognition (3D)	Voice recognition	Signature recognition	Finger print	Iris recognition
Very high accuracy	Low accuracy	Medium-Low accuracy	Very high accuracy	Very high accuracy
Verification time is generally less than 5 s	Verification time is generally less than 6 s	Verification time is generally more than 5 s	Verification time is generally more than 5 s	Verification time is generally less than 5 s
No face picture or video can be used	Voice pitch not always exactly the same due to flue and surrounding environment	Signature not always exactly the same	Can be chopped off or damaged	No eye from a dead person can be used
Non intrusive	Non intrusive	Non intrusive	very intrusive	Intrusive
Medium storage required	Small storage required	Small storage required	Small storage required	More memory storage needed
Economical	Very cheap	Very cheap	Economical	Expensive

Facial recognition 3D technology is indeed the highly accurate, nonintrusive and economical biometric technology that can be incorporated in e-health security framework to improve the authentication and security.

3 System Solution Overview

Everybody is sensitive about their health status disclosure that is why carrying the files to the referred practitioner is always in a massive protected route. Hence, proposes a cost-effective e-health system to ensure that patient information is highly secured over the internet in developing countries. It shall be an integrated multi-authentication with a Web application for transactions, Web servers, Wi-Fi, smartphone, database and facial recognition applications for authentication.

3.1 Web Authentications

The patients, hospital receptionists, health practitioner assistance, pharmacists or health practitioners (like Drs and Specialists) are always using the smartphone for different

tasks every day, but this paper proposes the use of the same mobile device with Wi-Fi switched on for both registration and authentication process. This will enable the system to register the device and store the information such as serial number, MAC address and IMEI on the background linked with the user profile for authentication process.

3.2 Device Role

A device used for profile creation or to activate a user account is the primary device that will be used in the future to authenticate and link with other devices if the users have multiple devices. All devices must be on the same network during the process. The user will need to type in the e-health URL and the device information will be mapped and linked with the information stored. A web server will reply with a face recognition application request to user's smartphone for an auto login authentication process. In a case of a loss or theft of one of the devices, the system administrator can easily disable the device from the database at the backend to enable the user to register a new device.

3.3 User(s) Role

The roles will be created based on the levels such as patient, hospital receptionist, health practitioner assistance (nurses), pharmacist and health practitioner (like Drs and Specialists), whereby the patient have the full control of his or her electronic health record. Doctors and Specialists will have full view and edit of the records while others will have row or table level view permission only.

3.4 Face Recognition Application

Smartphone's front face camera shall be used to capture face live via 3D face recognition application, processed and sent to the backend for storage. The face recognition application shall also be used for face scanning and a quick user authentication without login credentials been required.

3.5 Wi-Fi and Smartphone Roles

A smartphone always sends a signal when the Wi-Fi is turned on regardless of connections to the network. Therefore, the smartphone information shall be easily retrieved and used for user identification, matches, face and frame instant processing; and analysis of activity logs or communication packets. Instead of using computers for authentication, smartphone on the same Wi-Fi with the computer will be used for login and access onto e-health system.

4 Proposed System Architecture

When devices are on the same network their information can uniquely be retrieved, paired and stored. They can also establish an easy and fast communication channel to distribute packages over the network amongst themselves. Hence, it can be told which device was used and by whom, when and for what purpose.

The proposed system architecture includes several devices and components that contribute to the effectiveness of a solution. A personal computer and smartphone are the key components for user identification and authentication, whereby a Wi-Fi network role is to gel and harmonize the whole solution with the implementation of a 3D facial recognition application and a database. During the registration process the communication channel between the personal computer and smartphone was established whereby a network has retrieved the device information and stored it temporarily. The system shall use the channel to forward the response request for the user to launch a 3D facial recognition application on the smartphone. Then enable a database to retrieve, map, process and store information gathered from both devices for in future when a registered user login with his or her personal computer to access a patient electronic health record via the URL.

In Fig. 1, the high-level system overview illustrates how the solution should work for user identification and authentication. A user login with his or her personal computer, and then a network retrieves the device information temporarily for a database to perform user match for identification and authentication. Then if a device is registered already, a database will respond with a query for the web server to ask for a launching of the 3D

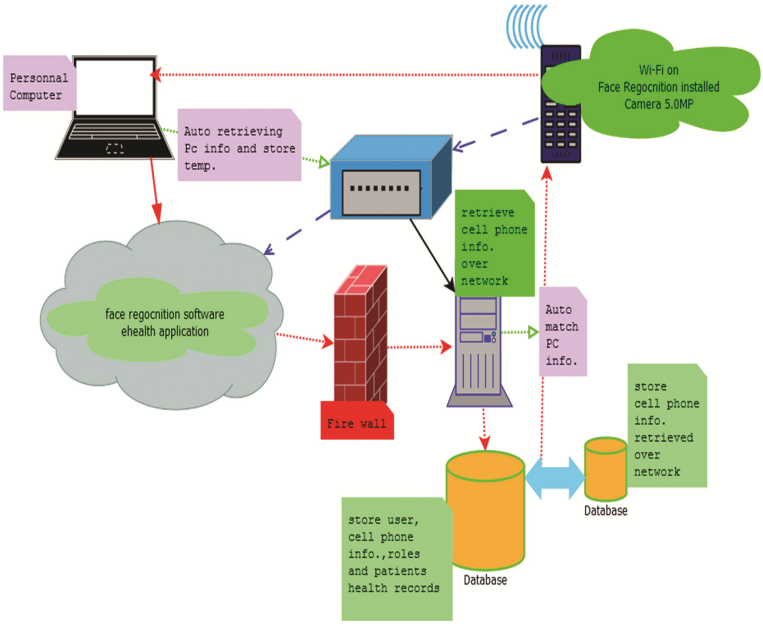

Fig. 1. Proposed system architecture and interactions

facial recognition application for authentication. If it's a new device then it means a new registration process.

5 Conclusions

This paper proposed the integrated multi-authentication processes into a single login procedure for e-health system. The system framework includes the popularity usage of computer networking, 3D face recognition technologies and smartphone device for a secure login. Integrated multi- factor authentication includes Wi-Fi for mobile device detection and face recognition pair as well as username and password when necessary. The proposed security framework can overcome the vulnerability of a traditional authentication process in developing countries. The idea of this security framework system is to leverage the mobile device as a personal and unique identifier for each user. The system brings many advantages in improving the security of the secure authentication and it is efficient, affordable and easy to implement in developing countries.

Appendix: Acronyms and Definitions

1. E-health- is an electronic patient health record system used to store and help in centralizing the individual's medical history.
2. Wi-Fi- a local area network that uses high frequency radio signals to transmit and receive data over distances of a few hundred feet; uses Ethernet protocol.
3. MAC- a media access control address is a unique identifier assigned to network interfaces for communications.
4. IMEI- a unique, number to identify mobile phones and satellite phones.
5. Smartphone- is a mobile phone with an advanced mobile operating system which combines features of a personal computer operating system with other features useful for mobile.
6. 3D facial recognition- is technique that uses 3D sensors to capture information about the shape of a face.
7. Drs- General health practitioners.
8. Specialist- a doctor highly skilled in a specific and restricted field of medicine.
9. Nurse- a person who is qualified to treat certain medical conditions without the direct supervision of a doctor.
10. Pharmacist- member of the health care team directly involved with patient care and dispense medicines.
11. URL- Uniform Resource Locator is a protocol for specifying addresses on the Internet.

References

1. Jacob, J., Agrawal, V.: Privacy in electronic health record systems – consumer's perspective (2003)
2. Barrows, J.R.C., Clayton, P.D.: Privacy, confidentiality, and electronic medical records. J. Am. Med. Inform. Assoc. **3**(2), 139–148 (1996)
3. Papoutsi, C., Reed, J.E., Marston, C., Lewis, R., Majeed, A., Bell, D.: Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study, October 2015
4. Crosman, C.P.: Biometric Tipping Point: USAA Deploys Face, Voice Recognition, February 2015. http://www.americanbanker.com/news/bank-technology/biometric-tipping-point-usaa-deploys-face-voice-recognition-1072509-1.html
5. PR Newswire: ZoOm™, The World's First Secure Selfie 3D Authentication App, Announced By FacialNetwork, July 2015. http://www.thestreet.com/story/13212142/1/zoom-the-worlds-first-secure-selfie-3d-authentication-app-announced-by-facialnetwork.html
6. Mirembe, D.P.: Design of a Secure Framework for the Implementation of Telemedicine, eHealth, and Wellness Services (2006)