Biometric-Based Patient Health Care System

Prof. Pritam Ahire[1], Nikita Patil[2], Pranita Raut[3], Nikita Sartape[4], Dr. Vilas Deoatare[5]

Department Computer Engineering [1,2,3,4]

Department of Electronics & Telecommunication [5]

Nutan Maharashtra Institute of Engineering and Technology, Pune [1,2,3,4,5]

Abstract **-** Accurate identification of patients remains not less than a headache in many countries in the sub-Asian region. Nonetheless, accurate patient identification is still essential to providing high-quality, safe healthcare. The following explanations help to explain why patient identification processes in Sub-Asian hospitals are flawed: Larger hospitals tend to have decentralized patient administration because the adoption of a degree of financial and managerial autonomy for clinical departments has encouraged the proliferation of redundant administrative patient management systems (every department wanting to handle its own bookkeeping). Patients so obtain ID numbers and medical records that are department-specific. Furthermore, it should be noted that the lack of a master patient index (MPI) is a general rule, meaning that there are no central patient identification systems that make use of the department's current patient information.

Keywords- patients, healthcare, master patient index (MPI), biometric authentication in healthcare, patient records

I.INTRODUCTION

Many hospitals now use encounter-centered filing systems rather than patient-centered ones. Patient records are classified in the filing system by date of last encounter. If the patient no longer remembers the time of this last meeting, it becomes very difficult to retrieve their records. Weak patient identifiers are commonly used: the most commonly used identifiers are patient name, date of birth, or department-specific internal medical record number. There are various problems with these types of identifiers:

1. Many patients do not know their exact date of birth. Even the year of birth can be approximate.

2. Patient names are unstable: newborns are often given temporary names that change later. Some patients don't even know how to write their name correctly.

3. As explained above, a patient may have multiple medical record numbers in a medical facility.

Patients often cannot remember all of these record numbers or even retain them. some traces. National personal identification tools could certainly significantly improve patient identification practices especially in sub-Saharan healthcare facilities. Unfortunately, very few countries are able to implement accurate and comprehensive identification procedures to ensure unambiguous identification of their citizens from the day they are born. In many places there are still fragmented identification systems covering at least part of the population: At age 16, Rwandans receive a national identity card that contains a machine-readable identification code that can be easily used for medical record identification purposes [7]. However, children under 16 years of age who are not eligible for this procedure still make up a very significant portion of the patient population. A comparable circumstance exists within the Law based Republic of Congo, where all grown-ups qualified to vote in legislative issues have a unique distinguishing proof number within the frame of a “voting card.” Once more, children and other ineligible citizens such as foreigners, uprooted people, military staff, and the rationally debilitated are cleared out behind. In the realm of healthcare administration, efficient and accurate patient identification stands as a cornerstone for effective medical care delivery. However, the existing landscape of patient record management often grapples with significant challenges, particularly evident in the prevalence of encounter-centered filing systems over patient-centered ones. Encounter-centered systems, while offering some organizational benefits, introduce complexities that hinder seamless record retrieval and patient care continuity. Records indexed solely by the date of last encounter render retrieval cumbersome, especially when patients fail to recall these specific dates. Compounded by weak patient identifiers such as name, date of birth, or facility-specific record numbers this approach becomes increasingly unreliable. The shortcomings of traditional identifiers are multifaceted: date of birth can be approximate or unknown to patients, while names may change or be misspelled, particularly in cases of newborns or individuals with limited literacy. Moreover, within a single medical facility, patients may possess multiple record numbers, exacerbating confusion and impeding effective record linkage. Addressing these challenges necessitates a holistic approach, one that extends beyond local healthcare systems to encompass national identification frameworks. While some countries have made strides in this regard, implementing comprehensive and accurate identification procedures from birth onwards, many regions still grapple with fragmented systems.

II. LITERATURE SURVEY

A new cloud-based granular medical information access control framework has been introduced to address the security challenges and reciprocity issues of the cloud [1].

A proxy-based approach for end-to-end communication between the IoT-enabled living systems was proposed to challenge the real world applications. A portable electric aid device was designed specifically for the blind people in which ultrasonic range finders are mounted on the belt to find the obstacles present in the user’s way and to direct the blind people. This ID card is the first proof of identity for the election. Students with a valid ID card can only participate in the election process. During the election process, students place the RFID card on the reader card. To ensure that the card

belongs to the same student who owns it, a second level of authentication is used

This article describes a simple and secure voting method using biometrics. The main goal is to increase the flexibility, security, reliability, scalability of the model and reduce the time to publish results. Fingerprint module is used here for voting. Fingerprint detail of a person is already stored in government database [2].

Elections are an important feature importance of democratic institutions. To make students understand the concepts of democratic structures and instill quality leadership in them, elections are held in schools and higher educational institutions. The student council is the largest student body at an educational institution. Through the Student Council, students express their opinions and complaints against the system. Technology has brought about radical changes in almost every field; The election process is no exception to this rule. People rely on technology to do their work easily, quickly and accurately.

By allowing electronic blood pressure monitors to communicate via Bluetooth, an Android application was developed to record data such as systolic blood pressure, diastolic blood pressure and heart rate. This app makes it easy for you to transfer recorded data using any mobile device [6] [10] [13]. This data is then recorded, anomalies are detected, and messages are transmitted to everyone.

Kolici et implemented a comparison of experimental results for different scenarios. Web real-time communication (WebRTC) was proposed by Sundholm et al who mainly focused on the secure transmission of multiple simultaneous data streams in an efficient manner.

A real-time application is presented with a distributed thread environment for healthcare IoT [11] [13]. When the observed person moves out of range, the data will be saved to the local server and reported later.

The conventional paper ballot system, although simple, is not transparent and error-free. To overcome the limitations of conventional paper ballots, an authenticated voting system (AVM) was introduced. It uses two levels of authentication namely radio frequency identification (RFID) and

In-discussion voting system works for up to three candidates for the same position. If there are multiple locations, a separate voting machine must be used for each location. To speed up the voting process when there are more than thousands of students, the entire university is logically divided into several blocks, and the number of required AVM units is equal to the number of blocks, and each block contains a cabin-level operator (BLO). Student fingerprint data will be taken into the school database. To do this, an Internet connection is required, preferably Wi-Fi.

In recent days, various IoT systems have been developed for health monitoring systems. Wang et al. designed an IoT system compatible for medical devices with multiple communication standards. A resource-based data retrieval method (UDA-IoT) was proposed by Xu et al. for information-intensive healthcare applications [15] [16] [19].

Peer-to-peer (P2P) technology and IoT have been combined into a medical system called smart box for patient control.

Article title: Design and development of a low-investment smart hospital using the Internet of Things through innovative approaches [4] [5] [9].

Galileo Card is an IoT-based Device with an integrated medical platform to analyze electrocardiogram (ECG) signals and algorithm-based heart function is monitored [21].

In the market, very few IoT medical wearable devices have been introduced, which help improve patient mobility. However, security threats and some limitations also arise when using wearable medical devices. When we started looking at lightweight IoT devices, using existing databases, diseases were predicted. But despite these predictions, the problem lies in the storage of databases and the analysis using those databases.

Level in the second level, student biometrics are accepted using the fingerprint scanner available on the voting machine. This fingerprint is compared with the fingerprint stored in the database. If both fingerprints match, only the student will be allowed to vote. The necessary details are stored in the university database and votes are stored in the voting machine itself.

Voting machines are connected to a computer that contains an entire database of people eligible to vote. The touch screen is used because it is user-friendly. The printer is used to obtain authentic probes. The GSM module is used to send the results to the respective authority [21].

Biometrics [14]. During the admission process, each student's biometrics are recorded and stored along with other necessary documents. Once the admission process is complete, an RFID-based ID card will be issued to each student.

III.PROBLEM DEFINATION

We are introducing a Fingerprint Based Medical System for efficient access to patient records using biometric identification technology. This system enables quick retrieval of past health records through fingerprint recognition, streamlining healthcare processes and improving patient care.

IV. PROPOSED METHODOLOGY

Doctors can log in to the system with a fingerprint.

After logging in, the doctor will have two options: update information or view patient information.

Patient's finger will be retained for identification; we will apply KNN algo to match the fingerprint.

If this is a new entry, personal information will be added and two additional fingerprints will be stored

If this is an update as a profile, they will be updated daily, the patient's fingerprint will be authenticated to confirm

K-nearest neighbor algorithm

In pattern recognition, the k-nearest neighbor (k- NN) algorithm is A non-parametric method is used for classification and regression. In both cases, the input is the k closest training examples in the feature space. The results depend on whether k-NN is used for classification or regression.

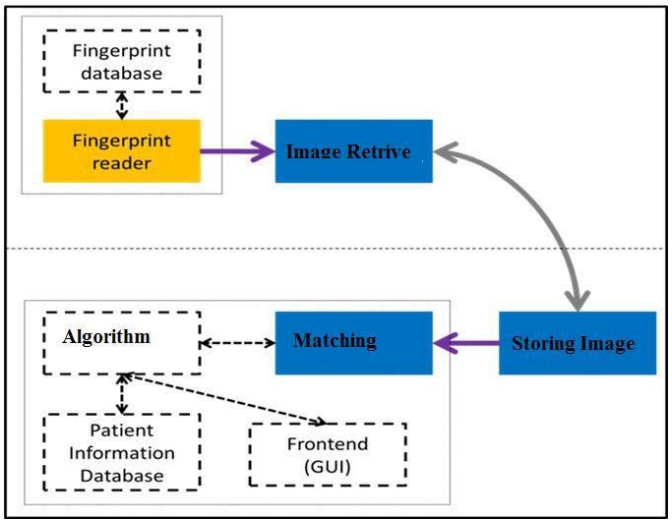

Fig 1. System Architecture

Module 1: Registration and Login for patient and Doctor
Module 2: Update Record or view record
Module 3: Fingerprint Matching
Module 4: Report Generation

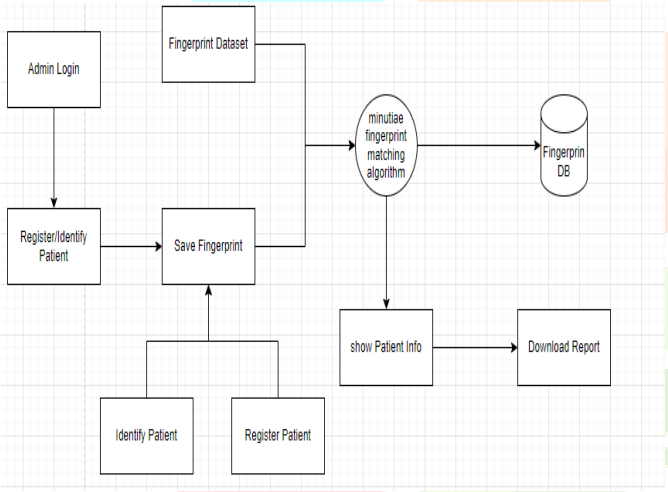

Fig 2. Flowchart

This is a system for patient registration and verification using fingerprint recognition technology. The system streamlines the process by registering new patients and verifying existing ones through fingerprint matching algorithms. Upon admin login, new patients are registered by capturing fingerprints and personal details, stored securely in a database. For verification, the system matches fingerprints using minutiae and KNN algorithms, providing instant alerts upon successful verification. Patient reports can be downloaded as needed. This system enhances efficiency, accuracy, and security in healthcare institutions.

VI. ADVANTAGES

Accurate patient identification: Biometric-based patient healthcare systems offer unparalleled accuracy in patient identification. Biometric data, such as fingerprints, iris scans, or facial recognition, is unique to each individual, eliminating errors or confusion associated with traditional identifiers like names or dates of birth. This accuracy is crucial for preventing medical errors, ensuring patients receive appropriate treatments, and enhancing overall patient safety.

Advanced security: Biometric data is inherently difficult to fake or manipulate, enhancing the security of patient information. Unlike passwords or ID cards, which can be stolen or shared, biometric identifiers are intrinsic to an individual and cannot be easily replicated. This reduces the risk of identity theft or unauthorized access to medical records, ensuring robust patient privacy and data security. Additionally, biometric systems often employ encryption and other security measures to further protect sensitive data, providing an additional layer of defense against cyber threats.

Efficiency: Biometric identification systems streamline administrative processes by automating patient identification, reducing the time and effort required for staff to manually search for patient records. This efficiency improvement translates to enhanced healthcare delivery and patient care. With biometric authentication, healthcare providers can quickly access relevant patient information, make more informed decisions, and provide timely interventions, ultimately improving patient outcomes and satisfaction.

Integration with existing systems: Biometric systems can seamlessly integrate with existing electronic health record (EHR) systems, facilitating interoperability and data sharing between different healthcare providers and systems. This integration enhances continuity of care and enables comprehensive patient management. By connecting biometric authentication with EHR platforms, healthcare professionals can access a patient's complete medical history, including diagnoses, medications, allergies, and treatment plans, regardless of where the patient received care. This holistic view of patient information enables more coordinated and personalized care, leading to better health outcomes and reduced healthcare costs.

Patient convenience: Patients no longer need to remember or carry cards or identification numbers, as their biometric data serves as a unique identifier. This is particularly advantageous for individuals who may have difficulty remembering or accessing traditional forms of identification. Moreover, biometric authentication is quick and easy, requiring only a simple scan or touch, which reduces wait times and enhances the overall patient experience.

VII. EXISTING SYSTEM DISADVATAGES

1. The predominant use of encounter-centered filing systems in hospitals is a major disadvantage.
2. Weak patient identifiers, such as name, date of birth, or facility-specific record numbers, contribute to the inefficiency of the current system.
3. Patients often struggle to provide accurate or consistent information, leading to difficulties in accessing their records and maintaining continuity of care.

4. Encounter-centered systems organize patient records based on the date of the last encounter, which can be problematic when patients cannot recall specific dates.
5. Patient identifiers like date of birth may be approximate or unknown, while names can change or be misspelled, further complicating record retrieval.
6. Within a single medical facility, patients may have multiple record numbers, causing confusion and hindering accurate record linkage.
7. This fragmentation of patient records complicates coordination among healthcare providers and undermines the continuity and comprehensiveness of patient care.
8. Overall, the existing encounter-centered filing systems, coupled with weak patient identifiers, result in inefficiencies, inaccuracies, and challenges in managing patient records within healthcare facilities.

VIII.APPLICATION

Patient Identification: Biometric systems play a crucial role in accurate and secure patient identification throughout various healthcare processes, including registration, admission, and medical consultations. By capturing unique biometric markers such as fingerprints or facial features, healthcare facilities can reliably authenticate patients' identities, reducing the risk of medical errors and ensuring the right care is delivered to the right individual.

Access Control: Authentication biometrics offer robust access control measures, particularly in safeguarding sensitive areas of healthcare facilities. For instance, biometric authentication can restrict access to medication storage rooms, ensuring only authorized personnel can handle and dispense medications. Similarly, access to electronic records systems containing sensitive patient information can be tightly controlled using biometric authentication, enhancing data security and privacy. Medication Administration: Biometric verification integrated into medication delivery systems enhances medication safety and accuracy.

Telemedicine Security: Biometric authentication plays a vital role in bolstering the security of telemedicine platforms, especially during virtual consultations. By verifying the identities of both patients and healthcare providers through biometric scans, telemedicine platforms can mitigate the risk of unauthorized access, protect patient privacy, and maintain the confidentiality of medical discussions and information exchanged during virtual appointments.

Clinical Trials Integrity: Biometric systems are instrumental in verifying the identities of participants in clinical trials, safeguarding the integrity and accuracy of research data. By capturing biometric data from study participants, researchers can ensure that each individual's involvement in the trial is accurately tracked and documented. This helps maintain the credibility and reliability of clinical trial results, ensuring that findings accurately reflect the effects of investigational treatments or interventions.

Emergency Response: Biometric identification systems can expedite emergency response efforts by quickly identifying patients in critical situations. In emergencies, such as mass casualty incidents or natural disasters, biometric data can rapidly authenticate patients' identities, enabling healthcare providers to access pertinent medical information, prioritize treatment, and coordinate care more effectively.

Blood Donation Management: Biometric systems can streamline the blood donation process by accurately identifying donors and tracking their donation history. By linking biometric identifiers to donor profiles, blood donation centers can ensure the safety and traceability of donated blood units, reducing the risk of transfusion-related complications and enhancing blood supply management.

Patient Consent Management: Biometric authentication can enhance patient consent management processes, particularly in healthcare settings where obtaining consent for treatment or procedures is critical. By requiring biometric verification for consent documentation, healthcare facilities can ensure that patient consent forms are accurately linked to the correct individuals, reducing the risk of consent-related disputes or legal issues.

Healthcare Fraud Prevention: Biometric systems serve as powerful tools in combating healthcare fraud and identity theft. By implementing biometric authentication for patient registration and insurance claims processing, healthcare organizations can verify the identities of patients and providers, detect fraudulent activities, and prevent unauthorized access to healthcare services and resources.

Long-Term Care Facilities: Biometric systems can enhance security and access control in long-term care facilities, such as nursing homes or assisted living centers. By using biometric authentication for resident check-in/out, medication administration, and access to resident rooms or common areas, these facilities can ensure resident safety, prevent unauthorized entry, and maintain accurate records of staff activities.

IX. CONCLUSION

In our project, fingerprint verification stands as a cornerstone in safeguarding transmitted medical information, ensuring data integrity, and upholding patient confidentiality. By utilizing biometric technology, particularly fingerprint recognition, we establish a robust authentication mechanism that fortifies the security of patient data throughout its transmission and storage. Patient data stored within the hospital's fingerprint database not only benefits from

enhanced security measures but also enjoys global accessibility. Through seamless connectivity and interoperability, healthcare providers worldwide can securely access patient records, enabling informed decision-making and coordinated care delivery regardless of geographical boundaries. Moreover, the implementation of fingerprint verification not only bolsters data security but also streamlines administrative processes, reduces errors, and enhances overall efficiency in healthcare delivery. By automating patient identification and record retrieval, healthcare professionals can devote more time and attention to direct patient care, ultimately improving patient outcomes and satisfaction. As we embrace the future of healthcare technology, our commitment to leveraging biometric solutions remains steadfast. By continually refining and innovating our biometric authentication systems, we aim to set new standards for patient data security, accessibility, and usability in healthcare settings. Through collaboration, innovation, and a steadfast dedication to patient-centric care, we can harness the power of biometrics to transform the healthcare landscape and improve the lives of patients worldwide.

X. FUTURE SCOPE

Looking forward, the future of biometric medical technology, fueled by advancements in machine learning, holds significant promise. Progress in sensor technology will facilitate the development of smaller, more adaptable sensors capable of capturing a diverse range of biometric data. The integration of these sensors with the Internet of Medical Things (IoMT) offers the potential for seamless data exchange across healthcare platforms. Artificial intelligence will play a crucial role in forecasting health outcomes, facilitating early disease detection, and customizing personalized treatment plans. However, it is essential to address ethical, legal, and regulatory considerations to protect patient privacy and rights. Adopting a user-centered design approach will enhance the user experience and accessibility of these technologies. Collaborative efforts across disciplines will drive innovation, and the application of these technologies can help reduce healthcare disparities and promote global health equity.

REFERENCES

[1] Barber B. Data and patient security: an overview, International Journal of Medical Informatics, 49(1), p. 19-30., 1998

[2] Pritam Ahire , Aspect based Sentimental Analysis of Medical data, Lemmas, LSTM, IJCRT, ISSN:2320- 2882, Vol 8, Issue 5, 5 May 2020

[3] Changrui Xia, Arthur Yu, Medical smart card system for patient record management, New Science magazine. 2006.

[4] Pritam Ahire , Aspect based Sentimental analysis of Medical data Lemmas, LSTM, IJRE, ID- IJREV1I29, Vol-1 Issue-II, January 2020

[5] Riazulislam, Daehankwak, M.H.K.M.H., Kwak, K.S.: The Internet of Things for Healthcare: A Comprehensive Survey. In: IEEE Access (2015).

[6] K.R. Darshan and K.R. Anandakumar, "A comprehensive review of the use of Internet of Things (IoT) in healthcare," in Proc. International Conference on Emerging Research in Electronics, Computers and Technology, 2015.

[7] S.H. Almotiri, MA Khan and MA Alghamdi. Mobile health system (m-health) in the context of IoT. 2016 IEEE 4th International Conference on the Future of Internet of Things and Cloud Workshop (FiCloudW), pp. 39-42, August 2016.

[8] Gulraiz J. Joyia, Rao M. Liaqat, Aftab Farooq and Saad Rehman, Internet. of Medical Things (IOMT): Applications, benefits and future challenges in healthcare, Journal of Communications Vol. 12, No. 4, April 2017.

[9] K. Perumal, M. Manohar, Survey on the Internet of Things: Case Studies, Applications and Future Directions, in the Internet of Things: These New advances and applications reviewed, Springer International Publishing, (2017) 281-297.

[10] P. Rizwan, K. Suresh. Low investment smart hospital design and development using Internet of Things through innovative approaches, Biomedical Research. 28(11) (2017).

[11] Shubham Banka, Isha Madan and S.S. Saranya, Smart Healthcare Monitoring using IoT. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 15, p. 11984-11989, 2018

[12] Internet of Things (IoT): Number of Connected Devices Worldwide From 2012 to 2020 (in billions).

[13] M. Hussain, A. Al-haiqi, A. A. Zaidan, and B. B. Zaidan, "The rise of keyloggers on smartphones: A survey and insight into motionbased tap inference attacks," Pervasive Mob. Compute., 2015.

[14] S.H. Almotiri, M. A. Khan, and M. A. Alghamdi. Mobile health (m- health) system in the context of iot. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pages 39–42, Aug 2016.

[15] V. Smejkal, L. Sieger, J. Kodl, D. Novak, and J. Schneider, "The dynamic biometric signature - Is the biometric data in the created signature constant" Proc. - Int. Carnahan Conf. Secure. Technol., vol. 2015-Janua, pp. 385–390, 2016.

[16] M. Choi and R. E. O. Paderes, "Biometric Application for Healthcare Records Using Cloud Technology," Proc. - 8th Int. Conf. Bio-Science Bio-Technology, BSBT 2015, pp. 27–30, 2016.

[17] K.R. Darshan and K.R. Anandakumar, "A comprehensive review on usage of internet of things (IoT) in healthcare system," in Proc. International Conference on Emerging Research in Electronics, Computer Science and Technology, 2015.

[18] Gulraiz J. Joyia, Rao M. Liaqat, Aftab Farooq, and Saad Rehman, Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain, Journal of Communications Vol. 12, No. 4, April 2017.

[19] K. Perumal, M. Manohar, A Survey on Internet of Things: Case Studies, Applications, and Future Directions, In Internet of Things: Novel Advances and Envisioned Applications, Springer International Publishing, (2017) 281-297.

[20] Pritam Ahire , Predictive and Descriptive Analysis for Healthcare Data, A Hand book on Intelligent Health Care Analytics Knowledge Engineering with Big Data"

https://www.wiley.com/enus/Handbook+on+Intelligent+H ealthcare+Analytics%3A+Knowledge+Engineering+with +Big+Data-p-9781119792536 Published by Scrivener Publishing, Wiley Group,2021

[21] Daesung,Moon,Yong Wha,Chung,Sung, Bum Pan, Jin Won Park, Integrating fingerprint verification into smart card-based healthcare information system intelligence, Computer methods and programs in medicine, 81 (1), pp.66-78.2006