International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | June 2022 www.irjet.net p-ISSN: 2395-0072

A Review on Biometric-based Systems for Patient Health Record Authentication

Arya J Nair[1], Sandhya S[2], Sreeja Kumari S[3]

[1,2,3] *Lecturer, Dept. of Computer Engineering, NSS Polytechnic College, Kerala, India*

Abstract – *Health records kept on paper have largely been replaced by electronic versions in the worldwide health sector. Now, patients, physicians, and healthcare providers have easier access to information about their health. Having access to personal health records raises privacy, confidentiality, and security concerns. This emphasizes the need for reliable and powerful identification. Using biometrics to identify patients can prevent duplication of medical records and detect fraud while increasing patient safety. The field of biometrics deals with finding ways to evaluate and use a person's physical and behavioral characteristics for identification and verification. A review of biometrics-based methods for patient identification and data security is provided in this paper.*

Key Words*: *Intelligence Quotient (IQ), Magnetic Resonance Image (MRI), Electroencephalogram (EEG), Convolutional Neural Network, Support Vector Regression (SVR), Small Visual Geometry Group (SVGG), Visual Geometry Group (VGG), Residual Network (ResNet), Artificial Neural Network (ANN)

1. INTRODUCTION

Over the past few years, the deployment of computer technology (CT) to improve health care services has proved to be highly beneficial [1]. Having electronic health records has helped hospitals reduce paperwork and alleviate the shortage of healthcare workers. It is essential to employ trusted technology for storing and retrieving records that allow users to quickly authenticate themselves. With biometric authentication technologies, patient healthcare data can be accessed more easily and transmitted securely. A biometric identification system uses physical and behavioral features to identify someone, whereas a biometric authentication system verifies the authenticity of an individual. Physical identification methods [2] utilize invariable physiological characteristics, such as face shape, fingerprint, retina, iris, DNA, etc. Behavioral identification methods consider the characteristics inherent in each individual as they repeat behavior which includes signature, gait, etc.

Medical biometrics refers to the use of biometrics in clinics, hospitals, or for patient monitoring. This might involve managing the workforce, controlling access, identifying people, or storing medical records [3]. Most hospitals use biometrics to identify their patients and personnel. It improves the workflow of the healthcare system, reduces medical data duplication, and identifies patients. Despite being a potential use case, patient matching among healthcare providers is still not extensively used [4].

A biometric-based system facilitates the maintenance of health records [5]. Patients are not required to bring any documents, prescriptions, or other items. The management of patient records is also made simpler for the practitioner. Doctors can read, edit, and remove patient medical records because of these technologies. The doctor can lessen the likelihood of records becoming mixed up by entering prescriptions and checking past data. Without the consent of both the patient and the doctor, a doctor is not permitted to make changes to a patient's records.

This article examines multiple biometric-based patient identification systems. In Chapter 3, the different methods of identification are discussed. The comparison of the various approaches is shown in Chapter 4. The study's conclusion is presented in Chapter 5.

2. LITERATURE REVIEW

The fingerprint scanner is used by the fingerprint-based patient authentication system to access the database and collect patient information [6]. The fingerprint is thought to be the most accurate and efficient biometric identification approach is thought to be a fingerprint. Everybody has a different fingerprint, and they do not alter over time. Users of this system will always have access to healthcare-related information.

The face-based system in [7] consists of a Raspberry Pi 3 processor and a Webcam for acquiring the face image of the patient. The facial attributes are extracted using the Local Binary Pattern (LBP) and Haar Cascade Algorithm. The classifier gets the extracted attributes, compares them to the ones it has learned, and then displays the data and reports that were saved in the database.

An iris-based cancelable biometric cryptosystem has been proposed in [8] to securely store patient medical information on smart cards. The information is then encrypted with symmetric-key cryptography and the encrypted data is then stored on the smart card. A fuzzy commitment technique is used to link the patient's revocable iris template and the secret encryption key. By utilizing the iris pattern of the smart card holder, this suggested system offers user

authentication and the decryption of healthcare data. The stolen healthcare card cannot be used by an attacker to access the patient's healthcare information or secret key.

An authentication scheme based on a fuzzy commitment scheme using a cancelable finger-vein-based bio-cryptosystem has been proposed in [9]. The proposed bio-cryptosystem maintains both the encrypted form of healthcare data and the biometric template on a smart card to guarantee that biometric data never leaves the card. Additionally, since the biometric template data never leaves the card, the notion of keeping both data on the smart card can prevent data leakage during information exchange or biometric template conversion.

BAMHealthCloud [10] is a cloud-based system for healthcare data management that uses behavioral biometric signatures to guarantee secure e-medical data access. Authentication samples have been trained in parallel using Resilient Backpropagation neural networks on the Hadoop MapReduce framework. The integration of patient medical information with electrocardiography (ECG) data based on location and biometrics has been shown in a cryptographic role-based access control system for electronic health record (EHR) systems in [11].

3. METHODOLOGY

Biometric systems have three common steps.

1. Taking down the chosen person's physiological or behavioral traits along with their name and/or identification number,
2. storing the chosen contents after they have been transformed into a graph or a program code, and
3. Evaluate the user credentials against its database of information to determine whether to permit or refuse access each time when someone tries to log in.

3.1 Fingerprint-based system

At first, the patient gets registered by the doctor using his fingerprint [6]. The patient's basic information, their blood type, blood sugar level, and whether they have any allergies, are included in the registration records.

When a patient sees the doctor, the doctor will scan his fingerprint, and the system will show the patient's data based on that fingerprint pattern. Authenticated data has kept in the database in encrypted form. The AES/MD5 technique is used in this system to encrypt data.

3.2 Facial image-based system

The system is made up of a Raspberry Pi 3 CPU and a webcam for facial recognition. The main control model of this system is the Raspberry pi 3, which is the cheapest and latest version of Raspberry Pi. The LBP and HAAR cascade classifier is used to acquire the face characteristics. For everyone to confirm that they are registered, their acquired characteristics are compared to their learned characteristics using the Arduino IDE, which was developed to program the microcontroller [7]. MySQL database was used to store the information from the medical record in encrypted form. The AES/MD5 technique is used in this system to encrypt data.

3.3 Iris pattern-based system

Iris-based Cancelable Biometric Cryptosystem System [8] consists of two steps i.e., data encryption & decryption. Inputs for the encryption task include the iris image, the encryption key, and the patient's medical record. An encrypted medical smart card is used to store helper data, cryptographic hashes of encryption keys, and encrypted medical information. To retrieve encrypted healthcare information from the smart card, the decryption procedure is performed without supplying an encryption key. Input is limited to the patient's iris picture and the data on their healthcare smart card. As a result of this input data, the decryption key is produced, which then functions to decode the encrypted healthcare data on smart cards.

3.4 Finger vein bio cryptosystem

During the encryption phase of the Finger vein system, the significant features of the finger vein of the user are extracted using the Gabor filter, and the feature vector obtained is converted to binary values. Then the confidential medical data of the user are encrypted using a secret key by the Fuzzy Commitment Scheme [9]. During decryption, similar to the template, query finger-vein characteristics are retrieved and processed. The FCS decoder is then given the query to get the secret key. Key recovery will be successful if the query closely matches the template. It is possible to decrypt medical data by using the obtained secret key.

3.5 Signature-based system

BamHealthCloud is a cloud-based approach for managing a large volume of medical data. The healthcare cloud oversees storing and retrieving this data. It has two elements: a security manager and storage for medical records. Security is managed by a biometric identification agent in the medical data store in the presence of a security manager. In this system, biometric signatures are used for authentication. With the help of a digitizing tablet, a variety of dynamic signature characteristics, such as pen velocity, time spent

No	Title	Techniques	Biometric Data
1	Fingerprint-Based Patient Information System [6]	AES/MD5	Fingerprint
2	Facial Recognition And Verification System For Accessing Patient Health Records [7]	HAAR, LBP	Face image
3	Iris-based cancelable biometric cryptosystem for secure healthcare smart card [8]	AES, IDEA	Iris image
4	Securing Mobile Healthcare Data: A Smart Card Based Cancelable Finger-Vein Bio-Cryptosystem [9]	Artificial Neural Network	Finger vein image
5	BAMHealthCloud: A Biometric Authentication and Data Management System for Healthcare Data in Cloud [10]	Hadoop MapReduce framework using Resilient Backpropagation neural network.	Signature
6	Hybrid Cryptographic Access Control for Cloud-Based EHR Systems [11]	Wavelet-based steganographic technique	ECG

Table 1: Comparison Table

signing, and angles, are recorded. After the key characteristics have been retrieved, the signature is preprocessed. The AI-based model is then trained using this feature dataset, which has been preprocessed and saved in the cloud. The saved model is compared against a user's signature during the verification step to determine if the user is real or not.

3.6 ECG-based system

Personal information from an electronic health record is concealed within the ECG host data using a steganographic technique [11]. Mobile users are verified based on their location and identity information in this approach. Upon accessing the domain server, a medical authority receives the request on behalf of the user. Accordingly, the domain server informs the CSP (Cloud service provider) to allow the transmission of the data requested. Using face biometrics, a user is automatically verified in a domain. In a secure environment recognized by the host network, these two attributes identify the user and confirm its identity.

Here, the EHR information is divided into sections and organized into a tree structure in order to embed it into the system. Then the ECG segments are assigned at random to the items in the EHR based on their indices (I) and ends (E). ECG signal is converted using Haar Transform afterward. Each HER segment has a hash value, and Each patient is assigned a secret key. Using this secret key, coefficients (CD) are rearranged, segment bits are hidden, and each EHR section is encrypted before it is hidden.

Afterward, Haar wavelet decomposition is performed on both CD and CA. This results in the creation of a fresh watermarked section of the document. A watermarked segment is reintegrated into the patient's original ECG signal using the index and end. Each segment is concealed by repeating this procedure. Likewise, the health authority maintains a unique ID for patients requiring retrieval, as well as data like segment indexes and ends, secret sections, and keys. Cloud servers store the patient ID-generated number and the watermarked ECG.

4. COMPARISON

The comparison of various gender recognition approaches using brain images is shown in Table 1.

5. CONCLUSION

Electronic health records have been replacing paper-based medical records in the global healthcare system. Traditional methods of patient identification and user authentication for accessing EHR include cards and passwords [12]. Biological devices collect specific physiological and behavioral traits of an individual and utilize them to identify them later. The biologically distinctive features (such as the face, fingerprint, iris, or voice) of a person are known as biometrics. The core components of a biometric identification system are a cloud-based scanner, software to convert the scanned data and a database for comparing the detected data with enrolled data [13]. In this paper, biometric-based authentication and identification methods for increasing electronic medical data security are discussed. Multi-trait authentication can be used in the future, thus further improving health care security.

REFERENCES

[1] A. A. Azeta, D. A. Iboroma, V. I. Azeta, E. O. Igbekele, D. O. Fatinikun and E. Ekpunobi, "Implementing a medical record system with biometrics authentication in E-health," 2017 IEEE AFRICON, 2017, pp. 979-983, doi: 10.1109/AFRCON.2017.8095615.

[2] https://recfaces.com/articles/types-of-biometrics

[3] https://www.biometricupdate.com/201312/explainer-healthcare-and-medical-biometrics

[4] https://itrexgroup.com/blog/biometrics-in-healthcare-applications-advantages-challenges

[5] O. F. Segun and F. B. Olawale, ‘‘Healthcare data breaches: Biometric technology to the rescue,’’ Int. Res. J. Eng. Technol., vol. 4, no. 11, pp. 946–950, 2017. 2020). https://doi.org/10.1007/s00429-020-02113-7

[6] Vedanti Suhas Mahulkar, Priyanka Babu Kachare, Divya Jain “Fingerprint Based Patient Information System,” in International Journal of Innovative Science and Research Technology. IEEE, pp. 94–98, 2019.

[7] S. Jayanthy, J. B. Anishkka, A. Deepthi and E. Janani, "Facial Recognition And Verification System For Accessing Patient Health Records," 2019 International Conference on Intelligent Computing and Control Systems (ICCS), 2019, pp. 1266-1271, doi: 10.1109/ICCS45141.2019.9065469.

[8] Kausar, Firdous. (2021). Iris-based cancelable biometric cryptosystem for secure healthcare smart card. Egyptian Informatics Journal. 22. 10.1016/j.eij.2021.01.004.

[9] W. Yang et al., "Securing Mobile Healthcare Data: A Smart Card Based Cancelable Finger-Vein Bio-Cryptosystem," in IEEE Access, vol. 6, pp. 36939-36947, 2018, doi: 10.1109/ACCESS.2018.2844182.

[10] Shakil, Kashish & Zareen, Farhana & Alam, Mansaf & Jabin, Suraiya. (2017). BAMHealthCloud: A Biometric Authentication and Data Management System for Healthcare Data in Cloud. Journal of King Saud University - Computer and Information Sciences. 32. 10.1016/j.jksuci.2017.07.001.

[11] U. Premarathne et al., "Hybrid Cryptographic Access Control for Cloud-Based EHR Systems," in IEEE Cloud Computing, vol. 3, no. 4, pp. 58-64, July-Aug. 2016, doi: 10.1109/MCC.2016.76.

[12] https://precisionit.co.in/resources/blog/biometrics-health-care

[13] https://veridiumid.com/biometric-authentication-for-healthcare/

[14] Azeta, Ambrose & Omoregbe, Nicholas & Misra, Sanjay & Iboroma, Da-Omiete & Igbekele, Emmanuel & Fatinikun, Deborah & Ekpunobi, Ebuka & Azeta, Victor. (2019). Preserving Patient Records with Biometrics Identification in e-Health Systems. 10.1007/978-981-13-6347-4_17.

[15] Mason, Janelle & Dave, Rushit & Chatterjee, Prosenjit & Graham Allen, Ieschecia & Esterline, Albert & Roy, Kaushik. (2020). An Investigation of Biometric Authentication in the Healthcare Environment. Array. 8. 100042. 10.1016/j.array.2020.100042.