Enhancing the Data Security in Healthcare System

Teki Saikrishna, Kallam Thanuja, Devarapalli Tejaswi and Krovvidi Prudhvi Nagaraju
Department of Advanced Computer Science and Engineering, Vignan's Foundation for Science, Technology & Research (Deemed to be University), Vadlamudi, Guntur (Dt)-522213, Andhra Pradesh, India

Keywords: Appointment Scheduling, Billing Management, Medical Record Updates, Notification System, Security Measures: HL7, SQL Injection Attack (SQLi), AES Encryption Technique, XSS Attack, Password Hashing.

Abstract: Hospital Management System (HMS) using MERN stack (MongoDBExpress. js, React, Node. js) to help hospitals operate more efficiently while safeguarding sensitive patient information. Sensitive information like patient records are secured via encryption and decryption with AES methods. The admins have it under control regarding the staff accounts. The receptionist can only register patients and encrypted information is securely saved in MySQL. When a doctor needs to consult or treat the patient, the decrypted patient information will be available for him/her.

1 INTRODUCTION

The healthcare sector is increasingly adopting digital solutions to streamline operations and enhance patient care. An effective Hospital Management System (HMS) is essential for enabling hospitals to carry out daily functions such as patient registration, managing medical records, making appointments, managing billing, and much more! Yet, as the industry shifts deeper into digital systems, safeguarding sensitive health records has become increasingly critical. Sensitive information including patient records, personal identification information, and billing details must be protected from unauthorized users, hacking, and data exfiltration. Protecting this information is critical for maintaining trust and ensuring adequate medical care. Classic hospital management systems focus on functionality and operational efficiency but generally lack protection against sophisticated cyber threats. Security vulnerabilities like SQL Injection (SQLi) (Zhang H et., al. 2018) (D. A. Kindy and A. K. Pathan, 2011) and Cross-Site Scripting (XSS) (M. I. P. Salas and E. Martins, 2014). Can put the privacy and integrity of sensitive medical data at risk. HMS (Hospital Management System) to MERN stack (MongoDB, Express. js, React, Node. js) for its scalability while adding modern security layers to secure sensitive health data. System uses AES encryption and decryption to ensure the data is protected and the patient data is not disclosed. Moreover, by integrating a Cyber Attack Detection (MCAD) module, the system becomes capable of recognizing and neutralizing sophisticated document-based attacks, such as SQL (Zhang H et., al. 2018) and NoSQL injections, XSS, and command injections, leading to a more resilient cybersecurity approach. Figure 1 shows the block diagram of SQL injection attack.

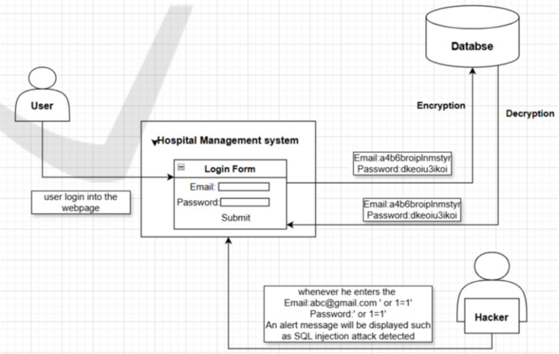


Figure 1: Block diagram of SQL injection attack.

It also follows HL7 international standards (2021) (2021) to provide interoperability between heterogeneous Healthcare systems. Moreover, a DoS attack detection module has been incorporated to prevent potential service disruption by malicious users. This project aims at creating a hospital management system as well as research into a strong security framework around it to meet the pathogenic Cybersecurity threats encountered in the healthcare

Saikrishna, T., Thanuja, K., Tejaswi, D. and Nagaraju, K. P.
Enhancing the Data Security in Healthcare System.
DOI: 10.5220/0013902800004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 3*, pages 609-617
ISBN: 978-989-758-777-1

domain. Such a system may help protect patient data, maintain privacy and create a safe atmosphere for the working of the hospital. In the healthcare industry, one of the challenges is operating the hospital while keeping the patient data secure and private. Current systems often have difficulty integrating hospital functions, such as staff management, patient registration, appointment, and billing, and applying these healthcare standards (e.g., HL7 (2021)) to them. In addition, there are fears of unauthorized access to sensitive patient data and attacks with DoS vulnerabilities. This common occurrence results in inefficiencies, data breaches and interruptions in service delivery. The following project is a hospital management system using the MERN stack that will manage hospital operations in a simplified manner. You will use Hassan, M., Saeed, M. (2021). AES encryption and password hashing to secure sensitive data to keep the integrity and confidentiality. Data processing of patient data from managing medical records to billing will also be incorporated into the system to achieve a secure patient management system (HIMSS) (2022). It will also support interoperable data transfer with other healthcare systems via encrypted HL7 data exchanges (2021). In addition, this system will include a detection module for DoS attacks, which is essential to prevent service disruptions, providing enhanced security and scalability and reliability.

2 LITERATURE SURVEY

In the literature review, previous studies and research on the hospital management system, data security in healthcare, cyber-attacks, and technologies to improve protection of healthcare systems will be explored. This review aims to identify the existing gaps and limitations of current systems and explain how this research is adding value to existing evidence.

Exasperation in healthcare management system: History and Evolution of Hospital Management Systems Hospital management systems have been widely adopted throughout healthcare for digital transformation. Sharma et al. (2018), HMS has simplified many aspects of the hospital to improve operations including patient records, appointment scheduling and billing management. These systems indeed help streamline operations, but Patel and Patel (2019) states that they do not enforce strong security practices, leaving hospital data open to cyber raids. The majority of existing HMS solutions depend on simple practices encryption and networks cut off; few incorporate extended solution layers which create automated, real-time attack detection systems or security intrusion prevention measures. Zhang et al. (2017) claimed that hospitals SQL Injection, XSS, and DoS attacks are the most common attacks targeting healthcare systems as a whole due to the vulnerabilities present within the software associated with hospital management. Consequently, these vulnerabilities leave a void in protecting patient data and this research aims to fill in that void. HL7 (2021) Security and communication networks: In healthcare, securing patient data is not merely a technical necessity; it's a core duty. Medical records contain particularly sensitive information, so ensuring that they are secure is paramount. Cheng et al. (2020) studied various encryption methods to secure electronic health records (EHRs), finding that AES encryption is one of the most preferred and suitable standards. While a number of healthcare systems that use encryption, there's often little emphasis on end-to-end security, especially when data transfers between various systems and providers. Bambang et al. (2018) that emphasized the necessity of encrypting data at rest and in transit, but few studies have tried to address the specific challenges of providing access to data across distributed healthcare systems in which multiple actors require access. This research intends to fill that void by embedding the AES encryption algorithm within the MERN stack architecture to ensure that patient data stays secure at every point in transit, exchange, and access amid healthcare domains.

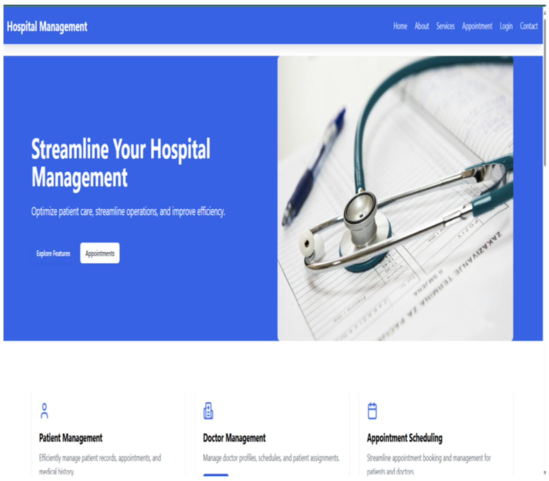
3 METHODOLOGY

The methodology of this research is centered towards the implementation of a Hospital Management System (HMS) that offers increased efficiency in hospital operation management along with improved security for sensitive healthcare data. In this section we present the research design: the methods and techniques used in the development/evaluation of the system and the proposed model/algorithm for cybersecurity detection and encryption/system architecture.

System Design and Development.

The Hospital Management System (HMS) development using the MERN stack (MongoDB, Express. js, React, Node. js) and MySQL for storing data. The system has a set of functionalities, which include: Appointment booking Patient management medical records notifications the development is being done following the agile development methodology, so we can always continuously test it and obtain feedback. The main elements of the system are:

- **Frontend:** Built with React. js, offering a dynamic and responsive interface for administrators, doctors, receptionists and patients.
- **Backend:** Express Built backend using express. js and Node. js, managing API requests, role-based access, encryption and communication with the database.
- **Database:** Patient records are stored securely using MySQL, and data is encrypted with AES encryption.
- Cybersecurity Validation through Simulations to validate the security features of the system, simulations, and experiments are conducted to assess how the system performs under different threat scenarios.
- **These include:** SQL Injection, XSS attack simulations evaluating the system's ability to detect and block SQL Injection and Cross-Site Scripting (XSS) attacks using adaptive machine learning models. The implementation methodology adopts a systematic approach:
- **MERN Stack:** The MERN stack is a full-stack JavaScript framework designed for building interactive web applications. It comprises four core technologies: MongoDB, Express, ReactJS, and NodeJS.
- **MongoDB:** Manages the storage and retrieval of unstructured patient data within a NoSQL database. Express.js– Handles API and middleware for backend frameworks.
- **React.js:** Used for user interface development in dynamic websites. Node.js– Server-side processing is done via this JavaScript runtime environment.
- **Security Technologies:** These include protecting the patient's sensitive information from any unauthorized access to maintain the confidentiality, Integrity, and Availability of the data. Figure 2 shows the Home Page of hospital management system.
- **AES Encryption:** It is a strong encryption algorithm that safeguards the sensitive data of patients during storage and retrieval.
- **AES Encryption:** It is a strong encryption algorithm that safeguards the sensitive data of patients during storage and retrieval.



Streamline Your Hospital Management

Optimize patient care, streamline operations, and improve efficiency.

Patient Management

Efficiently manage patient records, appointments, and medical history.

Doctor Management

Manage doctor profiles, schedules, and patient assignments.

Appointment Scheduling

Streamline appointment booking and management for patients and doctors.

Figure 2: Home page of hospital management system.

- **JWT (JSON Web Token):** For secure authentication a role-based access control (RBAC).
- **Bcrypt.js:** Enables the hashing of passwords for safer storage.
- **HL7 (Health Level Seven):** It is a new standard that is similar to the GDPR and HIPAA. The HL7 (Health Level Seven) standard mainly focuses on protecting healthcare data when the data is exchanged between the web application and the database.
- **Cybersecurity Threat Detection:** Detecting Cyber threats such as SQL Injection, XSS, NoSQL Injection, and DoS attacks is essential for maintaining the security of web applications. One common attack method involves hackers inputting malicious SQL commands like'' or 1=1' '— into a login form. If successful, this can grant them unauthorized access to sensitive data or even control over the system.

4 RESULTS AND DISCUSSIONS

To safeguard against such attacks, our system continuously monitors for any suspicious inputs. If someone tries to enter a potentially harmful command in the login field, an alert is immediately triggered, preventing unauthorized access. This proactive security measure helps protect sensitive information and ensures that the system remains safe for legitimate users.

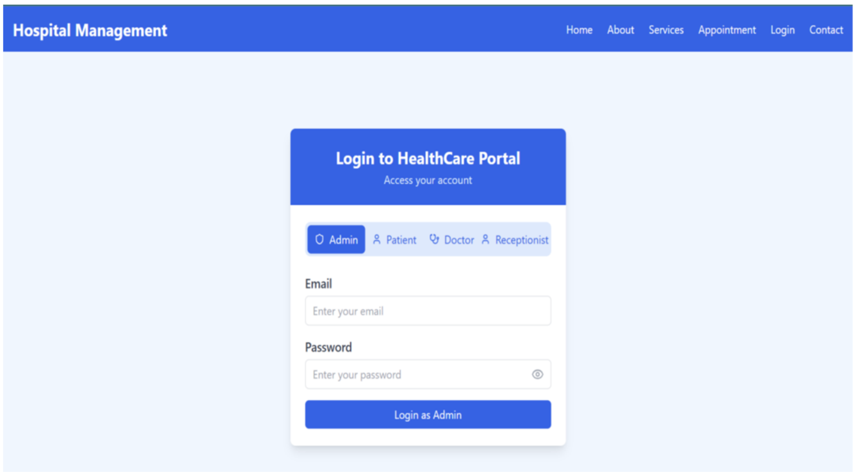


Figure 3: Login page.

The image in figure 3 shows the login page of our Hospital Management System. It includes separate login forms for different users, such as administrators, doctors, patients, and receptionists, ensuring that each person can securely access their respective information.

1. ADMIN: Figure 4 represents the dashboard of an admin page, where the admin has access to add the doctors belonging to different departments and receptionists and he can also check who all the available patients present in the hospital are.

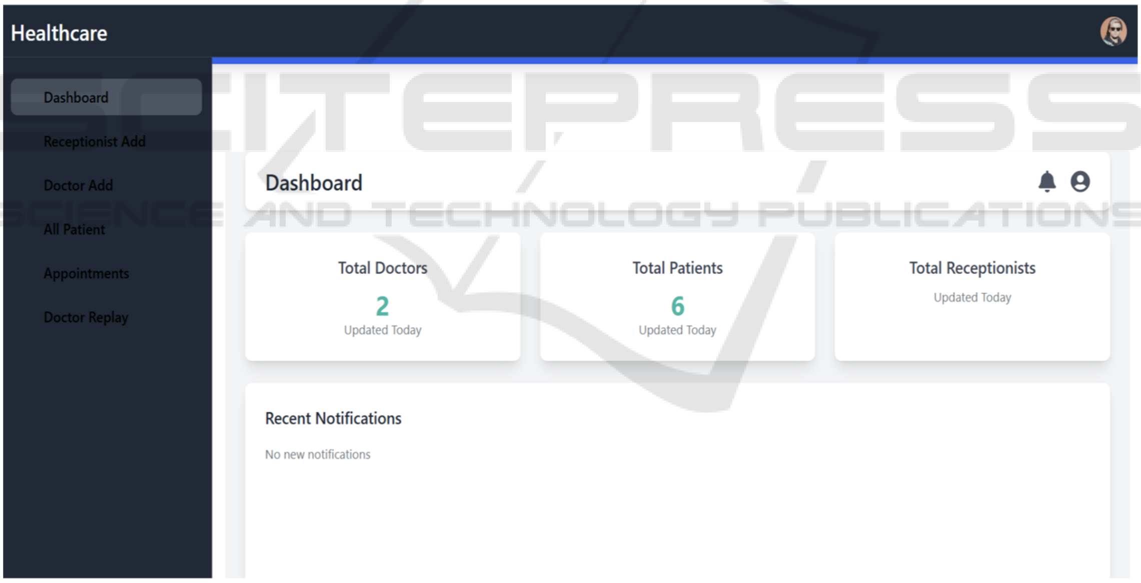
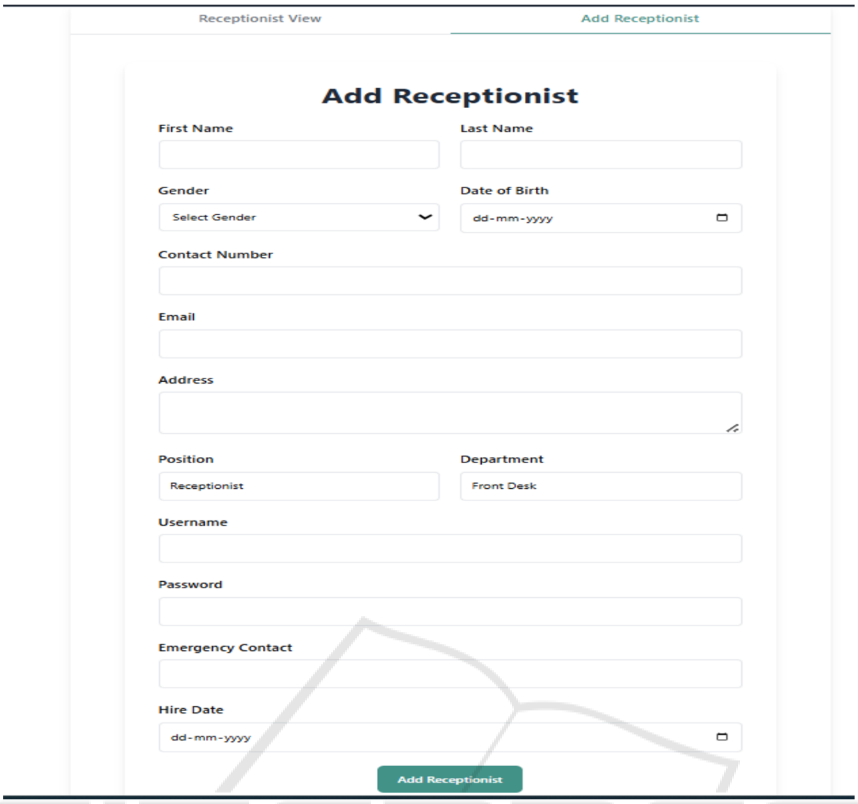


Figure 4: Admin dashboard.

In Figure 5, the admin is going to enter all the information related to the receptionist, and he can view all the receptionists present in the hospital along with their details, such as first name, last name, contact number, and date of birth. The admin can also edit the information related to a particular receptionist, and he can delete the receptionist from the list once they resign from their job. Figure 6 shows the page for Form for adding Doctors.



Receptionist View | Add Receptionist

Add Receptionist

First Name

Last Name

Gender: Select Gender

Date of Birth: dd-mm-yyyy

Contact Number

Email

Address

Position: Receptionist

Department: Front Desk

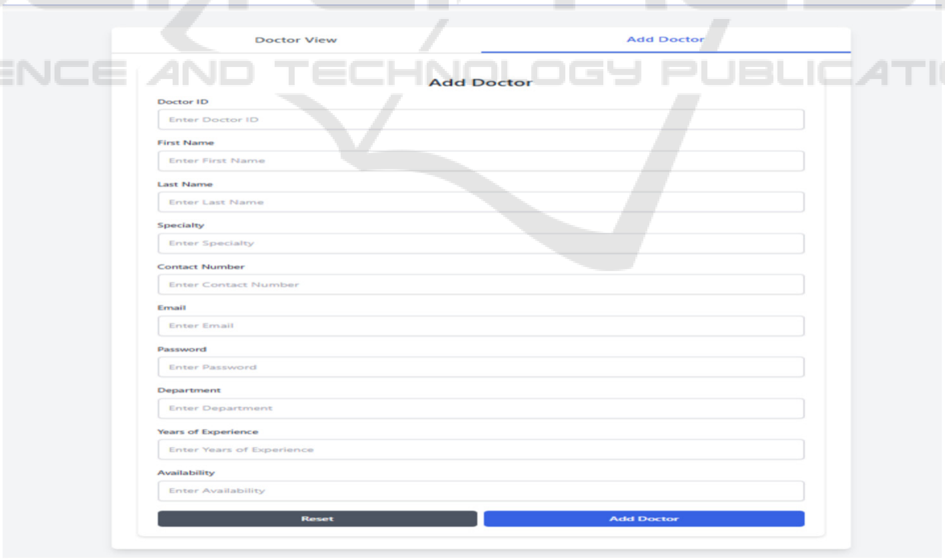
Username

Password

Emergency Contact

Hire Date: dd-mm-yyyy

Figure 5: Form for adding receptionist.



Doctor View | Add Doctor

Add Doctor

Doctor ID: Enter Doctor ID

First Name: Enter First Name

Last Name: Enter Last Name

Specialty: Enter Specialty

Contact Number: Enter Contact Number

Email: Enter Email

Password: Enter Password

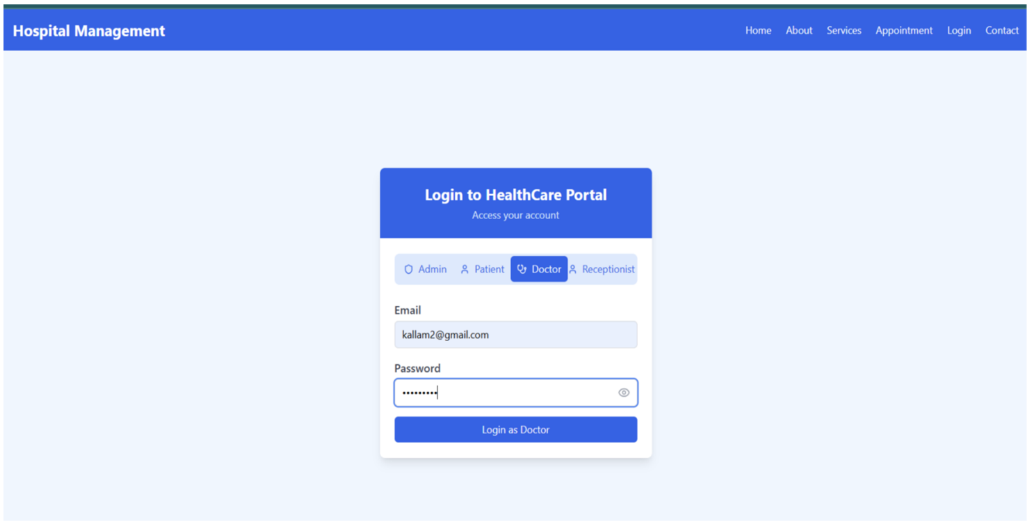
Department: Enter Department

Years of Experience: Enter Years of Experience

Availability: Enter Availability

Figure 6: Form for adding doctors.

2. DOCTOR: The figure 7 represents the login page for the doctor. Whenever the doctor logs in with their respective email and password, the dashboard will be displayed, consisting of their personal information such as name, email, specialization, years of experience, contact number, and availability i.e.,whether he/she is available 24/7 or not.



Email: kallam2@gmail.com

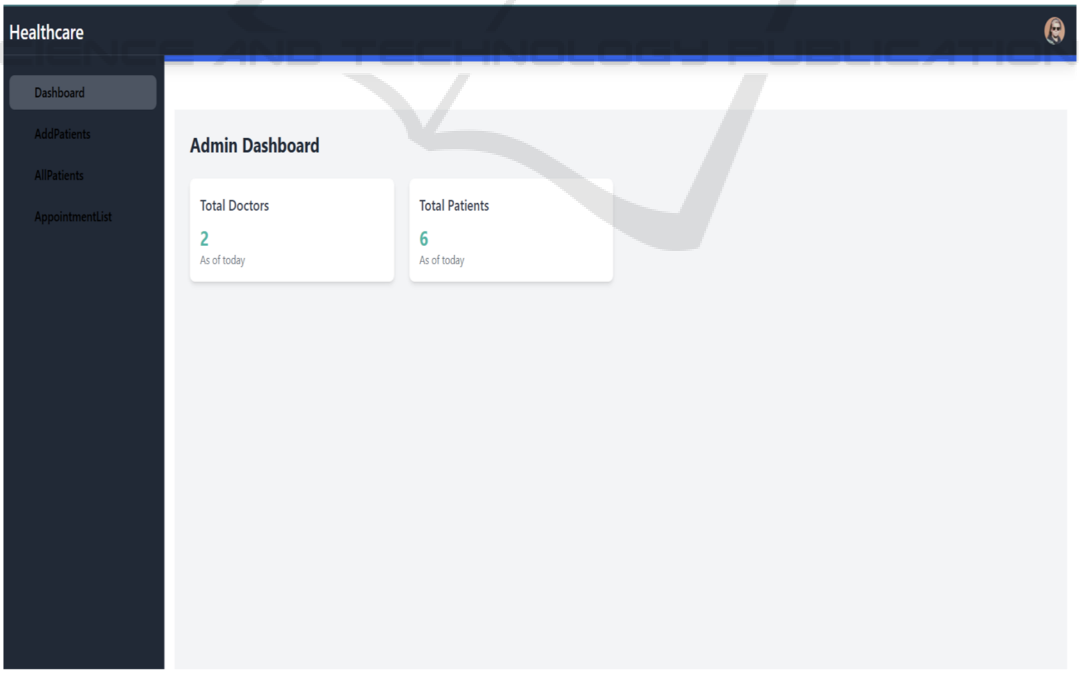
Password: •••••••••

Figure 7: Doctor login page.

In their particular dashboard he can also see who are the patients assigned to him and he can also give the prescriptions for the patients who have been under his consideration and the patients who have booked an appointment.

3. PATIENT: Whenever a patient logs in with their particular email he/she will be redirected to another web page which consists of his/her personal information such as patient ID, email, symptoms, health condition, assigned doctor, etc. The patient can also see the reply given by the doctor about his/her condition.

4. RECEPTIONIST: Receptionist has access to add new patients and can view the list of available patients in the hospital (figure 8).



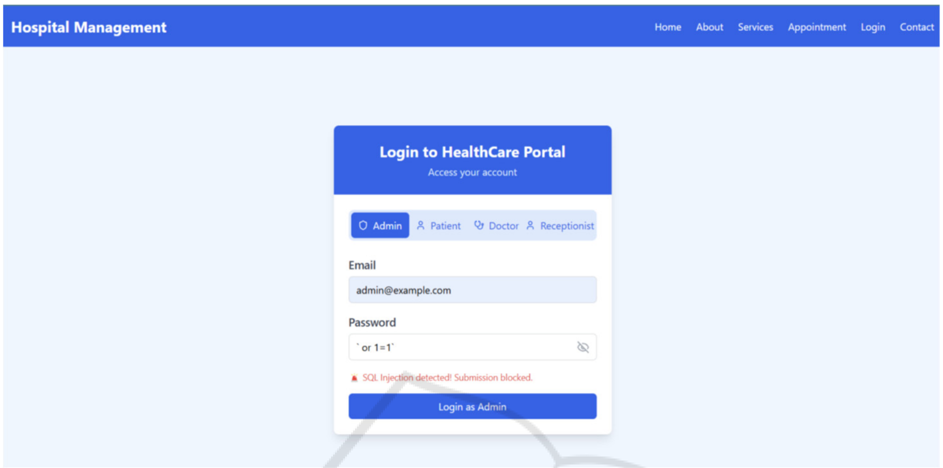
Total Doctors: 2 (As of today)

Total Patients: 6 (As of today)

Figure 8: Receptionist dashboard.

5 ATTACKS PERFORMED ON HOSPITAL MANAGEMENT SYSTEM

SQL INJECTION ATTACK: SQL Injection is a widespread security vulnerability in web applications that occurs when attackers insert harmful SQL code into input fields. This can enable them to access confidential data, modify database records, or even gain control over the system. Understanding and mitigating SQL Injection is one of the corner stones of web application security in protecting user data (figure 9).



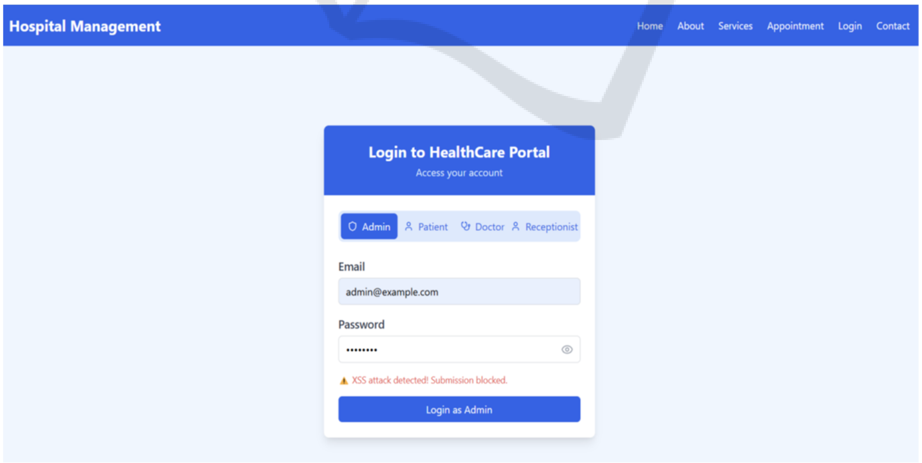
Email
admin@example.com

Password
` or 1=1`

SQL Injection detected! Submission blocked.

Figure 9: Prevention of SQL injection attack.

XSS ATTACK: A Reflected Cross-Site Scripting vulnerability in canonical link tag occurs when an attacker trick a user into clicking on a URL parameter with a manipulated value that contains malicious code. When a user clicks that URL, their browser unknowingly executes the malicious code which can result in major security problems. Such an attack is capable of endangering user data and even changing the content of a website. It underscores the need for strong security measures to detect and block such threats (figure 10).



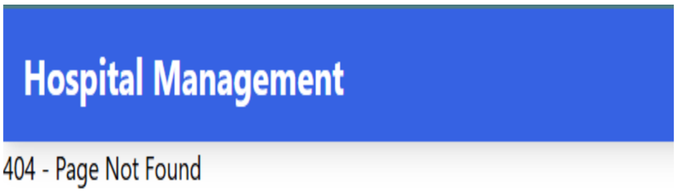
Email
admin@example.com

Password
••••••••

⚠ XSS attack detected! Submission blocked.

Figure 10: Prevention of XSS attack.

When the attacker attempts to input any XSS header, such as the tag, an alert message will display and the attacker will not be able to log in to the web page. Otherwise, every time the attacker attempts to change the URL of the web page, it outputs the result shown in Figure 11, indicating that '404 - Page Not Found'.

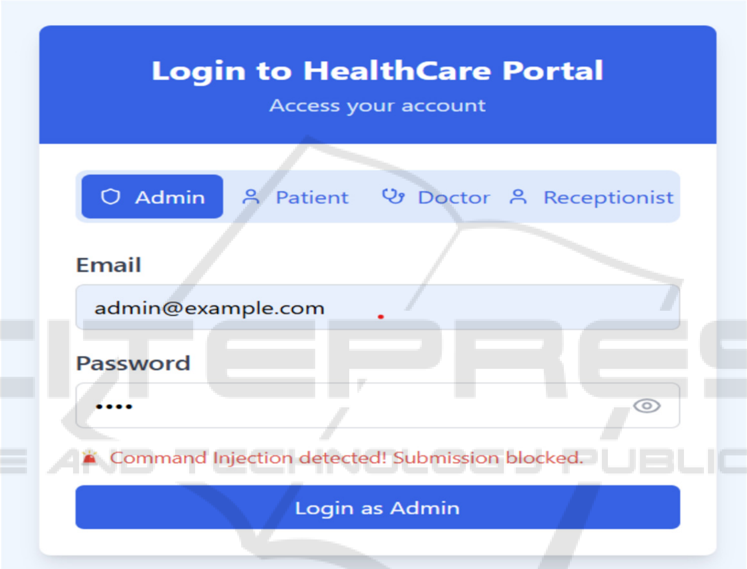


Hospital Management

404 - Page Not Found

Figure 11: Prevention of XSS attack.

COMMAND INJECTION ATACK: When hackers make a web, app execute undesirable operating system commands that is what we call a command injection attack. The attacker may leverage the vulnerabilities found within the application to inject and execute harmful commands. This can result in data breaches, manipulation of the web application, or other security threats, hence it is important to secure your applications against such attacks (figure 12).



Login to HealthCare Portal

Access your account

Email

admin@example.com

Password

••••

Command Injection detected! Submission blocked.

Figure 12: Prevention of command injection attack.

6 CONCLUSIONS

The paper contributes to an efficient and effective Hospital Management System (HMS) based on MERN stack through eliminating the various issues on data security in the health care system. Our research emphasises the need to have Solid Security measures in place that can keep sensitive patient information from unauthorised access and a host of cyber threats. The introduction of encryption using a method such as AES, as well as enhanced cybersecurity implementations with attack detection methods like SQL injection (SQLi) detection and Cross-Site Scripting (XSS) detection, helps to improve the security of medical records substantially. Therefore, the existence of these helps ensure the confidentiality and integrity of patient data, and the overall safety of patient information in the medical environment. This confirms that by integrating these security protocols, the overall efficiency of hospitals is improved while remaining compliant in ensuring the confidentiality and integrity of patient data. Our system supports secure data sharing between different healthcare systems, following HL7 standards to meet compliance requirements & ensuring interoperability. Nonetheless, we acknowledge that there are hurdles to overcome in terms of ongoing staff training and system updates, especially with the rapidly changing landscape of cyber threats. It will be significant for future research to design adaptive security measures robust against prospective attacks that can respond to new threats in real-time. In summary, securing your hospital management system records is fundamental to ensure patient trust and providing quality services. With the ongoing digital transformation across the healthcare landscape, it is essential that every link in the chain places a high priority on data security and plan out a world where patient data is respected and protected. This sets the stage for continued research into novel security mechanisms that can adequately address the evolving threats present within the healthcare domain.

REFERENCES

Ariani, M., Wulandari, R. (2021). “Improving Security in Healthcare Information Systems: A Case Study of Data Breaches and Mitigation Strategies.” Procedia Computer Science, 179, 110- 118. doi:10.1016/j.procs.2021.01.016

Cybersecurity Challenges in Hospital Management Systems: Vulnerabilities and the Need for Enhanced Protection” by Sharma et al. (2018), Patel and Patel (2019), Zhang et al. (2017).

D. A. Kindy and A. K. Pathan,” A Survey on SQL Injection: Vulnerabilities, Attacks, and Prevention Techniques 2011 IEEE.

Hassan, M., Saeed, M. (2021). “A Comprehensive Survey on Cyber- Attacks in Healthcare Systems: Vulnerabilities, Threats, and Countermeasures.” Computers, Materials Continua, 67(1), 533- 550.doi:10.32604/cmc.2021.014298

Hassan, M., Saeed, M. (2021). “A Comprehensive Survey on Cyber- Attacks in Healthcare Systems: Vulnerabilities, Threats, and Countermeasures.” Computers, Materials Continua, 67(1), 533- 550. doi:10.32604/cmc.2021.014298

Health Level Seven International (HL7). (2021). HL7 Standards Overview. Retrieved from https://www.hl7.org/

Health Level Seven International (HL7). (2021). HL7 Standards Overview. Retrieved from https://www.hl7.org/3.

Healthcare Information and Management Systems Society (HIMSS). (2022). Cybersecurity in Healthcare: Protecting Patient Data and Information. HIMSS Analytics. Retrieved from https://www.himss.org/

M. I. P. Salas and E. Martins, “Security testing methodology for vulnerabilities detection of XSS in web services and ws-security,” Electron Notes in Theoretical Computer Science, vol. 302, pp. 133–154, 2014

National Institute of Standards and Technology (NIST). (2020). Cybersecurity Framework for Healthcare. NIST Special Publication 800-53. Retrieved from https://www.nist.gov/cybersecurity-framework

Patel, R., Shah, N. (2021). ”Machine Learning-Based Cyber-Attack Detection in Healthcare: A Review.” Journal of Healthcare Cybersecurity, 6(2), 112-128. doi:10.1109/JHCS.2021.3045.

Zhang H, Zhang X. " SQL injection attack principles and preventive techniques for PHP site,” in Proceedings of the 2nd International Conference on Computer Science and Application Engineering.2018;1-9.