Published by :
http://www.ijert.org

Health Connect – Centralized Medical History Platform

Sidharth D
Dept. of Computing Technologies,
School of Computing,
College of Engineering and Technology
SRM Institute of Science and Technology, Kattankulathur,
Chennai, India

Rayi Sowmya
Dept. of Computing Technologies,
School of Computing,
College of Engineering and Technology
SRM Institute of Science and Technology, Kattankulathur,
Chennai, India

Dr. P. Murali
Associate Professor
Dept. of Computing Technologies,
School of Computing,
College of Engineering and Technology
SRM Institute of Science and Technology, Kattankulathur,
Chennai, India

***Abstract*— The centralized medical history platform for patients represents a sophisticated and user-centric web application meticulously crafted on the SpringBoot framework. Engineered to elevate patient management processes within healthcare institutions, this system endeavors to harmonize and optimize various facets of patient care. By furnishing healthcare practitioners with efficient tools for managing patient information, appointments, and medical records, it provides a secure and centralized platform for hospitals and clinics. This initiative aims to amplify the patient care journey, fostering seamless decision-making for healthcare professionals. With its intuitive interface and robust functionalities, the centralized medical history platform for patients aspires to elevate the standards of healthcare provision, all while upholding the utmost standards of data confidentiality and integrity. Furthermore, the platform integrates advanced encryption techniques, such as AES-256, to ensure that patient data remains highly secure and protected from unauthorized access, thereby reinforcing trust and confidence in the system.**

***Keywords*—Medical history, AES-256 encryption, centralization, data integrity, healthcare.**

I. INTRODUCTION

In modern healthcare systems, the cumbersome nature of managing physical medical records poses a substantial challenge, particularly for patients who frequently consult multiple doctors. The inconvenience of transporting and organizing these records not only increases the likelihood of misplacements but also disrupts the continuity of treatment processes. To tackle this pressing issue, we propose the implementation of a centralized medical history system via a user-friendly web application. This innovative solution harnesses the expansive capabilities of cloud services, encompassing a diverse array of computing resources such as servers, storage, and databases, all accessible through a cloud platform. Cloud computing presents unparalleled advantages, including rapid innovation, scalability, and cost-efficiency, thereby eliminating the need for traditional on-premises infrastructure. Furthermore, data stored within the cloud environment is fortified by robust encryption measures, ensuring an additional layer of security to safeguard sensitive medical information.

By centralizing medical records and leveraging the power of cloud technology, our proposed system aims to streamline the process of accessing patient information while simultaneously enhancing data security and accessibility for both healthcare providers and patients. This introduction outlines the critical importance of addressing the challenges posed by physical medical records and introduces our innovative solution, which seeks to revolutionize the management of medical history through the integration of user-friendly web applications and cloud-based infrastructure.

To tackle the inconveniences linked with physical medical records and the risk of misplacement, we suggest implementing a centralized medical history system through a user-friendly web application. This system harnesses cloud services, providing rapid innovation, scalability, and cost-efficiency, while ensuring data security through robust AES-256 encryption measures. The primary objectives encompass streamlining patient care processes, enhancing accessibility to medical records, and improving efficiency in managing patient information.

The proposed centralized medical history system offers several advantages over traditional paper-based records. Firstly, it eliminates the need for patients to carry physical records, thus reducing the risk of loss or damage. Instead, medical records can be accessed securely through a web application from any internet-enabled device, enabling healthcare providers to retrieve vital information promptly. Additionally, the system enables seamless communication between healthcare professionals by allowing them to access patient records remotely, thereby improving the coordination of care. Moreover, real-time updates and stringent security measures ensure that patient data remains current, accurate, and protected against unauthorized access, in the end leading to improved outcomes and a more efficient means of healthcare system.

The platform aims to streamline patient care by providing healthcare practitioners with efficient tools for managing patient information, appointments, and medical records. It facilitates quicker decision-making and improves the patient care journey by enhancing accessibility to medical records for both healthcare providers and patients. Leveraging cloud services and robust encryption, the platform ensures the security and confidentiality of patient data, mitigating risks associated with physical record misplacements.

Key areas of the centralized medical history platform include patient information management, appointment scheduling, and medical records storage. It prioritizes secure data access, interoperability with existing healthcare systems, and scalability to accommodate growing patient data volumes. The platform features an intuitive interface for healthcare providers and offers reporting and analytics capabilities for quality improvement and cost optimization for all the users.

II. LITERATURE REVIEW

The paper “A blockchain enabled sharing platform for personal health records” [1] covers the challenges of managing patient health records across multiple organizations, emphasizing the need for secure and consent-driven solutions. It reviews encryption methods and access control models, highlighting the limitations of traditional models in distributed systems like PHR. It discusses the adoption of blockchain, particularly Hyperledger Fabric, to address these challenges. Additionally, it touches on patient self governance and the trend of zero-trust security models. Overall, the survey provides background for the proposed blockchain implemented PHR sharing platform with user-controlled security and privacy.

The paper “A blockchain-based scheme for secure storage and sharing of medical records” [2] highlights the growing role of IoT in healthcare, emphasizing its use in patient monitoring and data collection. Security concerns regarding medical data collected through IoT devices are identified, leading to the proposal of an AI and blockchain-enabled solution for enhanced cybersecurity. The review discusses prior research, noting limitations such as scalability issues and centralized trust. Overall, it provides background on the challenges in securing medical IoT data and sets the stage for the proposed cybersecurity solution.

The paper “Research on medical data storage and sharing model based on blockchain” [3] addresses medical data security and sharing challenges using blockchain and homomorphic encryption. Previous studies explored blockchain for data sharing and access control. However, they often lacked efficient data transmission and were limited to specific institutions. This paper proposes a blockchain-based model with homomorphic encryption to ensure secure storage and transmission of medical data. It aims to overcome previous limitations, offering decentralized storage, privacy, and efficient data processing.

The paper “Med EHR-Electronic health Record using Blockchain” [6] proposes the Recent technological advancements are reshaping healthcare, addressing issues such as security and user experience. Despite improvements, challenges persist regarding data integrity and ownership. Blockchain offers a decentralized solution, enhancing trust and security in healthcare systems. Its adoption in cryptocurrency domains underscores its potential to revolutionize healthcare, enabling a patient-centric approach and refining electronic healthcare record precision. Blockchain addresses the challenge of effective data sharing by ensuring authenticity and integrity through its decentralized and immutable nature.

The paper “Centralized Concurrency of Medical Records” [7] proposes a Personal Health Records (PHRs) are vital for consolidating patients' health data to provide a comprehensive view of their well-being. However, integrating this data from various electronic health systems poses challenges. Adhering to patient-defined privacy policies is crucial when accessing sensitive PHR data, requiring careful consideration in PHR architecture design. Cloud computing offers scalability, accessibility, and elasticity, making it suitable for PHR systems. This study conducts a scoping review of integrated, reliable, and cloud-based PHR systems to address complexities in healthcare data integration and privacy.

The paper “A Blockchain-Based Architecture for Interoperable Healthcare Data Exchange” [9] introduces a decentralized data-sharing solution using blockchain to improve healthcare interoperability and patient data control. It tackles challenges in accessing and transferring healthcare data between providers due to system incompatibility. Leveraging Hyperledger Fabric, patients can manage their data securely, enabling seamless sharing. The architecture facilitates creating, updating, and sharing transactions while ensuring patient ownership. With multi-signature transactions and integration with existing decentralized models, the approach offers a promising solution for healthcare data management.

III. MATERIAL AND METHODS

A. Proposed Model

1) Framework Integration:
- Employ AES-256 for real-time data encryption.
- Integrate decryption using security key at the backend for seamless transaction.

2) Technology Stack:
- Leverage AES-256 for encryption and password that will work as decrypt key to view the data.

3) User Interaction:
- Allow users to interact via website.
- Provide a user-friendly interface via springboot application for seamless interface.

4) Real-time Encryption:
- Implement AES-256 encryption and decryption for accurate and secure storage of data.

5) Output and Deployment:
- Offer downloadable reports and visualizations for detailed analysis.
- Design the system for cloud deployment, ensuring scalability and accessibility.

B. System Implementation

The implementation of the proposed system are given in detail in this section.

1) Software and Hardware

The system requires a central server with Java installed, along with necessary database storage components. It is compatible with different operating systems. To manage large data volumes and ensure continuous system operation, it is crucial to have a configuration consisting of at least 8GB of RAM and an Intel i5 processor .

2) Dataset

The data includes the previous medical prescriptions or reports that that user uploads while booking an appointment with the doctor.

The doctor can also upload the reports after the appointment is completed and results are obtained.

The uploaded data is secured and stored with the help of AES-256 encryption algorithm.

3) Parameters

BLOCK SIZE: AES operates on a fixed-size block of data, with the size of block being128 bits for AES-256.

KEY SIZE: AES-256 uses a 256-bit key for encryption and decryption.

NUMBER OF ROUNDS: AES-256 consists of 14 rounds of encryption and decryption, each comprising a series of substitution, permutation, and mixing operations.

SUBSTITUTION TABLE (S-BOX): AES-256 utilizes a fixed substitution table known as the S-box, which substitutes each byte of the data block during encryption and decryption.

ROUND KEYS: Key expansion generates additional round keys from the original 256-bit encryption key, which are used in each round of encryption and decryption.

C. Methodology

The implementation of the centralized medical history platform leverages Java, SpringBoot, Thyme leaf,
and Java 11 to create a robust and efficient web application. Java's versatility and object-oriented design provide a solid foundation for the platform, allowing it to compile into bytecode for universal compatibility. Spring Boot simplifies setup and configuration, enabling rapid application development while integrating seamlessly with other Java frameworks like JPA/Hibernate ORM and Struts. Thyme leaf enhances template rendering with its transformation-based approach and full integration with Spring, facilitating dynamic web content creation. Java 11 introduces optimizations for performance, particularly on ARM64 processors, aligning the platform with advancements in hardware acceleration.

The web server component acts as the interface between clients and the centralized medical history platform, delivering web pages and application content via HTTP protocols. It plays a crucial role in facilitating file transfers, email services, and web page hosting, supporting diverse user needs across internet infrastructure.

The user interface of the centralized medical history platform is designed to be intuitive, user-friendly, and accessible to healthcare practitioners and patients alike. Leveraging Thyme leaf templates and Java-based rendering, the interface offers a responsive and dynamic experience, allowing users to navigate seamlessly through different functionalities. Clear and concise layouts enable efficient management of patient information, appointments, and medical records, while intuitive controls streamline interactions. Customizable dashboards and reports provide valuable insights into patient care processes, facilitating informed decision-making for healthcare professionals.

For data security, the platform employs AES 256 encryption, ensuring the confidentiality and integrity of patient information. Key management procedures include generating a secure 256-bit key using cryptographically secure random number generators, securely storing the key, and regularly rotating it to mitigate the risk of compromise. The encryption process involves preparing the file, initializing the cipher, encrypting blocks of data, and writing the encrypted data securely. Decryption follows a similar process, involving loading encrypted data and the key, initializing the cipher, decrypting blocks of data, and validating authenticity before processing.

D. System Architecture

The architecture of the system, as shown in Fig. 1, is outlined with this section. It is structured around the interconnected entities of hospitals, users, and doctors, facilitating seamless interactions and efficient management of patient information. At the core of the architecture is the relational database, where hospitals store fixed appointments, track doctor activity, and view user appointments. Backend services, implemented using Java and SpringBoot, handle business logic and data processing, enabling hospitals to log in, view appointments, and monitor doctor activities.

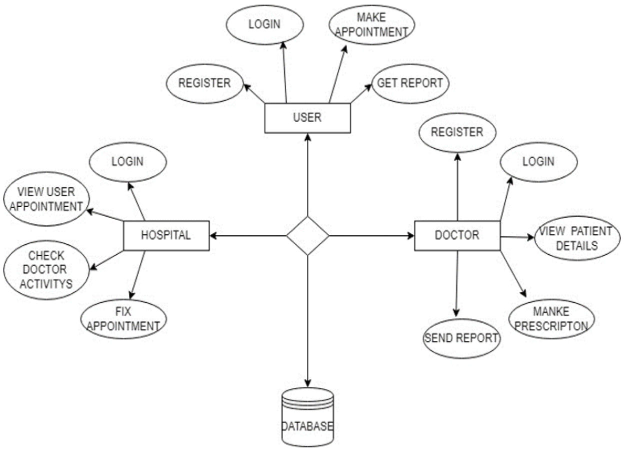


Fig. 1 proposed system architecture

Users interact with the platform through a frontend interface developed using HTML, CSS, and JavaScript, allowing them to register, log in, make appointments, and access medical reports. Backend services process user requests, authenticate user credentials, manage appointment scheduling, and provide access to medical reports securely.

Similarly, doctors utilize the platform to register, log in, view patient details, prescribe medication, and send medical reports. Backend services enable doctors to access patient information securely, make prescriptions, and communicate medical reports efficiently. Cloud infrastructure hosts the platform, ensuring scalability, reliability, and security. The system architecture incorporates robust security measures, including AES-256 encryption, user authentication mechanisms, and secure data storage, to protect patient confidentiality and integrity.

Integration points facilitate interoperability with existing healthcare systems, allowing seamless exchange of data and integration with electronic health records (EHR) systems, medical imaging systems, and laboratory information management systems (LIMS). This cohesive system architecture ensures efficient management of patient information, streamlined appointment scheduling, and enhanced communication between hospitals, users, and doctors, ultimately improving the delivery of healthcare services.

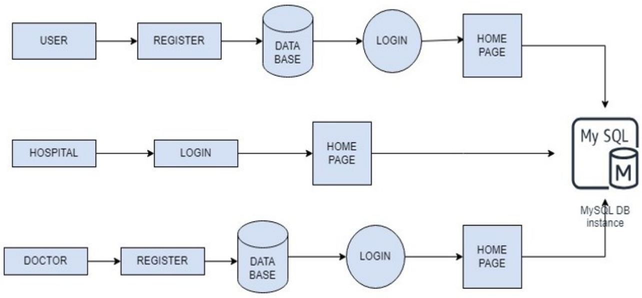


Fig. 2 Data flow diagram of the proposed system architecture

E. AES – 256 algorithm

AES 256, a symmetric encryption algorithm, operates on 128-bit blocks of data and utilizes a 256-bit encryption key. Key expansion generates additional round keys from the original key, facilitating multiple rounds of encryption and decryption. Each round comprises substitution, permutation, and mixing operations, ensuring confusion and diffusion to thwart cryptanalysis. Sub Bytes substitutes each byte using a fixed substitution table (S-box), while Shift Rows rearranges bytes within rows and Mix Columns combines bytes in columns through matrix multiplication. The final round excludes Mix Columns, yielding ciphertext resistant to decryption without the correct key. AES 256's intricate operations and large key size provide robust encryption, making it a widely trusted standard for securing sensitive data.

To ensure robust encryption, a secure 256-bit key is generated using a cryptographically secure random number generator, guaranteeing uniqueness and strength against cryptographic attacks. This key is then securely stored, considering options such as hardware security modules (HSMs) or encrypted key stores, to prevent unauthorized access and safeguard against key compromise. Regular key rotation is implemented to mitigate risks further, enhancing the overall security posture of the encryption process.

For encryption, the file is divided into fixed-size blocks, typically 16 bytes for AES 256, to facilitate efficient processing and enhance security. A Cipher object is initialized with the AES algorithm, mode, and padding scheme, such as PKCS#5, ensuring compatibility and adherence to cryptographic standards. The 256-bit key, securely loaded from a trusted source like an HSM or encrypted key store, is used to encrypt each block of data, leveraging the robust encryption capabilities of AES-256. The encrypted blocks, along with the initialization vector (IV) if used, are stored in a new file or database field, preserving the confidentiality and integrity of the data.

During decryption, the encrypted data and key are retrieved securely to prevent unauthorized access or tampering. A Cipher object is initialized with the same configuration as encryption, ensuring compatibility and enabling decryption of the data. The encrypted blocks are decrypted using the 256-bit key, leveraging the advanced decryption capabilities of AES-256. Before processing, the authenticity of the decrypted data is verified to detect any unauthorized modifications or tampering. The decrypted blocks are then assembled to reconstruct the original file, ensuring data integrity and completeness.

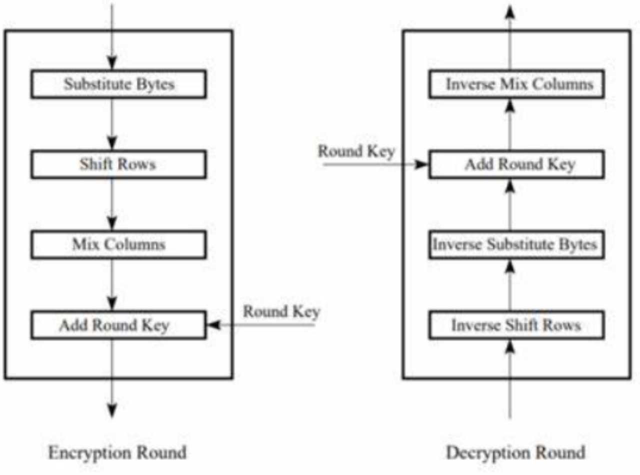
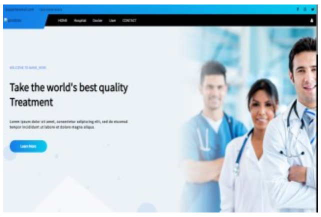


Fig. 3 AES-256 encryption decryption

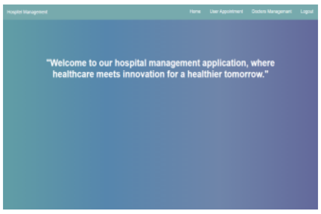
IV. RESULT AND ANALYSIS



Take the world's best quality Treatment

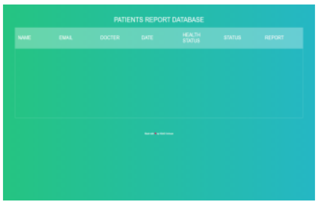
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Fig. 4 Homepage



"Welcome to our hospital management application, where healthcare meets innovation for a healthier tomorrow."

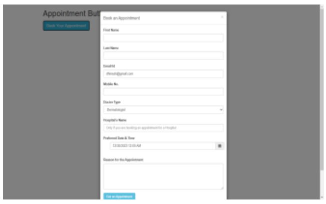
Fig. 5 Hospital main page



PATIENTS REPORT DATABASE

NAME	EMAIL	DOCTER	DATE	HEALTH STATUS	STATUS	REPORT

Fig. 6 Report history



Appointment But

Book Your Appointment

Book an Appointment

First Name

Last Name

Email Id

dhinesh@gmail.com

Mobile No.

Doctor Type

Dermatologist

Hospital's Name

Only if you are booking an appointment for a Hospital

Preferred Date & Time

12/30/2023 12:00 AM

Reason for the Appointment

Get an Appointment

Fig. 7 Appointment form

The Fig. 4 displayed above represents the homepage off the website, featuring the navigation to go to doctor, hospital, or user section. In Fig. 5 The hospital main page is where they manage doctor and user appointments. Subsequently, in Fig. 7 the appointment form is filled for the user to be appointed to a doctor and after the diagnosis is completed the doctor can upload the report onto the website where it is encrypted using AES-256 and when the user wants to see the report the data is decrypted and made available for the user to view in Fig. 6 .

V. CONCLUSION

In conclusion, the centralized medical history system for patients marks a significant milestone in healthcare technology, leveraging the robust capabilities of the Spring Boot framework to deliver a comprehensive and user-friendly web application. Through its innovative design, the system streamlines various patient management processes, including appointment scheduling, medical record management, and information retrieval. This consolidation of essential functions empowers healthcare professionals to administer more efficient and personalized care, ultimately leading to improved patient outcomes.

A paramount focus on security underscores the system's commitment to safeguarding the confidentiality and integrity of patient data. With stringent security measures in place, including encryption protocols and access controls, patients and healthcare providers can trust that sensitive medical information remains protected from unauthorized access or breaches.

Furthermore, the centralized nature of the platform enhances decision-making and coordination within healthcare facilities. By providing a unified interface for accessing patient records and streamlining communication among care teams, the system facilitates smoother workflows and ensures continuity of care across various medical departments.

Overall, the implementation of this innovative system contributes to an enhanced patient care experience, fostering better healthcare delivery, accessibility, and quality. Its integration of intuitive interfaces and robust functionalities makes it a valuable asset for hospitals and clinics striving to optimize their operational efficiency and elevate the standard of healthcare services provided to patients. Contributes to an improved overall patient care experience, fostering better healthcare delivery, accessibility, and quality.

The integration of intuitive interfaces and robust functionalities makes it a valuable asset for hospitals and clinics striving to enhance their operational efficiency and the quality of healthcare services provided.

VI. REFERENCES

[1] 1Yibin Dong, Seong K. Mun, Yue Wang, A blockchain-enabled sharing platform for personal health records, Heliyon, Volume 9, Issue 7, 2023, e18061, ISSN 2405-8440, https://doi.org/10.1016/j.heliyon.2023.e18061:

[2] Zhijie Sun, Dezhi Han, Dun Li, Tien-Hsiung Weng, Kuan-Ching Li, Xiaojun Mei, MedRSS: A blockchain-based scheme for secure storage and sharing of medical records, Computers & Industrial Engineering, Volume 183, 2023, 109521, ISSN 0360-8352, https://doi.org/10.1016/j.cie.2023.109521.

[3] Jian Zhao, Wenqian Qiang, Zisong Zhao, Tianbo An, Zhejun Kuang, Dawei Xu, Lijuan Shi, Research on medical data storage and sharing model based on blockchain, High-Confidence Computing, Volume 3, Issue 3, 2023, 100133, ISSN 2667-2952, https://doi.org/10.1016/j.hcc.2023.100133.

[4] Chad Anderson, Arthur Carvalho, Mala Kaul, Jeffrey W. Merhout, Blockchain innovation for consent self-management in health information exchanges, Decision Support Systems, Volume 174, 2023, 114021, ISSN 0167-9236, https://doi.org/10.1016/j.dss.2023.11402.

[5] S. Balla1, Y. Chandr, R. Pise, B. Sonare and S. Patil, "Blockchain-Based Decentralized Platform for Electronic Health Records Management," 2023 IEEE Internationa1 Conference on B1ockchain and Distributed Systems Security (1CBDS), New Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICBDS58040.2023.1034639.

[6] S. Siingh, S. Guptaa and Indu, "MedEHR-Electronic health Record using Blockchain," 2023 Internationa1 Conference on Computationa1 Intelligence, Communnication Technology and Networking (C1CTN), Ghaziaabad, India, 2023, pp. 58-62, doi: 10.1109/CICTN57981.2023.10141053.

[7] P. Yellamma, S. S. Kathera, D. S. V. S. U. S. S. N. Sarma and Y. Palukuri, "Centralised Concurrency of Medical Records," 2023 Internationa1 Conference on Inventive Compuutation Technologies (1CICT), Lalitpuur, Nepal, 2023, pp. 635-642, doi: 10.1109/ICICT57646.2023.10134315.

[8] N. Gupta, J. Shah, V. Shah and S. Patil, "Secured Medical Record Sharing Application Using Blockchain Technology," 2023 14th Internationa1 Conference on Computing Commuunication and Networking Technology (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10306929.

[9] N. Sahi, A. Liang, S. McHale, W. Van Devanter and P. Zhang, "A Blockchain-Based Architecture for Interoperable Healthcare Data Exchange," 2023 IEEE Internationa1 Conference on Bionformatics and Bio-medicine (B1`BM), Istanbul, Turkiye, 2023, pp. 4404-4410, doi: 10.1109/BIBM58861.2023.10385970.

[10] B. Panchal, S. Parmar, T. Rathod, N. K. Jadav, R. Gupta and S. Tanwar, "AI and Blockchain-based Secure Message Exchange Framework for Medical Internet of Things," 2023 International Conference on Network, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2023, pp. 1-6, doi: 10.1109/NMITCON58196.2023.10275980.