IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

Digital Health Record System Using Fingerprint Authentication

Anita Shinkar[1], Yash Dhumal[2], Mayur Shinde[3], Vaishnavi Tandale[4], Swarupa Shinde[5]
Assistant Professor[1]
Students[2,3,4,5]
Dr. D. Y. Patil College of Engineering and Innovation, Pune, India

Abstract: *This paper discusses the development and implementation of a Digital Health Record System (DHRS) that will use fingerprint biometric authentication to provide secured accessto health records. Here, the objective remains the same as was mentioned earlier, to enable doctors to access information about patients in an expeditious manner, especially in the event of emergencies such as accidents. The research leads to the conclusion that the system does value the importance of improvement of health and patient care.*

Keywords: Health Records, Fingerprint, Image Processing, EmergencyAccess, Decentralized Data

I. INTRODUCTION

There is a fantastic need for securing electronic access to patient medical records in consideration of the fact that people's lives are increasingly being managed within the digitized healthcare sector. In fact, even in emergency cases, timeconsuming delays in accessing vital patient history sometimes lead to cases of misdiagnosis or otherwise, an adverse outcomein the treatment process. The current Digital Health Record System that utilizes fingerprint biometrics allows for very fast and secure access of a patient's health information, therefore immensely reducing response time in critical accidents or in cases of life-threatening emergencies. This paper reviews the technical and operational viability of such a system. Advanced biometric technology helps the DHRS overcome common challenges of health care providers, such as verification of patient identities quickly and accurately. Traditional methods of patient identification can be cumbersome and prone to errorsin those high-pressure situations where even fractions of a minute are vital.

Motivation

The main motivation behind the project is the need for immediate access to patients' medical history in emergency situations. Often, important medical information is not immediately available to doctors or medical professionals, which can lead to incorrect or delayed treatment. The integrationof multiple databases offers the capability to access health information records from a variety of healthcare organizations and, simultaneously, helps ensure that strong security measures are in place. Biometric technology provides an efficient and secure way to establish the identity of patients before treatment, which allows doctors to make quicker and betterinformed action.

Objectives

- **Fast and Secure Patient Identification:** A fingerprintbased system designed for secure rapid patient identification.
- **Availability of Immediate Access to Medical Records:**Ensure that there are readily retrievable patient health records with background history and current treatments in case of emergencies.
- **Crime Investigation:** It can enable forensic teams to compare evidence found at the crime scene with biometrics from known individuals, hence allowing investigatorsto cross-refer and identify potential suspects or details of missing persons which helps them to apprehend criminalsfaster or locate missing people.
- **Decentralized Record Management:** Store the patient data in a decentralised way for its multihospital and multienvironmental accessibility while ensuring that one does not succumb to various security and privacy breaches.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

- **User-Friendly Interface Design:** Design an intuitive, user-friendly interface that's highly navigable and brings quick access to patient records for healthcare professionals.
- **Real-time update:** The record of such patients would automatically be updated real-time. So that any information related to the patient and even changing the medical status, treatment plans, or any new informationis reflected immediately within the system.

II. LITERATURE SURVEY

Identity Privacy Preserving Biometric-Based Authentication Scheme for Naked Healthcare Environment, 2017-Written by Tanesh Kumar, An Braeken, Madhusanka Liyanage, and Mika Ylianttila, the paper introduces a biometric-based authentication system for hospitals with privacy-protecting aspects that don't rely on external gadgets. The system is common-attack resistant and offers a healthy solution for healthcare environments. It also states the need for lightweightand low complexity security solutions that can be practically implemented in real-world healthcare settings.
Biometric Authentication in Health Care Sector: A Survey, 2019-Authored by Kalsoom Fatima, Sumbal Nawaz, and Sobia Mehrban, the present paper describes different biometric methods used for healthcare security. The presented method indicates that the proper implementation of these systems is possible as it will protect the patient record; besides, the best security effect will be achieved in combination with more than one biometric technique. However, there is a flow of significant challenges that lack standardization, high cost alongwith complex technicalities may pose constraints for adopting multi-modality biometric systems in healthcare settings.
Evaluation of Electrocardiogram Biometric Verification Models Based on Short Enrollment Time on Medical and Wearable Recorders: A Comparison Study with Random Forest Classifier and Deep Learning (2021)-The paper, undertakenby Hazal Su Bıçakcı, Marco Santopietro, and Richard Guest, investigates the biometric verification models that can be developed based on the ECG signals received from wearable and medical devices. The authors presented a pipeline for the authentication of ECG-based authentication that successfully would offer biometric verification with only heart data. However, the scope is limited because it focuses just on heart biometrics instead of full-body authentication that may limitits broader applicability in healthcare.
[4]A Touch-Free Biometric Approach for Electronic Healthcare Database System using SAML 2021-Written by Devi T. Ramachandra A. and Deepa N., it provides a biometric system designed specially for an electronic health care database for patients affected by COVID-19. SAML is incorporated for mobile applications to allow access and control in a safe way, so giving a touch-free system. It is limited to this application due to not being versatile enough for other disease types since the whole system focuses around the health care management of COVID-19.
[5]Medical Systems Data Security and Biometric Authentication in Public Cloud Servers (2023)-Nelson Santos, Bogdan Ghita, and Giovanni Masala proposed a system for storing and safeguarding health information on the cloud with a data fragmentation technique that solves user identity management using multimodal biometrics. This system solves two critical issues: the security of health data stored in cloud servers and digital identity recognition issues. Thus, the paper focuses on the relevance of cloud security in a health system while using biometric data for verification in general and for accessing thedata.

Feasibility

The feasibility of using fingerprint biometric authentication with the DHRS is appraised:

- **Technical Feasibility:** The technology used in DHRS relies on a well-established and mature technology: that of biometric fingerprint which is as trustworthy in patient identification. Those technologies capable of integrating biometric systems with health-care databases and decentralized storage systems are technically feasible via existing hardware and software solutions. Furthermore, sensitive information about patients can be safely handledthrough deployment of encryption and privacy protocols.
- **Operational Feasibility:** The system will simplify operations in health-care facilities as patient information is accessed much quicker, particularly in emergency cases. There is nothing complex about training health-care professionals on fingerprint scanner usage and access ofpatients' records since the biometric system is quite userfriendly. Furthermore, since the new system complementsexisting healthcare infrastructure, a disruption to the current workflow is completely minimal.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

- **Economic Feasibility:** It lessens the overhead costs associated with administrative overheads relevant to manual patient data extraction and tries to minimize the wrong identification of patients. The cost justification is highly robust in terms of operational saving along with better patient care outcomes while its decentralized storage curtails infrastructure expenses pertaining to centralized data centers.

III. METHODOLOGY

Generally, when structured development is concerned, designing the DHRS making use of fingerprint biometric authentication involves the following key steps:

- **System Design:** Here, the system architecture is designed in such a manner that a biometric fingerprint scanner and a verification module are placed with a decentralized patient records database. The design here focuses on how to securely link patient data to biometric identifiers so that quick access can be established in case of emergencies.
- **Biometric Data Collection:** Collect biometric data about the patient through fingerprint, which occurs at the time of registration. The fingerprint data is encrypted and stored on decentralized databases for privacy compliance and security.
- **Verification module:** There's a biometric verification module, that verifies the fingerprint data provided by the patients with the already stored encrypted fingerprint data. On successful verification, it retrieves the stored records of the patients and displays it to the healthcare providers.
- **Decentralized Storage:** Patient data stored via decentralized storage, therefore enabling wide access to multiple institutions involved in healthcare without compromising data security and privacy.
- **Testing and Validation**: The system was tested in simulated healthcare environments in order to test the effectiveness of biometric verification and retrieval of the data, including all the validation measures to test the security checks and response times from integration with existing healthcare information systems.
- **Security and Privacy:** This can be achieved with encryption of biometric data, role-based access controls, and strict health data protection regulations to ensure patient data confidentiality, security, and protection from unauthorized access.

This methodology would ensure that the DHRS is secure, efficient, and suitably deployable in real-world medical environments.

Algorithm

Fingerprint Minutiae Algorithm: It identifies minutiae points in a fingerprint; that is, ends of ridges, bifurcations, etc. The extracted minutiae points are matched with the fingerprint database of other people for identification or verification purposes. Based on the conditions such as quality of fingerprints and environmental conditions, the proposed algorithm generally offers an accuracy of 90-98 percent. The algorithm is widely implemented in authentication biometric systems.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

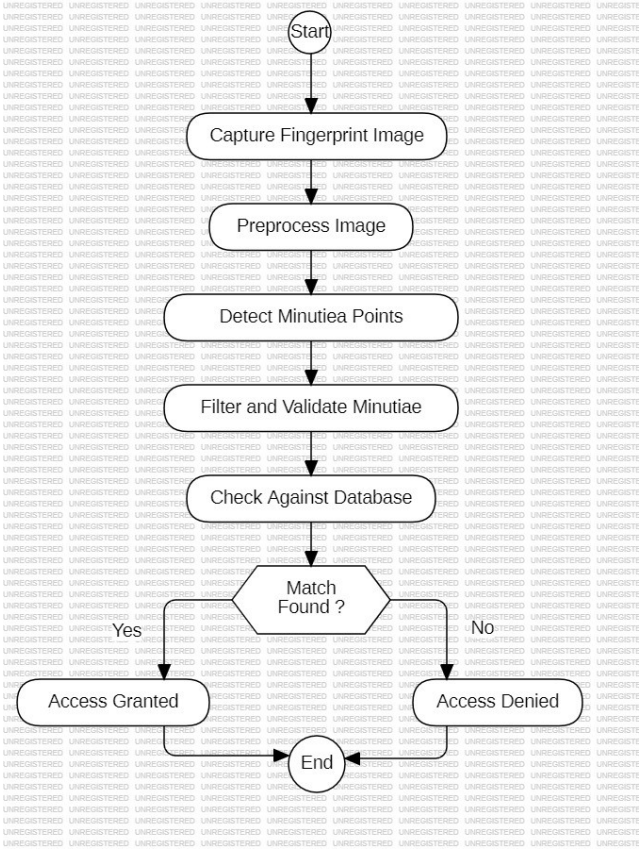

Fig. 1. Flowchart of Fingerprint Minutiae Algorithm

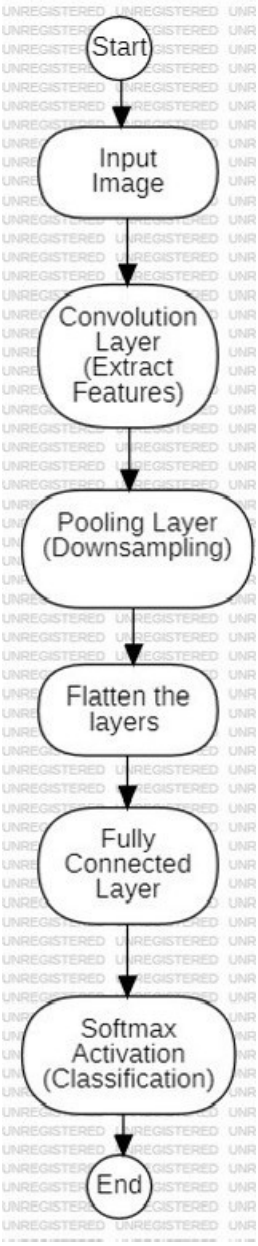

Fig. 2. Flowchart of Convolutional Neural Networks

Convolutional Neural Networks (CNN):CNNs are a type of deep-learning model designed specifically for image recognition and classification. The data processed within such models is passed through hierarchical layers that might automatically learn the detection of distinct features at different levels, including edges, textures, and patterns. CNN can classify images using convolutional layers, pooling layers, and fully connected layers. With datasets like ImageNet, CNN achieves over 95 percent accuracy in most cases. Several architectures that are well-known are ResNet, VGG, and Inception.

K-means Clustering for Image Segmentation:K-means clustering is the unsupervised learning algorithm used for allocating an image into different groups on the basis of similarity among the pixels. The algorithm groups an image into K clusters by minimizing the variance between the elements in the cluster, and thus pixel similarity involves

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

assigning them to the nearest one based on the features, like color intensity. It is widely applied in the image segmentation and can attain 70-80 percent of accuracy according to the complexity levelof the image.

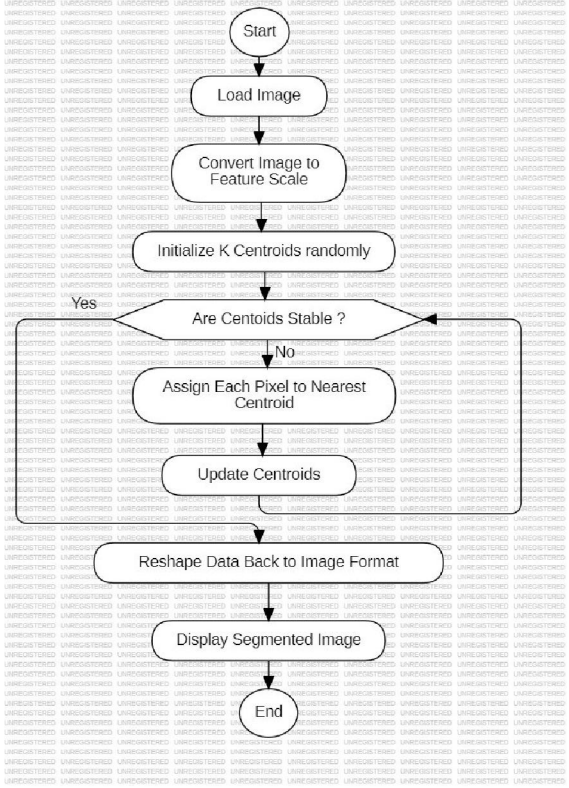

Fig. 3. Flowchart of K-means Clustering

IV. ARCHITECTURE

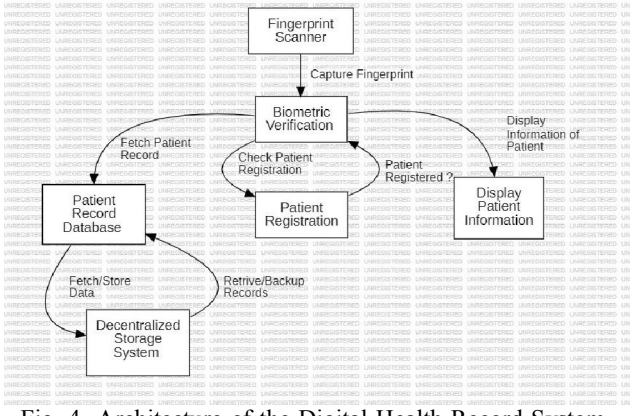

Fig. 4. Architecture of the Digital Health Record System

- **Capture Fingerprint:** It captures the fingerprint of thepatient.
- **Verify Patient Registration:** The fingerprint is then sentto Biometric Verification module where it checks if the patient exists within the Patient Registration database.
- **Retrieve Patient Record:** In case the patient is registered,it retrieves all the medical records of the respective patientfrom the Database of Patient Records.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

- **Display Information:** All the medical data is displayed through Display Patient Information module to the doctors.
- **Fetch/Store Data:** The Patient's data will always be safely stored and backed up to ensure accessibility and security of data in the Decentralized Storage System.

V. COMPARISON WITH AYUSHMAN BHARAT SCHEME

Ayushman Bharat Scheme	Digital Health Record System
More time consuming	Less time consuming
It does not provide security	It provides more security
User verification can be done only one time	User verification can be done multiple times
It stores only emergency details	It stores all patient-related records
It stores the records of 30+ patients	It stores records of all patients
This scheme has limited scope	The scope is not limited; records can be used at anyMedical Centre
It does not cover all health-care facilities	It covers all healthcare facilities
Sometimes fraud can occur as the patient can providewrong information	Fraud cannot occur in this system, as patients with certain diseases must visit the hospital where records can be maintained

VI. CONCLUSION

Fingerprint biometric authentication for a Digital HealthRecord System will greatly advance how health practitioners access patient data, especially in an emergency. The healthcare providers may seek to retrieve critical health data instantly, thus eliminating possible delay times that could be life threatening in emergency situations. Using biometrics, like fingerprints, guarantees safe and unique identification of patients. Fingerprints are very unique and difficult to replicate, meaningan added degree of security unmatched to what passwords or PIN codes can do. It makes it even more secure to access sensitive data related to the patients, thus reducing the risksof unauthorized access or data breaches. Also, because such systems authenticate identity without a physical paper attached to the patient, health records can easily be accessed at a moment's notice in case the patient has lost consciousnessor is incapable of verbal communication

REFERENCES

[1] Kumar, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2017). Identity Privacy Preserving Biometric Based Authentication Scheme for Naked Healthcare Environment. Journal of Medical Systems, 41(5), 1-12.
[2] Fatima, K., Nawaz, S., & Mehrban, S. (2019). Biometric Authentication in Health Care Sector: A Survey. IEEE Access, 7, 145307-145321.
[3] Bıc¸akcı, H. S., Santopietro, M., & Guest, R. (2021). Evaluation of Electrocardiogram Biometric Verification Models Based on Short Enrollment Time on Medical and Wearable Recorders. IEEE Transactions on Biomedical Engineering, 68(1), 323-331.
[4] Ramachandra, D. T., & Deepa, N. (2021). A Biometric Approach for Electronic Healthcare Database System using SAML A Touch Free Technology. International Journal of Innovative Technology and Exploring Engineering, 10(12), 331-335.
[5] Santos, N., Ghita, B., & Masala, G. (2023). Medical Systems Data Security and Biometric Authentication in Public Cloud Servers. IEEE Transactions on Cloud Computing.
[6] Panda, S., & Mahapatra, D. R. (2021). A Survey on Biometric Authentication Systems in Healthcare. International Journal of Computer Applications, 177(11), 1-6.
[7] Wang, Y., & Li, X. (2020). A Survey of Biometric Authentication Systems for Healthcare. Journal of Healthcare Engineering, 2020.
[8] Zhang, Y., & Wang, J. (2019). An Efficient and Secure Biometric Authentication Scheme for Electronic Health Records. Journal of Medical Systems, 43(4), 1-9.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, November 2024

[9] Nishanthi, S., & Jothi, S. R. (2021). A Review on Biometric Authentication for Healthcare Systems. International Journal of Healthcare Information Systems and Informatics, 16(3), 1-16.
[10] Chaudhary, S. K., & Tiwari, P. (2022). Advanced Biometric Techniques for Secure Healthcare Systems: A Review. Journal of King Saud University Computer and Information Sciences.
[11] Mhase, A., Suryawanshi, S., Vaishnav, T., Malphedwar, L. (2022). Diabetes Prediction Using Machine Learning. *International Journal*, 16(4), 1-12.
[12] Borude, A., Kolhe, S. N., Patil, H. R., Malphedwar, L. (2020). CNNBased Lung Disease Detection. *International Journal*, 5, 45-56.
[13] Shinkar, A., Devale, P. (2007). Contrast Enhancement Technique for Medical Images. *Proceedings: NCSPA-07*, DYPIET, Pune, India.