IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SECURE HEALTHCARE MANAGEMENT APPLICATION

[1]Ajeeb Nazer, Arunmon C R, Jeny K Berly, Sachu K S

[2]Prof. Praseetha S Nair

[1](Final Year Students, Department of Computer Science & Engineering, Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India)

[2](Assistant Professor, Department of Computer Science & Engineering, Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India)

Abstract : Security of health information has been a major issue in the health care industry. As health information is exchanged between doctors, patients and health care providers it is important to secure the patients information. Protecting the patient's medical record from prospective attackers is one of the key criteria in today's health care systems. The proposed work aims to develop a robust HealthCare Data Management System that ensures the security and privacy of patient health records while incorporating blockchain technology for secure payment processing. The system leverages AES (Advanced Encryption Standard) encryption algorithms to safeguard patient health records, providing confidentiality and integrity. Additionally, blockchain technology is employed to encrypt payment details, ensuring secure and transparent transactions. The system also offers a user-friendly mobile interface for patients. This paper outlines the key components, functionalities, and benefits of the proposed system.

***IndexTerms* – AES Algorithm, Blockchain.**

INTRODUCTION

Hospitals deal with the life and health of their patients. Good medical care relies on well-trained doctors and nurses and on high quality facilities and equipment. Good record keeping is essential to providing quality medical treatment. More and more organizations especially the healthcare industry adopt cloud technology because of the large volume of data processed in the healthcare industry. Cloud computing facilitates and secures medical record exchange. Better anywhere, anytime access to the cloud will also enable the effective use of healthcare resources and effective exchange of information. But still, no privacy and protection laws are created for cloud computing. So there is a need to secure health information locally and globally. To make electronic health records more secure employ various encryption techniques and blockchain technology. The blockchain contains a list of records called blocks linked together by hashing mechanism. The purpose of the work is to aid the healthcare industry.

The healthcare industry faces significant challenges in managing patient data securely and facilitating seamless financial transactions. This research paper proposes a HealthCare Data Management System that leverages AES encryption and blockchain technology to address these challenges. The paper provides an overview of the current healthcare landscape, identifies the need for improved data security and financial transaction efficiency, and introduces the research objectives.

Potent security and privacy risks of Health Information (HI) have appeared as considerable issues. An organization's records are created, protected, retrieved, and eventually disposed of according to business standards that are defined and put into practise by the discipline of records management. Good records care ensures the hospitals administration runs smoothly; unneeded records are transferred or destroyed regularly, keeping storage areas clear and accessible; and key records can be found quickly, saving time and resources. Records also provide evidence of the hospital's accountability for its actions, and they form a key source of data for medical research, statistical reports and health information systems. A management information system (MIS) is a method or system that offers the data required to successfully manage an organisation. Tele-monitoring has been utilized to remotely screen the patient's health, like clinical centers and emergency clinics. These days, it is a potent E-health service. By the utilization of telecommunication technologies, the diagnosis, evaluation, and treatment of the patient are being carried out. While performing diagnosis and treatment, access to Electronic Health Information (EHI) is a prerequisite. There are many security issues, despite the growing popularity of EHI cloud-based maintenance and monitoring. Among these challenges, attack for information theft is a key challenge. AlSheikSalem proposed a scheme for private healthcare information security utilizing fog computing i.e., tri-party one round authenticated key agreement protocol. One of the emerging technologies in healthcare monitoring is the Internet of Things (IoT). This technology refers to interact with everyday objects. Ciphertext Policy Attribute-Based Encryption (CP-ABE) for the realization of fine-grained access control against smart health security was performed by Zhang. The utilization of CP-ABE in smart-healthcare comprises different issues. Physicians perform the remote monitoring of patient's data using electronic healthcare systems. The E-health systems provide easy data management by using different technologies like cloud computing but on the other hand, it entails many security issues. Due to different security and privacy challenges, to preserve the patient's secrecy, an efficient and flexible scheme is required that

ensures the disclosure of information to selectively authorized entities. Sanchez thus suggested a profile management system that creates a robust, unique credential for user claims.
Electronic healthcare services utilize different schemes for patient care, which can be utilized in different clinical applications. Patient data is enciphered to ensure authoritative access to patient's sensitive information. In the framework provided by Padmasree, the patient gives the key to the specialist. While in emergency-care, a patient offers an Attribute-Based-Key (ABK) with a lot of emergency-supporting representatives and allows access to the specialist for using the Emergency Key (EK). To preserve the patient's life, the Doctor uses ABK and EK to decrypt the clinical records. Cyber-attacks in social insurance have extended by 125% since 2010 and are presently the main source of HI security threats, as pointed by Kodmon et al. accordingly provided a mix of LSB and 3DES to enhance the security measures applied to medical information. To build up the experimental simulation, the Java programming language was utilized. Common block ciphers against the HI security at cloud comprises AES, DES, 3DES, IDEA Blowfish, RC5, and RC6, etc.

LITERATURE SURVEY

1. A Decentralized Cryptographic Blockchain Approach for Health Information System, 2019.

The use of blockchain technology for health information systems (HIS) has gained considerable attention due to its potential for enhancing the security, privacy, and interoperability of healthcare data. In recent years, several studies have proposed decentralized cryptographic blockchain approaches for HIS.
Due to the movement of patients, medical research entails and necessitates the processing and storage of massive amounts of health information throughout a wide range of geographic locations. When numerous people have access to the information systems, it is simple to change the data trails created by patients and medical professionals. Based on the sensitivity of medical information, which will be gathered, handled and managed. There is, therefore, the need for securing the medical data that will be saved as electronic health records (EHR). The usage of blockchain, allowing for a decentralized architecture for EHRs, and the validation and verification of medical data on a network of health information systems utilizing the MD5 cryptographic hash algorithm. The detailed information of a patient's medical ledger generated from the EHR. After that, the patient's medical records are then hashed using the MD5 cryptographic algorithm. This then yields a chain of blocks created to securely validate and verify the patient's entire ledger within the health information system. Thus, preventing any form of alteration or data falsification. The values from the patient's medical records were captured in blocks based on blockchain principles showing the patient's medical data information, timestamp of the medical data and the hash value computed on the patient's medical data captured. The subsequent blocks are then created from the updated patient's medical data, with the new hash of the updated medical records and the hash of the previous hash block and so on for the remaining blocks forming the chain. Overall, the paper provides a valuable overview of the current state of the art in blockchain technology for healthcare, and highlights the opportunities and challenges associated with its adoption.

2. Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain, 2019.

Blockchain technology has enormous potential for revolutionizing healthcare by providing a secure, immutable, and decentralized platform for the management and sharing of electronic health records (EHRs). Traditional EHR management systems face several challenges, including data breaches, cyber-attacks, and lack of interoperability between different healthcare providers. Blockchain technology can address these challenges by providing a secure and transparent platform that allows for the safe and efficient sharing of sensitive patient data. One of the key benefits of blockchain technology in healthcare is that it can help simplify pharmaceutical supply chains and accelerate drug development. With the help of blockchain technology, healthcare providers can track the entire lifecycle of a drug, from manufacturing to distribution, ensuring that it meets quality standards and regulations. This can help to reduce the risk of counterfeit drugs, enhance patient safety, and improve the overall efficiency of the pharmaceutical industry.
Moreover, blockchain technology can aid in clinical research by providing a secure and decentralized platform for storing and sharing patient data. Clinical researchers require access to vast amounts of patient data to develop and test new treatments and therapies. However, traditional EHR management systems are often siloed, making it difficult to access and share data. Blockchain technology can solve this problem by creating a secure and transparent platform that allows researchers to access patient data without compromising their privacy. To make healthcare data accessible for researchers while ensuring privacy, a proposed model focuses on aggregating customized access control protocols and asymmetric cryptography. This model separates sensitive and non-sensitive data of a patient, enabling effective sharing of healthcare data with researchers without compromising patient privacy. The use of a proxy re-encryption technique allows sensitive medical information to be shared without revealing the patient's private key. Overall, blockchain technology has the potential to transform the healthcare industry by providing a secure, transparent, and decentralized platform for managing EHRs, tracking pharmaceutical supply chains, and enabling clinical research. By leveraging blockchain technology, healthcare providers can improve patient outcomes, enhance data security, and ensure that patients' privacy is protected.

3. Cloud-based Secure Personal Health Record Management System using Mixnode and Blockchain, 2020.

The security and privacy of personal health information in e-health systems is a major concern. In this regard, several approaches have been proposed to ensure the confidentiality and integrity of e-health documents. One such approach is the use of symmetric key-based schemes that employ mix networks for achieving unobservable outsourced data access and blockchain for achieving outsourced data integrity. This approach ensures that unauthorized users, including third parties, cannot link outsourced e-health documents to their owners. A recent study proposed a secure and efficient cloud-based personal health record (PHR) management system that implements data access control using an efficient symmetric key-based cryptosystem. The use of blockchain ensures outsourced data integrity, even restricting a user with knowledge of encryption keys from modifying a committed PHR block. Moreover, the system ensures privacy and user unlikability using mix nodes between the PHR owner and the cloud service provider (CSP). This approach confuses adversaries capable of observing network traffic and ensures efficient access to PHR documents.
The proposed system allows each healthcare service provider (HSP) to have direct access to the outsourced data, eliminating the need for forwarding data through the mix node. However, the PHR owner must still access her data through the mix node, which introduces a delay due to the mixing process of the requests. Despite this delay, the proposed system does not affect the diagnosis processing time of a patient. The study implemented an important security requirement named forward secrecy, which restricts

medical health care providers from accessing any future health document after their session expires. Additionally, the study proposes procedures for publishing and accessing e-health documents, ensuring the confidentiality and integrity of e-health documents.
The proposed model successfully ensures the confidentiality, integrity, and privacy of personal health information in e-health systems. The use of blockchain, symmetric key-based schemes, and mix networks provides an efficient and secure mechanism for managing personal health records. The study demonstrated that the proposed model could address the issues related to security and privacy of personal health information and facilitate efficient and effective access to e-health documents. Future research could investigate the scalability and performance of the proposed system under various scenarios.

4. A Patient-Centric Health Information Exchange Framework Using Blockchain Technology, 2020.
Health Information Exchange (HIE) is a valuable tool in improving patient care, however, it is challenged by issues such as security, privacy, and costs. The Office of the National Coordinator (ONC) for Health Information Technology has sought to overcome these challenges by seeking patient centric HIE designs that shift data ownership from providers to patients. To address these challenges, this paper proposes utilizing blockchain technology to protect data security and patients' privacy while ensuring data provenance and providing patients full control of their health records.
The proposed blockchain model incorporates smart contract features, which are programmable self-executing protocols running on a blockchain. This solution achieves patient centric HIE with feasibility, stability, security, and resilience by personalising data segmentation and establishing a "allowed list" for physicians to access their data.
The paper proposes several practical characteristics to the blockchain system to achieve patient centric HIE, including a blockchain adapter setup to facilitate communication with the blockchain, process the sending/receiving of healthcare records, and provide graphical user interfaces for users to interact with the blockchain system. Additionally, two layers of security settings are implemented to ensure that only authorized users can execute certain smart contract functions and minimize the risk of data breaches. A hashing mechanism is also utilized to ensure data consistency. Furthermore, personalized data segmentation provides patients with control over their records by allowing them to choose only the information they would like to share, while touchpoint selection enables clinicians to select the relevant health records related to the visit without browsing through entire records.
Overall, this paper provides a feasible solution to the challenges of patient centric HIE through the use of blockchain technology, which provides enhanced data security, privacy, and control. The proposed blockchain model could potentially lower barriers to the implementation of patient centric HIE systems by mitigating privacy and security concerns among healthcare stakeholders.

5. MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address, 2021.
Health Information Exchange (HIE) offers several benefits for patient care, such as improving healthcare quality and streamlining administrative work. However, the implementation of HIE is hindered by security, privacy, and cost-related challenges. Recent studies have suggested the use of blockchain-based HIE for resolving security and privacy issues. Existing research on blockchain-based HIE, however, do not take into account privacy concerns brought on by the examination of sender and receiver addresses on the blockchain.
To address this limitation, this paper proposes the MEX change method for blockchain-based privacy-preserving HIE. The MEX change obscures the sender and conceals receiver addresses, preventing privacy issues. The proposed smart contracts and workflow utilize ring signature and stealth address for blockchain-based HIE. The paper discusses the software components and implementation of MEX change on the Ethereum private network. Additionally, the paper evaluates MEX change quantitatively by measuring the transaction latency and throughput of exchanging and qualitatively using the requirements of the Office of National Coordinator for Health Information Technology (ONC). Moreover, the paper proceeds with a threat modeling based on STRIDE. Finally, the paper evaluates MEX change with Ancile, FHIR Chain, Integrating the Healthcare Enterprise Cross-Enterprise Document Sharing (IHE XDS), and Med Rec.The proposed MEX change method reduces barriers to the implementation of blockchain-based HIE systems by mitigating privacy and security issues among healthcare stakeholders. The method shows strength in the privacy aspect by preventing the inference problem. The MEX change is an important contribution to the field of blockchain-based HIE, providing a practical solution for privacy issues in the blockchain.

IMPLEMENTATION

1. Proposed work

The suggested HealthCare Data Management System intends to improve healthcare organization security and efficiency by utilizing AES encryption for data protection and blockchain-based payment processing. The system is made up of various essential components and features, which are as follows:

1.1 User Authentication and Roles:

- The system supports different user roles, including staff, patients, doctors, and administrators.
- Users can use their credentials to register and log in to access the system's functions based on their roles and permissions.

1.2 Patient Records Management:

- All the records are stored in the server and authorized user can only access it.
- Doctor can access and upload patients' medical records.
- To secure and preserve sensitive patient data, AES encryption is used, assuring confidentiality and integrity.

1.3 Appointment Scheduling:

- Patients can request appointments and view their scheduled appointments through the system or a mobile application.
- Doctor can allot visiting time.

1.4 Blockchain-based Payment Processing:

- For safe and transparent payment processing, the system incorporates blockchain technology**.**
- Patients may use the system to pay for healthcare services, making use of the features of blockchain's decentralized and immutable record for financial transactions.

The suggested system is created with XAMPP as the server-side environment, Python Django as the backend framework, MySQL as the database management system, and HTML, CSS, and JavaScript as frontend languages. AES encryption is used to protect patient health records, while blockchain technology assures safe and transparent payment processing.

2. Introduction to Tools

2.1 Back-end

2.1.1 Python

Python is a general-purpose, interpreted, interactive, and object-oriented high-level programming language. Guido van Rossum designed it between 1985 and 1990. Python source code, like Perl, is accessible under the GNU General Public License (GPL). Python is a scripting language that is high-level, interpreted, interactive, and object-oriented. Python is intended to be extremely readable. It commonly employs English terms rather than punctuation, and it has fewer syntactical structures than other languages. Python is a must-have for students and working professionals who want to become exceptional software engineers, especially if they work in the web development domain. JavaScript, for example, is the most popular language among web developers since it allows the developer to manage applications using various frameworks such as react, vue, and angular, which are used to design attractive User Interfaces. Similarly, they have both advantages and disadvantages. So, if we take Python, it is general-purpose, which means it is extensively utilized in every domain. This is due to its ease of use and scalability, which allows for rapid development. You can see why it's popular among developers because, other from learning Python, it doesn't require any programming experience. Python's grammar is comparable to that of the English language, and it also helps developers to construct programs with fewer lines of code. Because it is open source, there are several libraries available to make developers' tasks easier, resulting in great productivity. In the digital age, when information is available in enormous data sets, they may readily focus on business logic and its demanding abilities.

2.1.2 Django

Django is a Python framework that simplifies the creation of web applications in Python. Django handles the tricky parts so you can focus on developing web apps. Django emphasizes component reusability, commonly known as DRY (Don't Repeat Yourself), and includes ready-to-use functionality such as a login system, database connection, and CRUD operations (Create Read Update Delete). Python-based web framework that allows you to easily construct web applications without the installation or dependency issues that are common with other frameworks. A comparable set of components is usually required when establishing a website: a mechanism to handle user authentication (signing up, signing in, signing out), a management panel for your website, forms, a way to upload things, and so on. Django provides you with ready-to-use components. Django is used by several major websites, including Discuss, Instagram, the Knight Foundation, the MacArthur Foundation, Mozilla, and National Geographic. The Django framework is used by over 5000 internet domains. (Source)Hot Frameworks ranks framework popularity by calculating the number of GitHub projects and Stack Overflow inquiries for each platform; Django is ranked sixth. Web frameworks frequently refer to themselves as "opinionated" or "UN-opinionated" depending on their views on the best approach to perform each given task. Django is slightly opinionated; thus he provides the best of both worlds (opinionated and un-opinionated).

2.1.3 MySQL

MySQL is the most widely used open-source database in the world. MySQL has become the preferred database choice for web-based applications, with high-profile online sites such as Facebook, Twitter, YouTube, and Yahoo! relying on its proven performance, dependability, and ease-of-use. MySQL is a relational database management system (RDBMS) based on Structured Query Language (SQL) that is free and open source. Almost every platform, including Linux, UNIX, and Windows, supports MySQL. Although it may be used in a variety of applications, MySQL is most commonly linked with web-based applications and online publishing, and it is a key component of the LAMP open-source corporate stack. LAMP stands for Linux as an operating system, Apache as a Web server, MySQL as a relational database management system, and PHP as an object-oriented programming language. (Occasionally, Perl or Python are used in place of PHP). MySQL, which was created by the Swedish company MySQL AB, was purchased by Oracle in 2008. MySQL may still be used by developers under the GNU General Public License (GPL), but businesses must get a commercial license from Oracle.

2.2 Front-end

2.2.1 HTML

The Hyper Text Markup Language, or HTML, is the standard markup language for texts meant to be displayed in a web browser. Technologies like Cascading Style Sheets (CSS) and programming languages like JavaScript can help with it. From a web server or local storage, web browsers accept HTML documents and transform them into multimedia web pages. HTML semantically explains the structure of a web page and initially provided signals for the look of the content. HTML components are the foundation of HTML pages. Images and other objects, such as interactive forms, can be embedded within the produced page using HTML structures. HTML allows you to generate organized documents by expressing structural semantics for text elements like headers, paragraphs, lists, links, quotations, and so on. HTML components are divided by tags, which are expressed in angle brackets. Tags like < image /> and < input /> insert material directly into the page. additional tags, such as <p>, surround and offer information about document content and may incorporate additional tags as subcomponents. Browsers do not display HTML tags, but instead utilize them to decipher the page's content.

2.2.2 CSS

CSS (Cascading Style Sheets) is a language used to describe the appearance of Web pages, such as colors, layout, and fonts. It makes it possible to modify the presentation to a variety of devices, including big monitors, small screens, and printers. Any XML-based markup language may be used with CSS because it is self-contained. The separation of HTML and CSS makes site maintenance easier, as well as sharing style sheets across pages and tailoring pages to diverse settings. This is known as separating structure (or substance) from appearance.

2.2.3 JavaScript

JavaScript is a dynamic programming language for computers It is a common component of websites and is lightweight. Client-side script can interact with users and generate dynamic pages thanks to implementations of this technology. It is an interpreted object-oriented programming language. JavaScript was originally known as Live Script, but Netscape changed its name to JavaScript, probably due to the enthusiasm caused by Java. JavaScript initially appeared in Netscape 2.0 in 1995 as Live Script. Netscape, Internet Explorer, and other Web browsers all feature the language's general-purpose core.

3. Algorithms

3.1 AES-256

The AES-256 (Advanced Encryption Standard 256-bit) algorithm is a popular symmetric encryption technique. It belongs to the AES family of encryption algorithms, which was chosen as the standard for safe data encryption by the National Institute of Standards and Technology (NIST). AES-256 operates on data blocks of 128 bits in size. It encrypts and decrypts data with a 256-bit private encryption key. The strength of AES-256 resides in its key length, which gives a high number of potential key combinations, making it computationally impossible to break the encryption by testing all possible keys. AES-256 performs a number of mathematical operations on the input data in numerous rounds, including substitution, permutation, and mixing. These rounds modify the data so that it is resistant to various cryptographic assaults like brute-force attacks, differential attacks, and linear attacks. AES-256's security is well-established and generally recognized, with no practical flaws or weaknesses identified. The cryptography community has exhaustively analyzed and tested it, and it is commonly used to safeguard sensitive data in a variety of applications, including secure communications, data storage, and personal information encryption. AES-256 is regarded as one of the most powerful symmetric encryption algorithms available today, delivering sensitive data with a high level of protection and secrecy. It is frequently used in sectors and organizations that require strong encryption to prevent unauthorized access to their data.

3.2 SHA-256

The Secure Hash Algorithm 256-bit (SHA-256) is a popular cryptographic hash algorithm. It is part of the SHA-2 algorithm family and is intended to provide a high level of security and data integrity. The SHA-256 algorithm generates a fixed-size 256-bit (32-byte) hash value from an input message. Because the resultant hash is unique to the input message, even little changes in the input message will result in a dramatically different hash value. The avalanche effect assures that any changes or tampering with the input message will be noticed, making SHA-256 excellent for maintaining data integrity. SHA-256 is computationally efficient and resistant to a wide range of assaults, including preimage attacks, second preimage attacks, and collision attacks. A preimage attack seeks the original input message that corresponds to a specific hash value, while a second preimage assault seeks a new input message that yields the same hash value. A collision attack seeks two distinct input messages that yield the same hash value. SHA-256 is widely utilized in different security applications due to its cryptographic strength, including digital signatures, password hashing, data integrity verification, and blockchain technology. It ensures the integrity and validity of data in digital systems by providing a high level of security.

4. Technical Requirements of The System

4.1 Hardware Requirements:

➢ System Processor: Core i3
➢ Hard Disk: 500 GB
➢ Ram: 4 GB

4.2 Software Requirements:

➢ Operating system: Windows 8 / 10
➢ Programming Language: Python
➢ Software Package: XAMP

5. Methodology

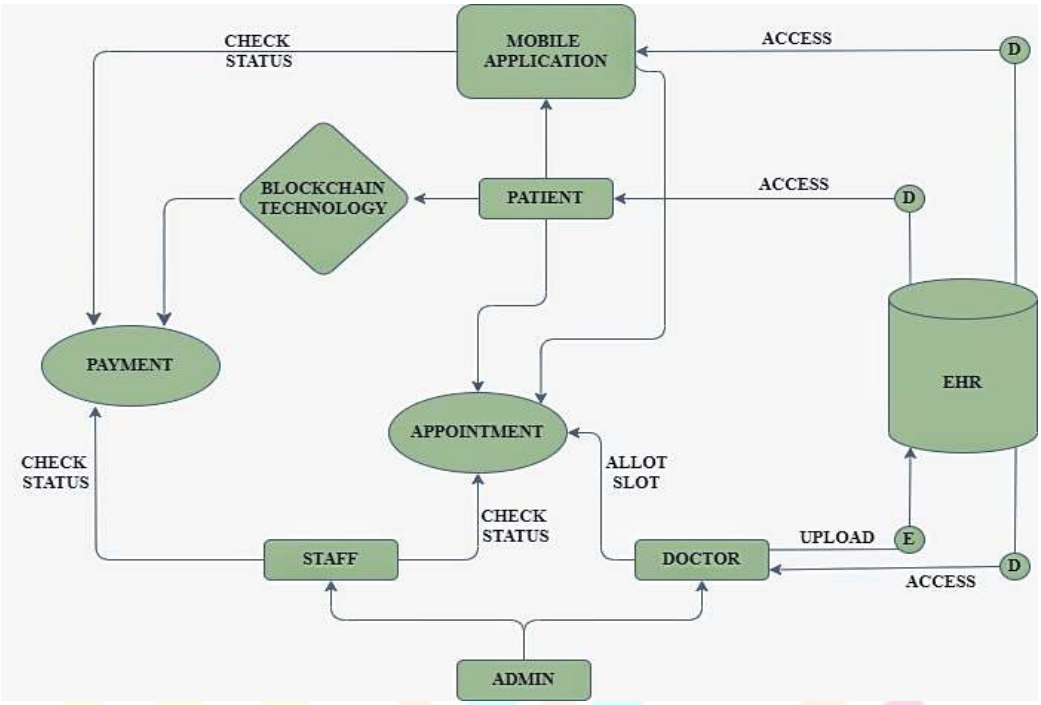
The methodology employed for the implementation of the System encompasses a systematic and structured approach, ensuring the successful execution of the project. The methodology's initial stage was to collect detailed requirements for the HealthCare Data Management System. Interviews were conducted with stakeholders like as administrators, staff members, physicians, and patients to determine their individual requirements and expectations. The needs obtained included user authentication, data administration, appointment scheduling, payment processing, and communication. After the collection of requirements, the following phase was system design. The system architecture, database structure, and user interfaces were all designed. The system architecture was created with scalability, security, and efficiency in mind. The database structure was designed to properly store and handle patient records, payment information, and other pertinent data. The user interfaces were created with a focus on usability and straightforward navigation in mind.

The deployment of the HealthCare Data Management System began once the system design phase was completed. XAMPP was used as the server environment, Python Django, a strong and popular web framework, was used as the implementation's backend framework. Django is a Python-based high-level framework that simplifies development and encourages code reusability and maintainability. It has capabilities like object-relational mapping (ORM) for easy database connectivity, URL routing, form handling, and session management, making it ideal for developing complicated online applications like the HealthCare Data Management System., and MySQL was chosen as the database management solution for storing and managing the data in the system. MySQL is a popular open-source relational database management system with high performance, scalability, and dependability. It has strong data storage and retrieval capabilities, allowing for the effective administration of patient health records, payment information, and other associated data. Standard web technologies were used for the system's front-end development. For content structuring, HTML (Hypertext Markup Language) was utilized, CSS (Cascading Style Sheets) for style and layout, and JavaScript for interaction and dynamic behavior. These front-end technologies enable the development of aesthetically beautiful and user-friendly interfaces, allowing patients, workers, physicians, and administrators to effortlessly engage with the system. To protect the security and confidentiality of patient health information, AES encryption techniques were used, while blockchain technology was used to provide safe and transparent payment processing.

AES (Advanced Encryption Standard) encryption algorithms were included in the system to protect the security and confidentiality of patient health records. AES is a commonly used encryption method that ensures the security and secrecy of sensitive data. The solution reduces the danger of unauthorized access and preserves patient privacy by encrypting patient health information. Blockchain technology was used to make payment processing safer and more transparent within the HealthCare Data Management System. The solution secures the immutability and integrity of payment records, eliminates the need for middlemen, and offers a decentralized and tamper-proof ledger for recording and validating payment transactions by utilizing blockchain. Blockchain uses the SHA-256 algorithm, which ensures great data integrity and security. SHA-256 ensures tamper-resistant records, transparent

transactions, and fast processing. It is resistant to collision attacks, increases trust, and adheres to security requirements. The implementation phase brought the system concept to existence by utilizing these technologies, including the essential tools and features to produce a strong, secure, and efficient HealthCare Data Management System.

ARCHITECTURE



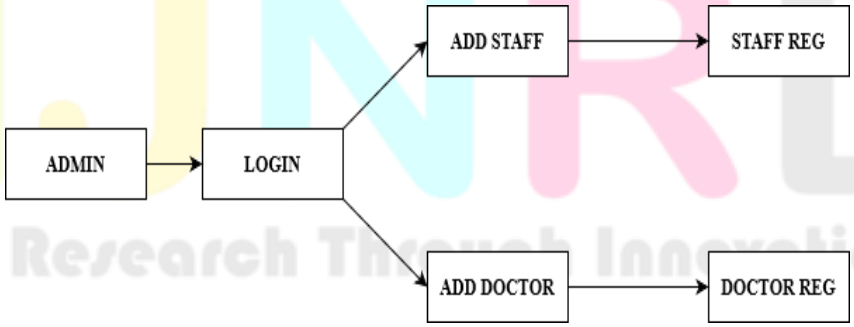
The System is built on the XAMPP server environment, utilizing Python Django as the backend framework. MySQL is used as the database management system to store and retrieve data. The frontend is developed using HTML, CSS, and JavaScript to create user-friendly interfaces. The system architecture incorporates modular components for staff, patients, doctors, and administrators, ensuring efficient data management and secure communication.

1. Modular Overview

The proposed architecture is divided into four modules:

- ADMIN
- STAFF
- PATIENT
- DOCTOR

1.1 Admin



Admin Login:

- The admin can securely log into the system using a unique user ID and password combination.

Registration Form Management:

- The admin has the responsibility to handle the registration forms of staff members and doctors.
- This includes reviewing and processing the registration information submitted by staff and doctors.

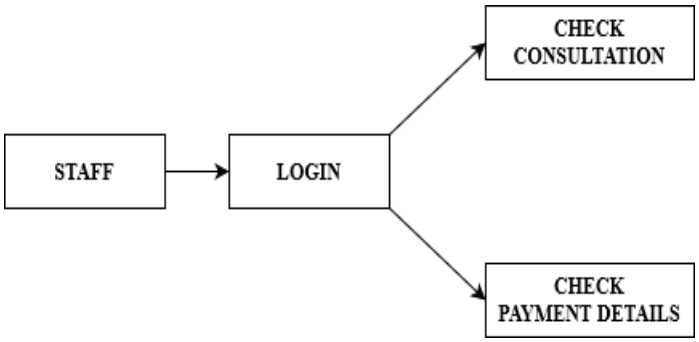
Staff and Doctor Management:

- Once logged in, the admin has the authority to add staff members and doctors to the website.
- This involves entering their relevant details, such as personal information, contact information, and professional qualifications.

Supervision of the Entire System:

- As the admin, they have the overarching responsibility of supervising and overseeing the entire HealthCare Data Management System.
- This includes monitoring system activities, ensuring compliance with regulations and policies, and addressing any issues or concerns that may arise.

1.2 Staff



Staff Login:

- Staff members can securely log into the system using their registered email ID and password.

Payment Status:

- Once logged in, staff members have the ability to check the payment status of patients.
- This includes accessing information regarding the payment history, outstanding payments, and payment confirmations.

Consultation Details:

- Staff members can view and access consultation details of patients.
- This includes information such as appointment schedules, previous consultations, and treatment plans.

Staff members play an important part in the system, resolving payment issues and guaranteeing correct and up-to-date consultation information. Staff members may easily manage payment-related enquiries and offer required information on patient consultations by using their login credentials, adding to the System's overall efficacy and seamless operation.

1.3 Patient

Patient Login:

- Patients can securely log into the system using their unique user ID and password.

Profile Viewing:

- Once logged in, patients can view and access their personal profile.
- This includes details such as name, contact information, address, and other relevant information.

Prescription Viewing:

- Patients can access and view their prescribed medications and treatment plans in the consulting section.
- This provides patients with easy access to their medical prescriptions and allows them to stay informed about their healthcare instructions.

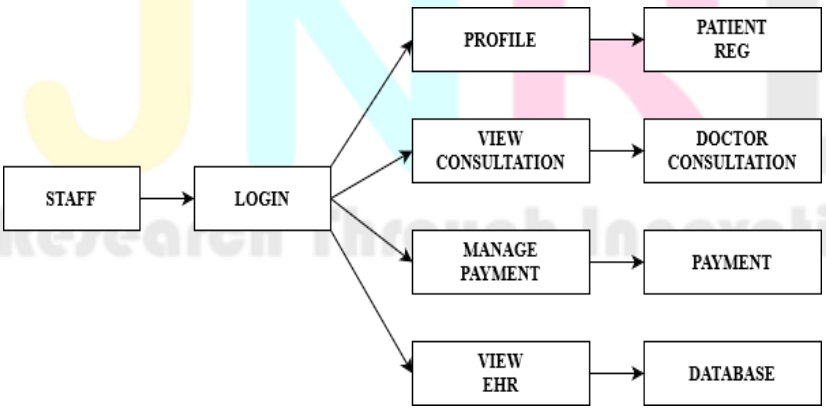
Easy Payment:

- Patients can conveniently pay their fees using a user-friendly payment system integrated into the website.
- This simplifies the payment process for patients, ensuring a hassle-free experience.

Health Records Viewing:

- Patients have the ability to view their health records stored within the system.
- This includes medical history, laboratory test results, diagnoses, and other relevant health-related information.

The patient role in the System is intended to give patients easy access to their profile information, prescription data, payment choices, and health records. By incorporating these features, the system hopes to improve patient participation, ease, and transparency in healthcare administration.



1.4 Doctor

Doctor Login:

- Doctors can securely log into the system using their unique user ID and password.

Consultation Management:

- Once logged in, doctors can add consultations for patients.
- This includes recording details of the consultation, such as diagnosis, treatment plans, and medications prescribed.

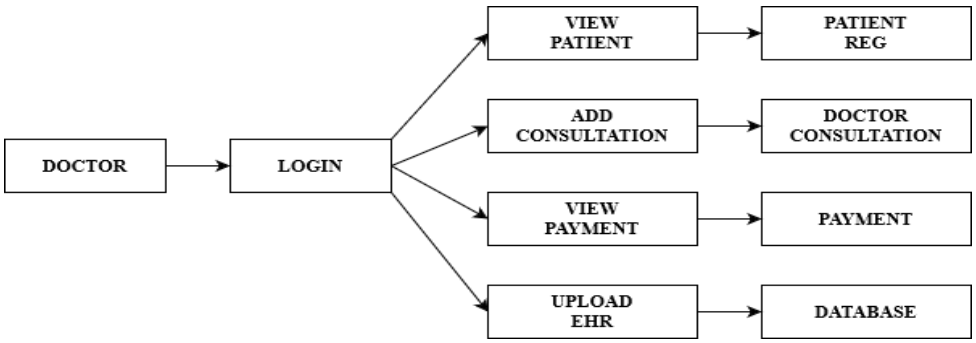
Payment Details:

- Doctors have the ability to view payment details of patients.
- This includes accessing information about payment history, outstanding payments, and payment confirmations.

Medical Records Management:

- Doctors can upload and view medical records of patients within the system.
- This enables doctors to access and review patient medical histories, test results, and other relevant healthcare information.

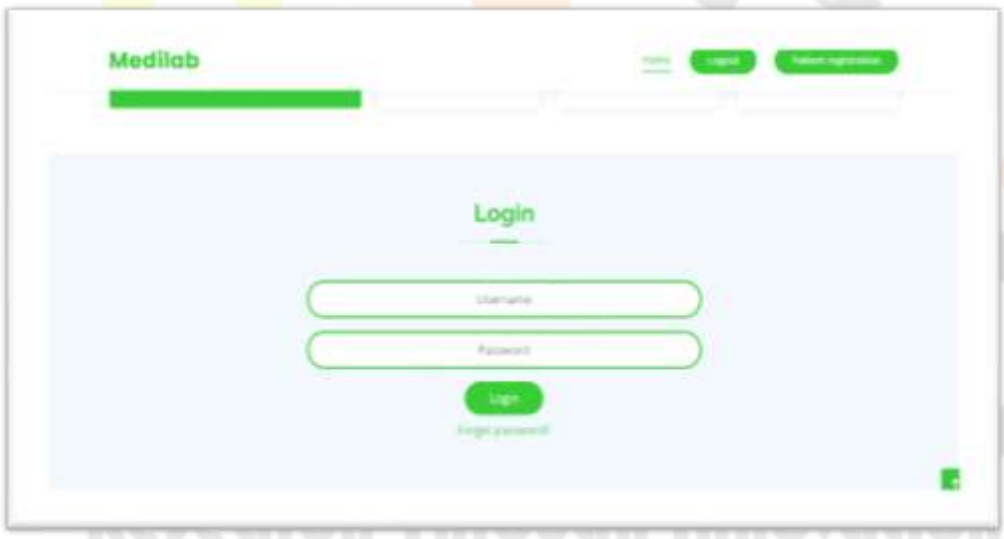
The function of the doctor within the System is critical in providing high-quality healthcare services. Doctors can conveniently organize consultations, retrieve payment data, and securely preserve patient medical records by using their login credentials. This improves the overall efficiency and efficacy of healthcare delivery, resulting in better patient care.



RESULT

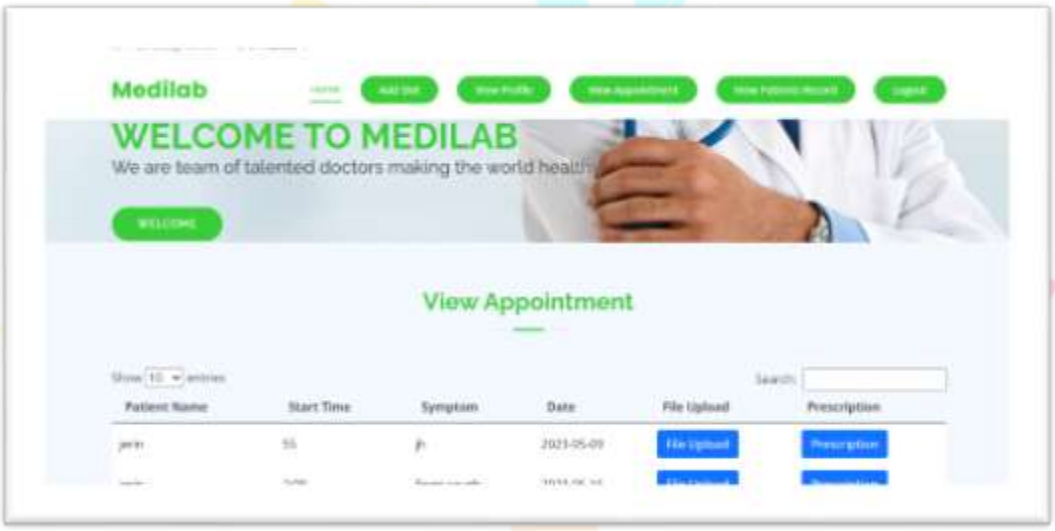
The project goal of the HealthCare Data Management System was to improve data security and streamline financial operations in the healthcare business. The project successfully deployed AES encryption for secure health record administration, assuring patient data security and integrity. Furthermore, blockchain technology was incorporated into the system to provide transparent and secure payment processing, decreasing fraud risks and enhancing financial transaction efficiency. The system was built with four modules: staff, patient, doctor, and admin, each with its own set of features geared to their respective user roles. A mobile application interface was added in the patient module, providing easy access to health information, appointment management, and payment processing. A user-friendly interface was prioritized throughout the project to provide simplicity of use and navigation for all system users. As a result of the initiative, data security, operational efficiency, and patient experience have all improved significantly. Administrative activities were streamlined, resulting in enhanced productivity for healthcare professionals and administrators by decreasing manual paperwork and optimizing operations. The approach also encouraged good communication and collaboration among healthcare stakeholders, which improved coordination and patient care. Compliance with privacy standards such as HIPAA was maintained, assuring patient information protection. Overall, the project's deployment produced favorable outcomes, providing healthcare organizations with a safe and efficient platform for managing patient data and financial activities.

1. Screenshots

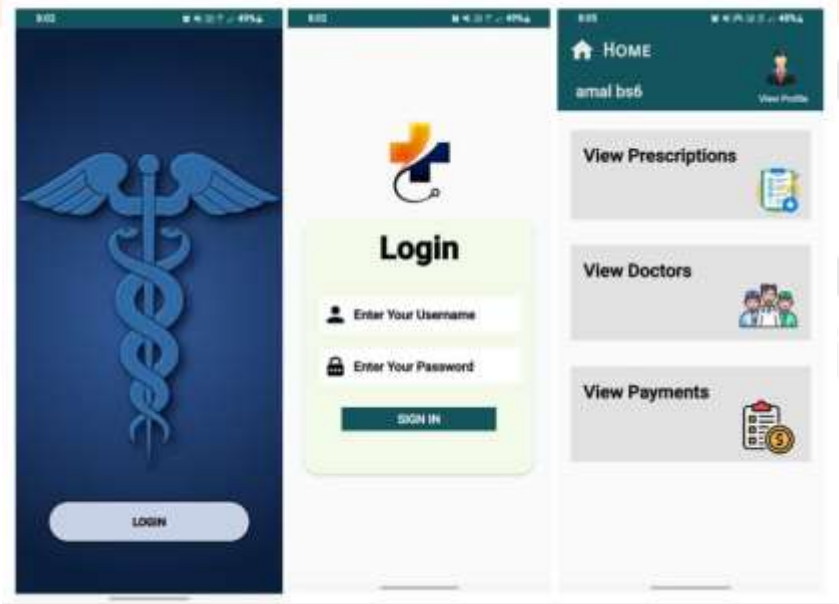


Registration Page

Patient interface



Doctor Interface



Mobile Application Interface

REFERENCES

[1] O. AlSheikSalem and M. S. Al-Ani, "Mobile cloud computing applied to healthcare approach," International Journal of Information Technology Convergence and Services, vol. 6, no. 5, pp. 1–8, 2016.

[2] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute based access control," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2130–2145, 2018.

[3] R. Sánchez-Guerrero, F. A. Mendoza, D. Diaz-Sanchez, P. A. Cabarcos, and A. M. López, "Collaborative eHealth Meets Security: Privacy-Enhancing Patient Profile Management," IEEE Journal of Biomedical and Health Informatics, vol. 21, no. 6, pp. 1741–1749, 2017.

[4] M. Padmashree, S. Khanum, J. Arunalatha, and K. Venugopal, "SIRLC: Secure Information Retrieval using Lightweight Cryptography in HIoT," in IEEE Region 10 Conference TENCON, 2019, pp. 269–273.

[5] J. Ködmön and Z. E. Csajbók, "Információbiztonság az egészségügyben," Orvosi Hetilap, vol. 156, no. 27, pp. 1075–1080, 2015.