International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Secure Online Patient Appointment Booking and Encrypted Medical History Management

Pervala Renu Sri, E. Vishveshwar*

Vaagdevi Engineering College, Warangal, 506005, Telangana, India.

*Correspondence: E. Vishveshwar

ABSTRACT

The rapid digital transformation of healthcare services has created a strong demand for secure, efficient, and user-friendly systems to manage patient appointments and sensitive medical information. Historically, healthcare institutions relied on manual registers and isolated digital tools for appointment scheduling and record maintenance, which often resulted in inefficiencies, data inconsistency, and limited accessibility. The problem is further intensified by the increasing volume of patients, the need for timely medical services, and strict requirements for data confidentiality. Traditional systems lack centralized control, real-time updates, strong authentication mechanisms, and adequate protection for sensitive medical data, making them prone to errors, delays, and security vulnerabilities. These limitations highlight the need for a robust digital solution that can streamline scheduling workflows while ensuring secure handling of patient information. To address these challenges, this research proposes a secure online patient appointment booking and encrypted medical history management system built using a web-based architecture. This research integrates structured backend processing with Flask, secure data persistence using SQL Alchemy (SQLA), Object Relational Mapper (ORM), and encrypted user authentication through bcrypt hashing (BCH). Role-based access control (RBAC) ensures that patients and administrators access only authorized functionalities, while automated workflows reduce manual intervention and scheduling conflicts. The system also provides dynamic dashboards for improved visibility and decision-making. The significance of this research lies in its ability to enhance operational efficiency, improve data security, and support scalable healthcare service delivery. By combining secure authentication, structured data management, and intuitive user interaction, the system demonstrates a reliable and performance-optimized approach suitable for modern healthcare environments. The proposed solution not only overcomes the limitations of traditional appointment systems but also establishes a strong foundation for future digital healthcare applications.

Key words: Online Patient Appointment System, Medical Data Security, Role-Based Access Control, Healthcare Information Systems, Hashing, Secure Healthcare Applications.

INTRODUCTION

Healthcare has undergone a significant digital transformation over the past few decades, driven by rapid advancements in information technology, mobile computing, cloud platforms, and intelligent healthcare systems. Hospitals, clinics, and healthcare providers now generate enormous volumes of medical information through Electronic Health Records (EHRs), diagnostic reports, laboratory results, medical imaging, wearable devices, and Internet of Things (IoT)-enabled health monitoring systems. These technologies have improved the accessibility and availability of medical information while enabling

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

continuous patient monitoring and remote healthcare services. However, the exponential growth of healthcare data has introduced new challenges related to secure storage, efficient management, data sharing, interoperability, and privacy protection. Healthcare organizations must efficiently integrate information collected from multiple sources while ensuring that sensitive patient records remain accurate, confidential, and readily accessible to authorized medical professionals. The increasing complexity of healthcare ecosystems further emphasizes the need for intelligent digital platforms capable of managing large-scale medical information while supporting collaboration among physicians, hospitals, laboratories, pharmacies, and patients [1].

The widespread adoption of wearable sensors, smart medical devices, and mobile healthcare applications has significantly increased the volume of patient-generated health data, creating additional challenges in data processing and long-term record management [2]. Continuous health monitoring technologies produce real-time physiological information that enables early disease detection, personalized treatment planning, and preventive healthcare services. Although these innovations improve patient care, healthcare institutions often face difficulties in organizing heterogeneous medical datasets originating from multiple clinical systems and monitoring devices. The absence of efficient data integration mechanisms may lead to fragmented patient records, duplication of information, and delays in accessing critical medical data. Therefore, modern healthcare systems require centralized and interoperable health information management solutions that facilitate secure information exchange while improving communication and coordination among healthcare stakeholders, ultimately supporting more effective clinical decision-making and patient-centered care [3].

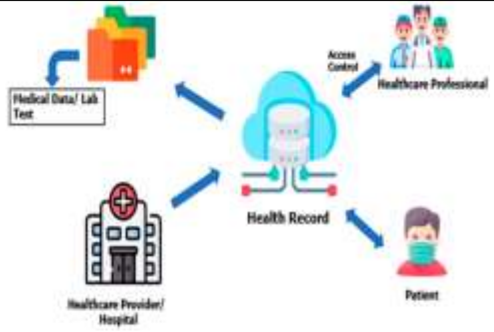

Fig. 1: Patient Appointment Booking

Another major challenge in healthcare is maintaining effective communication among patients, physicians, nurses, and other healthcare professionals. Communication barriers become particularly significant when treating elderly individuals or patients suffering from neurodegenerative disorders, cognitive impairments, speech disabilities, or chronic illnesses, where incomplete or inaccurate information may negatively affect diagnosis, treatment planning, and follow-up care [4]. Similarly, miscommunication among medical staff can contribute to clinical errors, delayed treatments, and reduced quality of healthcare services. Personal Health Record (PHR) systems and digital patient management platforms have emerged as valuable solutions for addressing these challenges by providing centralized access to comprehensive patient histories, medication records, laboratory reports, consultation details, and treatment progress. Such systems support continuous monitoring of chronically ill patients, facilitate timely medical interventions, improve collaboration among healthcare professionals, reduce medical errors, and enhance the overall quality, efficiency, and safety of healthcare delivery [5].

1.1 Research Motivation

The rapid digitization of healthcare services in real-time organizations such as large hospital chains, diagnostic networks, and healthcare management companies has created a strong demand for secure and data-driven systems.

Organizations like multi-specialty hospitals and telemedicine providers handle thousands of patient appointments and medical records daily, generating vast amounts of sensitive data. Data analysis plays a crucial role in these environments by helping administrators understand patient flow, peak appointment hours, doctor utilization, and service demand patterns. Without proper digital platforms, valuable data remains underutilized, leading to inefficiencies such as long waiting times and poor resource allocation. Additionally, frequent incidents of healthcare data breaches have increased awareness about the importance of secure data handling. As healthcare companies aim to improve service quality while complying with strict data protection regulations, there is a growing motivation to adopt systems that can securely store, manage, and analyse patient-related data in a structured and reliable manner.

2. LITERATURE SURVEY

Valerio Mandarino, et al. [6] proposed a decentralized application (dApp) architecture for secure healthcare data management using a hybrid storage strategy that combined blockchain technology with local storage of medical records. Instead of storing sensitive medical information directly on the blockchain, patient records were securely maintained on users' devices, while blockchain was utilized to manage encrypted indexes and metadata associated with those records. The proposed architecture employed smart contracts that enabled patients to define authorization policies, ensuring that only designated healthcare providers and authorized entities could access specific medical information. This decentralized approach enhanced patient privacy, reduced the risk of centralized data breaches, improved data ownership, and provided secure, transparent, and tamper-resistant management of healthcare records. Serkan Akbulut, et al. [7] investigated several emerging technologies to develop a patient-centric access management system for securing electronic health records and Internet of Things (IoT)-enabled medical devices. The proposed framework integrated International Ovarian Tumour Analysis (IOTA), Distributed Ledger Technology (DLT), InterPlanetary File System (IPFS), Application Programming Interfaces (APIs), Proxy Re-encryption (PRE), and advanced access control mechanisms to establish a comprehensive healthcare security architecture. The system provided patients with complete control over their medical records while enabling secure data sharing among healthcare professionals, improving interoperability, protecting sensitive health information, and ensuring secure communication between connected medical devices. Mary Nankya, et al. [8] explored the application of Artificial Intelligence (AI) in strengthening cybersecurity for electronic healthcare systems. The study demonstrated that AI-based techniques, including anomaly detection, automated threat response, adaptive learning algorithms, and intelligent intrusion detection systems, significantly improve the identification and mitigation of cyberattacks targeting healthcare infrastructure. Furthermore, the authors discussed future research directions such as quantum-resistant encryption, privacy-preserving AI models, and continuously learning cybersecurity systems capable of protecting patient confidentiality while supporting secure medical data analysis.

Naresh Sammeta, et al. [9] developed the Hyperledger Blockchain Enabled Secure Medical Data Management with Deep Learning-based Diagnosis (HBESDM-DLD) framework for secure storage and intelligent analysis of healthcare information. The proposed model incorporated multiple stages including medical data encryption, optimal cryptographic key generation, Hyperledger blockchain-based secure data management, and deep learning-driven disease diagnosis. By integrating blockchain technology with artificial intelligence, the framework enhanced medical data confidentiality, integrity, accessibility, and diagnostic accuracy while providing secure information sharing among healthcare stakeholders. Raj Kumar, et al. [10] proposed a Doctor Appointment System (DAS) integrated with Electronic Health Record (EHR) systems to improve appointment scheduling and healthcare service management. The proposed platform provided real-time updates regarding doctor availability and appointment slots while enabling patients and healthcare professionals to efficiently schedule, manage, and monitor appointments through a secure user interface. The integration of appointment management with electronic medical records improved communication, reduced scheduling conflicts, and enhanced the overall efficiency of healthcare delivery. Tiantian Niu, et al. [11] conducted a comprehensive review of optimization techniques used in healthcare appointment scheduling systems. The study identified genetic algorithms and simulation-based optimization as the predominant methods for appointment scheduling, while neural networks and deep learning emerged as core technologies for intelligent healthcare management. Bibliometric analysis further revealed increasing research interest in appointment scheduling optimization, particularly in China, and emphasized the need for advanced modeling techniques, practical deployment strategies, and comprehensive system optimization to improve healthcare service efficiency. Mr. M.R. Sukesh, et al. [12] developed a healthcare management platform that improved accessibility through a user-friendly dashboard for monitoring appointments and managing physician schedules. The proposed system minimized dependency on manual record management, reduced administrative errors, supported secure online transactions, and incorporated cloud storage to ensure continuous availability, protection, and accessibility of patient and doctor information.

Izabela Markiewicz, et al. [13] emphasized the importance of secure password hashing mechanisms for protecting authentication systems in modern web-based healthcare applications. The study highlighted the limitations of legacy hashing algorithms such as MD5 and SHA-1 and recommended the adoption of modern memory-hard algorithms including Argon2 and bcrypt. The authors further explained that incorporating salting and peppering techniques significantly strengthens password security by preventing rainbow table attacks, brute-force attacks, and GPU-based password cracking attempts. Toras Pangidoan Batubara, et al. [14] evaluated the security performance of the bcrypt password hashing algorithm through brute-force experiments involving alphabetic, numeric, and mixed-character passwords. The experimental analysis demonstrated the robustness of bcrypt against password recovery attacks, confirming its suitability for protecting user authentication credentials in secure applications. Oghenefego Etese, et al. [15] reviewed the evolution of password hashing techniques from traditional algorithms such as MD5 and SHA-1 to advanced cryptographic approaches including bcrypt and Argon2. The study analysed research published between 2000 and 2024 and highlighted how increasing computational capabilities and sophisticated attack techniques necessitated stronger password protection mechanisms capable of resisting modern cryptographic attacks.

3. PROPOSED SYSTEM

This research as shown in Fig. 2 defines a secure, role-aware, and data-centric workflow for managing healthcare appointments and sensitive medical information in a digital environment. The study adopts a layered architecture that begins with user interaction

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

through a web interface and proceeds through authentication, request validation, business logic processing, and persistent data storage. Each interaction is governed by strict access control and session validation to ensure confidentiality and integrity of healthcare data. The architecture emphasizes secure credential handling, controlled data flow, and reliable record management while supporting real-time appointment operations. By integrating backend logic with structured data models and validated user inputs, the study ensures consistency, scalability, and robustness in healthcare service delivery.

User Interface (Web Browser): Users access the system through a browser-based interface for login, appointment booking, and medical data management. Credentials and form inputs are securely submitted as HTTP requests. All interactions are validated before reaching backend services.

Flask Web Server (app.py & routes.py): The Flask backend receives and routes incoming requests to appropriate handlers. It enforces access rules, manages appointment workflows, and coordinates secure data exchange. This layer acts as the central control unit of the system.

Encrypted Authentication: User passwords are hashed using BCH before storage. During login, submitted passwords are hashed and compared against stored encrypted values. This prevents plaintext password exposure and protects against brute-force attacks.

Session Management & Role Validation: After successful authentication, secure sessions are created and maintained across user interactions. Role identifiers distinguish patients and administrative users, ensuring restricted access to sensitive operations. Unauthorized access attempts are blocked automatically.

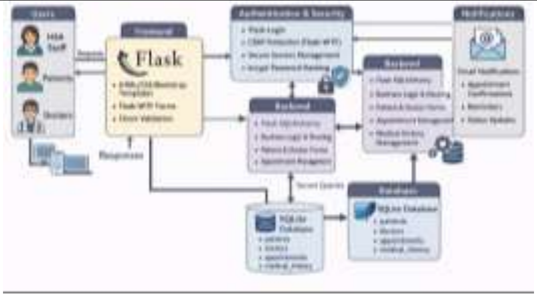

Fig. 2: System architecture of secure online patient appointment booking.

CSRF Protection & Request Validation: All form submissions are protected using CSRF tokens to prevent forged requests. Server-side validation ensures data completeness and correctness. This layer safeguards the system against malicious and unintended interactions.

Database & Data Persistence Layer Healthcare data is managed using SQLA ORM, which maps application objects to relational tables. Encrypted credentials, appointment records, and medical histories are stored securely. ORM-based queries ensure data consistency and protection from injection attacks.

Appointment Management Workflow: Patients submit appointment requests that are validated and stored with predefined status values. Administrative users review, approve, reschedule, or cancel appointments securely. All changes are recorded with timestamps for traceability.

Medical History Management Workflow: Medical records are accessed only after successful authentication and role verification. Updates are validated and securely stored in linked patient records. Controlled access ensures confidentiality of sensitive health information.

Reporting & Monitoring Layer: Administrative users retrieve aggregated appointment and system statistics through controlled queries. The reporting layer supports operational monitoring without

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

exposing individual sensitive data. This enables informed decision-making.

3.1 BCH

BCH as shown in Fig. 3 is a secure password hashing mechanism designed to protect authentication credentials in security-critical systems. It uses automatic salting to prevent identical passwords from generating the same hash. The algorithm introduces adjustable computational cost factors to resist brute-force and rainbow-table attacks. BCH performs one-way encryption, making password recovery computationally infeasible. It is widely adopted due to its robustness and long-term security guarantees. This hashing approach ensures safe credential storage and verification.

Password Intake & Salting: Passwords are combined with randomly generated salts before hashing. This guarantees unique hash outputs even for identical passwords. Salting significantly increases resistance to precomputed attacks.

Cost-Based Hash Processing: Multiple hashing rounds increase computational complexity. The adjustable cost factor slows down unauthorized attack attempts. The Fig. 4.3 ensures long-term cryptographic strength.

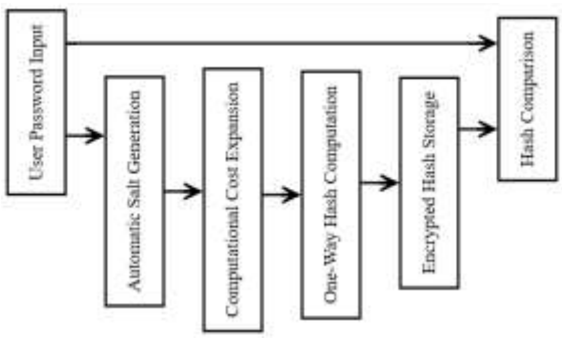

Fig. 3: Internal workflow of BCH

Secure Storage & Verification: Only hashed credentials are stored in the database. During login, hashes are recomputed and compared securely. Plaintext passwords are never revealed or stored.

4. RESULTS AND DISCUSSION

Fig. 4 illustrates the patient appointment booking module that allows users to schedule medical consultations in a structured and secure manner. This component captures appointment-specific details such as preferred date, time, and reason for visit to ensure proper scheduling. It minimizes scheduling conflicts by maintaining organized appointment records. The module supports efficient coordination between patients and healthcare providers through a centralized booking mechanism. This functionality significantly improves operational efficiency and reduces manual intervention in appointment management.

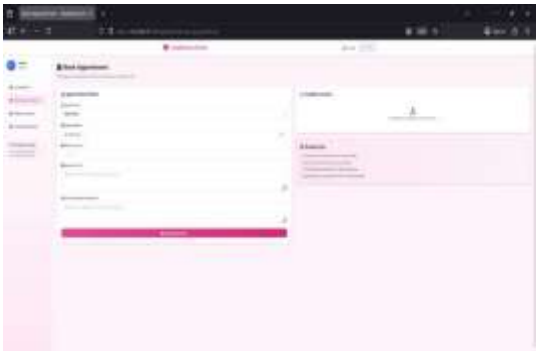

Fig. 4: Patient Appointment Booking

Fig. 5 depicts the patient medical history management module, which enables users to store, view, and update their health-related information securely. This module supports structured documentation of medical conditions, treatments, and related health data. It ensures confidentiality by restricting access based on user roles and authentication status. The medical history records serve as a critical reference for future consultations and continuity of care. This component strengthens long-term healthcare management through secure digital record keeping.

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Fig. 5: Patient Medical History

Fig. 6 illustrates the patient appointments overview module that displays both upcoming and past appointment records. This component allows users to track their consultation history and monitor scheduled visits within the system. It enhances transparency by providing a consolidated view of appointment activities. The module supports efficient appointment management by enabling users to review and plan their healthcare interactions. This feature contributes to improved patient engagement and organized healthcare service delivery.

Fig. 6: Patients Appointments

Fig. 7 illustrates the administrator login module of the healthcare portal, which enables secure authentication for authorized administrative users. This module validates administrator credentials before granting access to system-level functionalities. It ensures that only users with administrative roles can manage appointments, patient records, and doctor profiles. The login mechanism enforces role-based access control to protect sensitive operational data. This component is critical for maintaining administrative security and controlled system access.

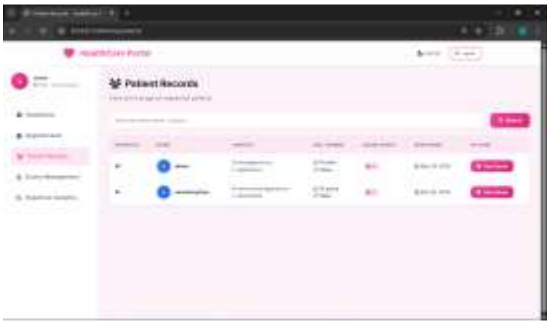

Fig. 8: Patient Records Screen

Fig. 9 illustrates the doctor management module, which enables administrators to manage healthcare provider profiles within the system. This module supports the addition, modification, and maintenance of doctor information, including specialization and availability. It ensures that only authorized administrators can control doctor-related data and scheduling parameters. The module facilitates efficient coordination between doctors and appointment scheduling processes. This functionality strengthens overall system organization and healthcare service delivery.

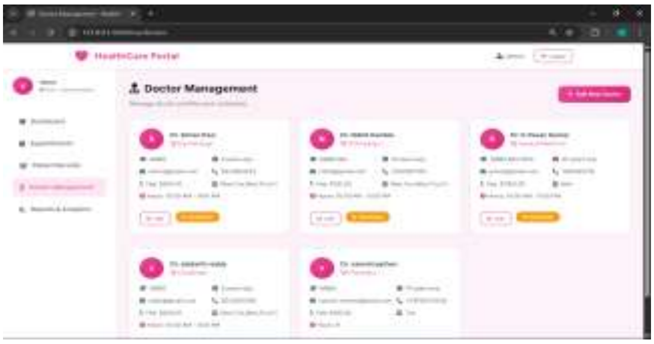

Fig. 9: Doctor Management

5. CONCLUSION

This research presents a secure and efficient healthcare management system that digitalizes patient appointment booking and medical history handling through a structured web-based approach. The integration of Flask for backend processing and SQLA for database interaction ensures smooth request handling and reliable data persistence. Encrypted authentication using BCH significantly improves security by protecting user credentials and preventing unauthorized access. Performance improvements are achieved by automating appointment workflows, reducing manual scheduling delays, and enabling faster administrative approvals. Role-based access control enhances system efficiency by ensuring that users interact only with permitted functionalities. The modular architecture supports concurrent user access while maintaining consistent response times and data integrity. Dynamic dashboards provide real-time visibility into appointments and system activity, improving operational awareness. Input validation and session management reduce errors and security risks during execution. The system demonstrates strong reliability, usability, and scalability for healthcare environments.

REFERENCES

[1] Vayena, E.; Dzenowagis, J.; Brownstein, J.S.; Sheikh, A. Policy implications of big data in the health sector. *Bull. World Health Organ.* 2018, *96*, 66–68.

[2] Baird, A.; North, F.; Raghu, T.S. Personal Health Records (PHR) and the future of the physician-patient relationship. In *Proceedings of the 2011 iConference*; ACM: Seattle, WA, USA, 2011; pp. 281–288.

[3] Alanazi, A.; Anazi, Y.A. The Challenges in Personal Health Record Adoption. *J. Healthc. Manag.* 2019, *64*, 104–109.

[4] Alsahafi, Y.A.; Gay, V. An overview of electronic personal health records. *Health Policy Technol.* 2018, *7*, 427–432.

[5] Manias, E.; Gray, K.; Wickramasinghe, N.; Manojlovich, M. Using electronic medical records to create big data and to communicate with patients—Is there room for both? *Collegian* 2018, *25*, 467–469.

[6] Mandarino, Valerio & Pappalardo, Giuseppe & Tramontana, Emiliano. (2024). A Blockchain-Based Electronic Health Record (EHR) System for Edge Computing Enhancing Security and Cost Efficiency. Computers. 13. 132. 10.3390/computers13060132.

[7] Akbulut, S.; Semantha, F.H.; Azam, S.; Pilares, I.C.A.; Jonkman, M.; Yeo, K.C.; Shanmugam, B. Designing a Private and Secure Personal Health Records Access Management System: A Solution Based on IOTA Distributed Ledger Technology. Sensors 2023, 23, 5174. https://doi.org/10.3390/s23115174

[8] Nankya, Mary & Mugisa, Allan & Usman, Yusuf & Upadhyay, Aadesh & Chataut, Robin. (2024). Security and Privacy in E-Health Systems: A Review of AI and Machine Learning Techniques. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3469215.

[9] Sammeta, N., Parthiban, L. Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model. *Complex Intell. Syst.* 8, 625–640 (2022). https://doi.org/10.1007/s40747-021-00549-w

[10] S., Raj & S., Shadheem & S., Surya. (2024). Web-based Application for Doctor-Patient Appointment Management System. Journal of ISMAC. 6. 261-270. 10.36548/jismac.2024.3.006.

[11] Niu, T.; Lei, B.; Guo, L.; Fang, S.; Li, Q.; Gao, B.; Yang, L.; Gao, K. A Review of Optimization Studies for System Appointment Scheduling. Axioms 2024, 13, 16. https://doi.org/10.3390/axioms13010016

[12] Sukesh, Mr & .V, Yuvaraj. (2025). Smart Healthcare Appointment System. International Journal of Research Publication and Reviews. 6. 7618-7623. 10.55248/gengpi.6.0325.12149.

[13] Markiewicz, Izabela. (2025). Password Hashing as a Key Element of Security in Web Services. 10.13140/RG.2.2.34995.69920.

[14] Batubara, Toras & Efendi, Syahril & Nababan, Erna. (2021). Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force. Journal of Physics: Conference Series. 1811. 012129. 10.1088/1742-6596/1811/1/012129.

[15] Etese, Oghenefego and Adesina, Al-Ameen, A Review and Comparative Analysis of Password Hashing Techniques: Evaluating Bcrypt and Argon2 (July 14, 2025). Available at http://dx.doi.org/10.2139/ssrn.5363433