WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Biometric Authentication Based Patient Database Management System and Prescription QR Generator

Narayanan.C[1], Krishna Priya. S[2], Arun Pandiyan M[3], Arunkumar. A[4], Kevinkumar .X[5].

Professor[1], Assistant professor[2], UG Student[3,4,5]
Dhanalakshmi Srinivasan Engineering College
dsec.krish17@gmail[2], arunofficial2k20@gmail.com[3]

ABSTRACT—

In the contemporary healthcare landscape, the management of patient data poses significant challenges in terms of security, efficiency, and accessibility. To address these challenges, this project presents a novel solution: a Fingerprint Authentication-Based Patient Database Management System (FAPDMS). FAPDMS leverages the unique biometric characteristics of fingerprints to authenticate users, offering a highly secure method for accessing and managing patient records. The system architecture comprises three main components: Fingerprint enrollment, secure database management, and real-time authentication. The fingerprint enrollment process involves capturing and storing the unique fingerprint patterns of patients and healthcare providers. These fingerprints serve as the primary identifiers within the system, eliminating the need for traditional authentication methods such as passwords or PINs. The secure database management component ensures that patient records are encrypted and stored in a centralized database, accessible only to authorized personnel. Access to patient data is granted solely through fingerprint Authentication, mitigating the risk of unauthorized access or data breaches. One of the key advantages of FAPDMS is its real-time authentication feature, which enables healthcare professionals to access patient records swiftly during consultations and treatments. By simply scanning their fingerprints, users can retrieve relevant medical information, facilitating informed decision-making and improving the efficiency of healthcare delivery. recognition.

Keywords: Patient data management, Security, Efficiency, FAPDMS, Real-time authentication, Healthcare professionals

1. INTRODUCTION

In the digital era, the healthcare sector is witnessing a paradigm shift in the way patient data is managed and accessed. With the proliferation of electronic Health records (EHRs) and the increasing reliance on digital platforms for healthcare delivery, the importance of robust data security measures cannot be overstated. The safeguarding of patient information against unauthorized access, breaches, and data theft has emerged as a paramount concern for healthcare providers worldwide.

Traditional methods of user authentication, such as passwords and personal identification numbers (PINs), have proven to be vulnerable to security threats, including password theft, brute force attacks, and social engineering exploits. Consequently, there is a growing need for innovative authentication solutions that offer enhanced security, reliability, and user convenience. In response to these challenges, this project introduces a Fingerprint Authentication-Based Patient Database Management System (FAPDMS). FAPDMS represents a pioneering approach to healthcare data security, leveraging fingerprint biometrics as a means of user authentication and access control. By harnessing the unique physiological characteristics of fingerprints, FAPDMS offers a robust and reliable method for verifying the identity of users, thereby minimizing the risk of unauthorized access to sensitive patient information.

The primary objective of FAPDMS is to address the shortcomings of traditional authentication methods while streamlining the process of patient data management in healthcare settings. By integrating fingerprint authentication with a comprehensive database management system, FAPDMS aims to enhance the Security, efficiency, and accessibility of patient records, ultimately improving the quality of healthcare delivery.

This introduction sets the stage for a detailed exploration of FAPDMS, including its underlying principles, system architecture, key features, and potential benefits for healthcare providers and patients alike. Through empirical testing and analysis, this project seeks to evaluate the effectiveness and feasibility of FAPDMS as a viable solution for addressing the evolving security challenges in healthcare data management.

2. EXISTING SYSTEM

A. Existing system

Current patient database management systems in healthcare rely on conventional authentication methods such as passwords and smart cards. However, these methods are associated with notable limitations and vulnerabilities. Passwords, for instance, are prone to security breaches due to factors like weak password selection or password reuse across multiple accounts. Moreover, healthcare professionals often struggle with the cognitive load of remembering numerous passwords, which can lead to frustration and inadvertently compromise security. Additionally, once authenticated, users typically have unrestricted access to patient records within these systems. This unrestricted access raises concerns regarding data privacy and confidentiality, especially given the sensitive nature of healthcare information. Furthermore, the lack of real-time authentication capabilities in existing systems can lead to delays in accessing patient records during critical moments of care delivery. These delays can impede clinical decision-making and potentially compromise patient outcomes.

B. Problem identification

In the current healthcare landscape, the management of patient data poses significant challenges in terms of security, efficiency, and accessibility. Conventional methods of user authentication, such as passwords and personal identification numbers (PINs), are prone to security breaches and are often cumbersome for healthcare professionals to manage. These challenges are further exacerbated by the increasing volume and complexity of patient data, as well as the evolving regulatory landscape governing data privacy and security.

The existing patient database management systems lack robust authentication mechanisms and granular access controls, leading to potential breaches of patient privacy and confidentiality. Moreover, authentication delays and administrative overhead associated with password management impede workflow efficiency and clinical decision-making in healthcare settings.

To address these challenges, there is a critical need for innovative solutions that offer enhanced security, efficiency, and user convenience in managing patient data. The development of a Fingerprint Authentication-Based Patient database Management System (FAPDMS) aims to address these pressing concerns by leveraging biometric authentication technology to secure access to patient records while streamlining workflow processes for healthcare professionals.

C. Disadvantages

1.Security Vulnerabilities: Conventional authentication methods such as passwords and PINs are prone to security breaches. Weak passwords, password sharing, and susceptibility to brute force attacks make it easy for unauthorized individuals to gain access to patient records, compromising data security and Confidentiality.

2.User Convenience: Healthcare professionals often struggle to remember multiple passwords for accessing different systems and applications. This can lead to frustration and inefficiencies in workflow as users may resort to writing down passwords or using easily guessable ones, further compromising security.

3.Limited Access Control: Once authenticated, users typically have unrestricted access to patient records. This lack of granular access control can pose risks to patient privacy, as sensitive information may be accessed by individuals who do not have a legitimate need for it.

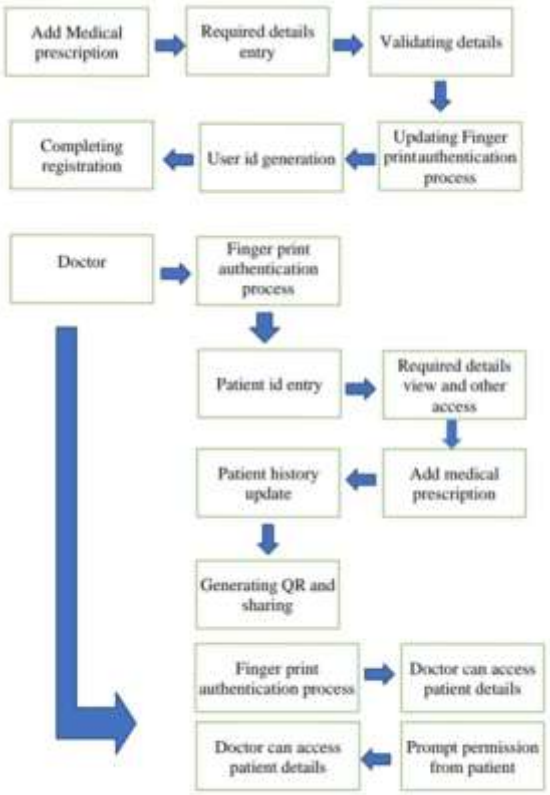
4.Authentication Delay: Traditional authentication methods require users to manually enter passwords or PINs, which can lead to delays in accessing patient records during critical moments of care delivery. These delays can impede clinical decision-making and compromise patient outcomes.

5.Regulatory Compliance Challenges: Healthcare organizations must comply with stringent data privacy regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection regulation). Conventional authentication methods may not adequately address regulatory requirements, increasing the risk of non-compliance and potential legal consequences.

6.Password Management Overhead: Healthcare IT administrators are tasked with managing user accounts, resetting passwords, and enforcing password policies. This administrative overhead consumes time and resources, diverting attention from other critical IT tasks.

7.User Resistance to Security Measures: Some healthcare professionals may resist implementing additional security measures due to perceived inconvenience or disruption to workflow. This resistance can hinder efforts to improve data security and compliance with regulatory requirements.

3. PROPOSED SYSTEM ARCHITECTURE



A proposed system for managing patient information and medication prescriptions could involve the creation of a secure database accessible via username and password authentication. This database would store detailed personal information about patients, including their medical history, allergies, and demographic data. Additionally, it would contain documents related to medical consultations, test results, and prescribed medications. The system would feature a user-friendly interface with tabs for different functionalities, and finger print access such as patient registration, medication suggestions, a patient registration tab would allow healthcare providers to input new patient information into the database, ensuring that all relevant details are accurately recorded and easily accessible for future reference. can generate the required sentence using minimum keystroke input and reduced input errors. Here, the system takes the lead in suggesting symbol candidates to the user. In our experiments, we use a decision tree.

The proposed Fingerprint Authentication-Based Patient Database Management System (FAPDMS) aims to revolutionize the way patient data is managed and accessed in healthcare facilities. FAPDMS will leverage cutting-edge fingerprint biometric technology to enhance security, efficiency, and accessibility in patient database management. The system will consist of the following key components:

1.Fingerprint Enrollment Module:

- Users, including healthcare professionals and patients, will be enrolled in the System by capturing their fingerprints using biometric scanners.
- Fingerprint templates will be generated and securely stored in the system's database as unique identifiers for each user.

2.Authentication and Access Control Module:

- FAPDMS will utilize fingerprint biometrics for user authentication, allowing authorized users to securely access patient records.
- Upon authentication, users will be granted access to specific functionalities and patient data based on their roles and permissions.

3.Secure Database Management:

- Patient records, including medical history, diagnostic reports, and treatment Plans, will be stored in a centralized database.
- The database will be encrypted to ensure the confidentiality and integrity of patient data, with access restricted to authorized users.

4. User Interface:

- FAPDMS will feature an intuitive user interface designed to streamline the navigation and interaction with the system.

 Healthcare professionals will be able to easily search, retrieve, update, and analyze patient records, facilitating informed decision-making and efficient patient care delivery.

5. Real-Time Updates and Alerts:

 The system will support real-time updates to patient records, allowing healthcare professionals to access the most current information during consultations and treatments.

6. Integration and Interoperability:

 FAPDMS will be designed to integrate seamlessly with existing healthcare information systems, electronic health records (EHRs), and medical devices.

 Interoperability standards such as HL7 (Health Level Seven) will be followed to facilitate data exchange and interoperability with external systems.

7. Scalability and Future Enhancements:

 The proposed system will be scalable to accommodate the evolving needs and growth of healthcare facilities.

 Future enhancements may include the integration of advanced analytics, artificial intelligence (AI), and blockchain technology to further enhance system capabilities and security.

Hardware description

A. FINGER PRINT SENSOR

Fingerprint scanners capture an image of a person's fingerprint and then compare it to a database of known fingerprints. If the fingerprint matches a known fingerprint, the person is authenticated. Fingerprint scanners are used in various devices, including laptops, smartphones, and tablets.

Capacitive or CMOS scanners use capacitors and thus electric current to form an image of the fingerprint. This type of scanner tends to excel in terms of precision. Ultrasonic fingerprint scanners use high frequency sound waves to penetrate the epidermal (outer) layer of the skin.

Software description

A. WEB APPLICATION

A web application (web app) is an application program that is stored on a remote server and delivered over the internet through a browser interface. The web application server processes the client requests and sends back a response. The requests are usually for more data or to edit or save new data. For example, if the user clicks on the Read More button, the web application server will send content back to the user. A web-application is an application program that is usually stored on a remote server, and users can access it through the use of Software known as web-browser.

B. MIT APP

MIT App Inventor is a high-level block-based visual programming language, originally built by Google and now maintained by the Massachusetts Institute of technology. It allows newcomers to create computer applications for two operating systems: Android and iOS, which, as of 25 September 2023, is in beta testing. MIT App Inventor is an educational tool to learn computational thinking and computational action principles through building mobile apps. Used by over one million people worldwide every year, it is one of the premier platforms for computer science education.

The web interface consists of a graphical user interface (GUI) very similar to Scratch and StarLogo, allowing users to drag-and-drop visual objects to create an application that can be tested on Android and iOS devices and compiled to run as an Android app.

4. ADVANTAGES

1. Enhanced Security: Fingerprint authentication offers a highly secure method of user verification, significantly reducing the risk of unauthorized access to sensitive patient data. Unlike passwords or PINs, fingerprints are unique to each individual, making them extremely difficult to replicate or compromise.

2.Improved Efficiency: The use of fingerprint authentication streamlines the process of accessing patient records, enabling healthcare professionals to retrieve information quickly and efficiently during consultations, treatments, and emergencies. This efficiency translates to improved patient care and reduced administrative burden.

3.User Convenience: Fingerprint authentication eliminates the need for users to remember complex passwords or carry physical access cards, enhancing user convenience and usability. Healthcare professionals can seamlessly access patient records with a simple fingerprint scan, saving time and minimizing cognitive load.

4.Real-time Authentication: Fingerprint authentication enables real-time verification of user identity, ensuring that only authorized personnel can access patient data at any given time. This real-time authentication capability enhances data security and confidentiality, especially in fast-paced healthcare environments.

5.Compliance with Regulations: By implementing robust authentication measures, such as fingerprint biometrics, the system ensures compliance with data privacy regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation), safeguarding patient privacy and confidentiality.

5.APPLICATION

The Fingerprint Authentication-Based Patient Database Management system (FAPDMS) proposed in this project holds immense potential for revolutionizing healthcare data management across various applications. Some key applications of FAPDMS include:

1.Hospitals and Healthcare Facilities:

FAPDMS can be implemented in hospitals, clinics, and other healthcare facilities to streamline patient data management processes. Healthcare professionals can securely access patient records in real-time using their fingerprints, facilitating prompt and informed decision-making during consultations, treatments, and emergencies.

2.Electronic Health Records (EHRs):

FAPDMS can integrate seamlessly with electronic health record (HER) systems, enhancing the security and accessibility of patient health information. By replacing traditional authentication methods with fingerprint biometrics, FAPDMS mitigates the risk of unauthorized access to sensitive medical data, ensuring compliance with stringent privacy regulations such as HIPAA.

3.Telemedicine and Remote Healthcare:

In the era of telemedicine and remote healthcare delivery, FAPDMS enables secure access to patient records from remote locations. Healthcare providers can authenticate themselves using their fingerprints, allowing them to access and update patient information securely, regardless of their physical location. This capability enhances the efficiency and effectiveness of telemedicine consultations while maintaining data security and confidentiality.

4.Pharmaceutical Industry:

FAPDMS can also find applications in pharmaceutical companies and research institutions involved in clinical trials and drug development. By providing Secure access to patient data, FAPDMS facilitates the management of clinical trial participants' information, ensuring compliance with regulatory requirements and safeguarding the integrity of research data.

6. RESULT AND CONCLUSION

A. RESULT AND DISCUSSION

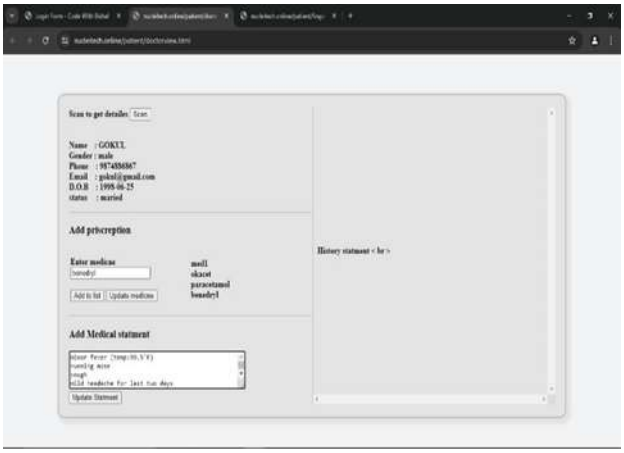
The implementation and testing of the Fingerprint Authentication-Based Patient database Management System (FAPDMS) have yielded promising results, demonstrating its effectiveness in enhancing healthcare data security and accessibility. Through rigorous testing and evaluation, the following key findings have emerged:

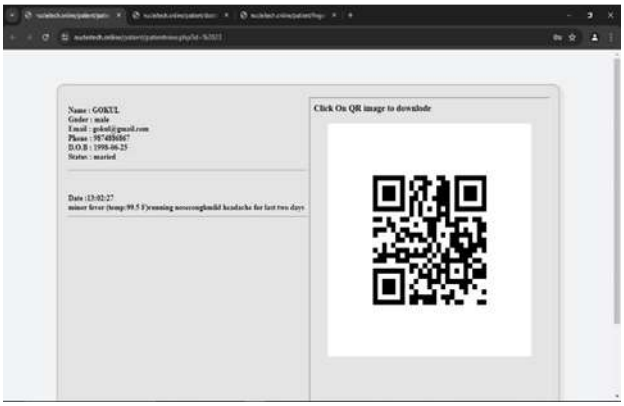
1.Enhanced Security: FAPDMS has significantly strengthened data security by replacing traditional authentication methods with fingerprint biometrics. The system's robust authentication protocols have successfully mitigated the risk of unauthorized access to patient records, ensuring compliance with stringent privacy regulations.

2.Improved Efficiency: FAPDMS has streamlined the process of accessing and managing patient records, resulting in improved efficiency and workflow Optimization within healthcare settings. Healthcare professionals can retrieve patient information swiftly during consultations and treatments, facilitating more informed decision-making and enhancing patient care quality.

3.User Acceptance: Feedback from healthcare professionals involved in the testing phase indicates high levels of satisfaction with FAPDMS's user interface and authentication process. The system's intuitive design and seamless integration into existing workflows have contributed to positive user experiences and acceptance among healthcare staff.

B. OUTPUT





C. CONCLUSION

In conclusion, the Fingerprint Authentication-Based Patient Database Management System represents a significant advancement in healthcare technology, offering a secure, efficient, and user-friendly solution for managing patient data. The system's proven efficacy in enhancing data security and accessibility, coupled with its potential for future enhancements, positions it as a valuable asset in the modern healthcare landscape.

By embracing emerging technologies such as biometric fusion, continuous authentication, blockchain integration, and predictive analytics, FAPDMS can continue to evolve and adapt to the evolving needs of the healthcare industry. With its ability to safeguard patient privacy, optimize workflow efficiency, and improve overall patient care quality, FAPDMS holds immense promise for driving positive transformations in healthcare data management.

D. FUTURE ENHANCEMENT

Integrate multiple biometric modalities such as fingerprint, iris, and facial recognition for more robust and reliable authentication. This fusion approach enhances security by requiring multiple biometric factors for user verification, reducing the likelihood of false acceptance or rejection. Implement continuous authentication mechanisms to monitor user behavior and dynamically adjust access privileges based on activity patterns. This proactive approach strengthens security by detecting anomalies in user behavior and responding in real-time to potential security threats.

Reference

[1] Sarath Krishnan P V; K Nanda Krishnan et al proposed " MedApp: An Application for Patient's Personal Medical History Maintenance " IEEE- 2023

[2] Gianpaul Custodio-Chavarría; Ricardo Paz Soldán-Araujo et al proposed "System to Optimize the Process of Medical Consultations Using QR Codes in the Hospitals of Peru " IEEE-2022

[3] Xuehu Yan; Yuliang Lu et al proposed " Applying QR Code to Secure Medical Management " IEEE- 2018

[4] José Alexander Cerrato Larios; Leslie Gabriela Ferrufino Aguilar et al proposed " QR Tech: Digital Platform for Medical Equipment Management in Public Hospitals " IEEE- 2023

[5] Yue Liu, Ju Ya g, Mingjun Liu, "Recognition of QR Code with mobile," Control and Decision Conference, CCDC 2008. Chinese, pp. 203 – 206,2-4 July 2008.

[6] Yu-Hsuan Chang, Chung-Hua Chu and Ming-Syan Chen, "A General Scheme for Extracting QR Code from a Non-uniform Background in Camera Phones and Applications," Ninth IEEE International Symposium on Multimedia, ISM 2007. pp. 123-130, 10- 12 Dec. 2012

[7] ScanLife.com, "QR Code Adoption: Trends and Statistics", www.scanlife.com

[8] Y. Yan, H.W. Liu, “Research and Application of Encoding and Decoding Tech. of QR Code”, University of Science and Tech, Beijing

[9] Aidong Sun, Yan Sun and Caixing Liu, “The QR-code

Reorganization in illegible snapshots taken by mobile phones,” International Conference on Computational Science and its Applications, 2007. ICCSA2007, pp. 532-538, 26-29 Aug. 2007.