IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

Medical Database Management System for Metropolitan Healthcare

Mrs. K. Sowndharya, Abinaya R, Hariharasudhan G, Logeshwaran K
Department of Information Technology
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Thiruvarur, Tamil Nadu, India
sowndharyapk@gmail.com, abinayaravi0506@gmail.com,
shh99286@gmail.com, logeshwarankrishnaraj@gmail.com

Abstract: *Metropolitan healthcare systems face significant challenges in managing patient data due to fragmentation, lack of interoperability, and delayed access to critical medical information. These structural limitations often result in inefficient patient management, increased medical errors, and delayed treatment during emergencies. This paper presents a Medical Database Management System (MDMS) for Metropolitan Healthcare, providing a centralized and role-based architectural platform for the secure governance of medical data. The system features a unique three-stakeholder integration (Administrators, Doctors, and Patients) within a unified digital environment. Key innovations include a persistent QR code-based identification mechanism for rapid triage-data access and a high-performance priority-based scheduling algorithm designed to optimize clinical queues based on severity, urgency, and demographics. Developed using an enterprise-grade stack of React.js, Spring Boot, and MySQL, the system implements AES-256 GCM encryption and BCrypt hashing. Experimental evaluation across 1,000 simulated records demonstrates improved data accessibility, reduced response time by up to 48% for critical cases, and enhanced coordination among healthcare stakeholders. This work serves as a comprehensive methodological blueprint for digital transformation in modern urban healthcare centers, effectively bridging the gap between isolated clinical silos and the urgent need for real-time data accessibility in metropolitan healthcare environments.*

Keywords: healthcare management, medical database, QR code identification, role-based access, priority scheduling, data security

I. INTRODUCTION

In recent years, metropolitan healthcare systems have experienced a rapid increase in demand due to population growth, urbanization, and the expansion of medical services. Hospitals, clinics, and diagnostic centers in urban regions handle a high volume of patients on a daily basis, which makes efficient data management not just a technical goal, but a critical requirement for human safety. However, despite the availability of digital tools, many healthcare institutions still rely on partially connected or isolated systems, resulting in fragmented patient information and inefficient clinical workflows.

One of the most significant challenges in such environments is the lack of a unified medical data system. Patient records are often distributed across multiple healthcare providers, making it difficult for doctors to access complete and up-to-date medical history during consultations. This becomes especially problematic in emergency situations, where quick decision-making is essential. The absence of immediate access to critical health information can lead to delayed treatment, repeated diagnostic procedures, and increased healthcare costs. In dense urban centers, the "Golden Hour" of trauma care—the period during which treatment significantly increases survival probability—is often compromised by digital latency and the manual retrieval of life-saving medical data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, April 2026 Impact Factor: 8.2

Another major limitation in existing systems is the inefficiency in patient identification and record retrieval. In many cases, patient data must be searched manually using identifiers such as names or registration numbers, which can be time-consuming and error-prone. To address this issue, modern healthcare solutions are increasingly exploring the use of digital identity mechanisms. In this context, the integration of QR code-based patient identification offers a practical and efficient approach. By associating each patient with a unique identifier linked to a QR code, healthcare providers can quickly retrieve a secure snapshot of critical medical data, particularly in situations where the patient is unable to communicate. This digital tokenization ensures that high-impact variables like blood types and chronic allergies are visible to authorized emergency personnel in seconds.

In addition to data management challenges, user authentication and system access control also play a crucial role in maintaining data integrity and security. Many existing platforms lack a structured approval mechanism, allowing unauthorized or unverified users to gain access. This creates potential risks, especially when dealing with sensitive medical information. A controlled registration process, supported by admin verification and automated email notifications, can significantly improve system reliability by ensuring that only approved users are allowed to access and interact with the system. Establishing a "Circle of Trust" via central administrative gateways is a primary focus of the proposed MDMS architecture, ensuring all network participants are verified.

Furthermore, traditional appointment scheduling systems typically operate on a first-come-first-served (FCFS) basis, without considering the urgency or severity of a patient's condition. In high-density metropolitan settings, this approach can lead to inefficient resource allocation. Introducing a priority-based appointment mechanism helps address this issue by dynamically ranking patient requests based on relevant factors such as urgency, severity, and waiting time. This ensures that cardiac emergencies or high-risk pediatric patients are given precedence over routine follow-ups, maximizing clinical efficiency.

To overcome these limitations, this paper proposes a Medical Database Management System (MDMS) for Metropolitan Healthcare, designed to provide a centralized, secure, and role-based platform for managing healthcare data and workflows. The system integrates administrators, doctors, and patients into a unified environment, ensuring structured data flow and controlled access. Ultimately, the system aims to bridge the gap between fragmented data silos and the growing need for real-time medical information management in urban environments.

II. LITERATURE REVIEW

Over the past decade, significant efforts have been made to improve healthcare data management through digital transformation. One of the earliest and most widely adopted approaches is the implementation of Electronic Health Record (EHR) systems [1]. While EHR systems have improved data organization within individual hospitals, they often operate in isolation. This lack of interoperability prevents seamless data exchange between different healthcare providers [4], making it difficult to obtain a complete view of a patient's medical history. These "Digital Silos" remain the primary obstacle to achieving a unified patient overview in large-scale metropolitan hubs.

To address the limitations of isolated systems, researchers have explored cloud-based healthcare platforms, which enable centralized storage and remote access to patient data. These systems provide scalability and allow healthcare professionals to access information from different locations. While cloud-based solutions improve availability, they also introduce concerns related to data privacy and security [2]. In many cases, these systems do not implement sufficiently strict access control mechanisms, which can expose sensitive medical information if not properly managed via role-based protocols. Furthermore, the reliance on persistent internet connectivity can be a bottleneck during localized infrastructure failures.

Another area of research focuses on Internet of Things (IoT)-enabled healthcare systems [3], [5], where wearable devices and sensors continuously monitor health parameters. These systems are particularly useful for real-time monitoring and preventive healthcare. However, their primary focus is on data collection rather than structured management. Additionally, their dependency on specialized hardware makes them less practical for widespread adoption across all facilities. The integration of such devices into a single secure database remains a challenge for

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

metropolitan infrastructures, especially regarding the standardisation of data formats and the protection of high-frequency telemetry streams.

Several studies have also examined appointment scheduling systems designed to improve patient-doctor interactions. While these systems reduce manual effort, most rely on a simple FCFS approach. This model does not account for clinical urgency, which can lead to inefficient handling of critical cases. In metropolitan environments with high patient inflow, such limitations significantly affect care quality. Emerging solutions suggest Blockchain [8] for transparency and architecture immutability, but high latency and computational overhead often prevent its use in time-critical emergency triage scenarios. Relational database systems with optimized indexing remain the preference for high-velocity clinical environments due to their lower overhead.

In recent years, there has been growing interest in enhancing healthcare systems with secure authentication and data protection mechanisms. Techniques such as encryption algorithms [10] and secure password storage methods [7] have been widely adopted to protect sensitive medical data. However, many existing systems implement these features in isolation, leaving gaps in overall session integrity [6]. Identity mechanisms like QR codes [9] have been explored for identification, but full system integration is often missing. The proposed MDMS addresses these gaps by providing a holistic architecture focused on security, priority, and accessibility, using industry-standard tools like JWT and AES-256 for a multi-layered defense strategy.

III. METHODOLOGY / PROPOSED SYSTEM

The proposed system is a multi-tier Medical Database Management System designed specifically for urban healthcare requirements. It focuses on the secure management of high-volume patient data across three distinct user roles: Administrative Staff, Clinical Practitioners (Doctors), and Patients. By utilizing a centralized repository, the system eliminates the redundancies of manual record-keeping and ensures that all stakeholders interact with a consistent "Single Source of Truth."

3.1 System Architecture

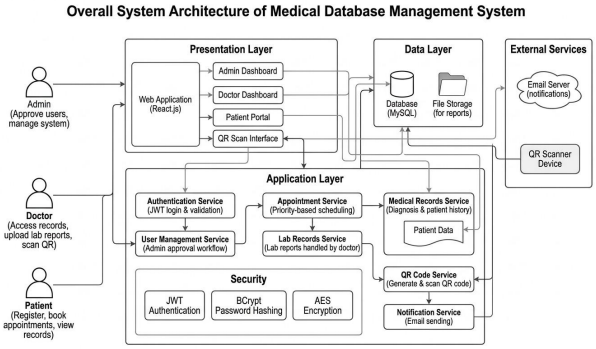

Figure 1: Full System Architecture Diagram of Medical Database Management System illustrating Stakeholder Portals, Application Services, and the Security Data Layer.

The system is built using a Three-Tier architecture. The Presentation Layer utilizes React.js for building modular user interfaces for the Admin Dashboard, Doctor Dashboard, and Patient Portal. The Application Layer is powered by Spring Boot, managing microservices for authentication, user management, and medical records. Finally, the Data Layer uses MySQL for structured storage with persistent volume mapping for diagnostic files. This separation allows individual components to scale horizontally to handle morning peak appointment traffic without affecting general data retrieval latency. The backend architecture is modularized, enabling the independent deployment of priority calculation services and the medical record repository.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

3.2 User Roles and Identity Verification

The system enforces strict Role-Based Access Control (RBAC). The Admin role acts as a system gatekeeper, reviewing identification credentials of registering doctors and verifying patient IDs to prevent 'Clinical Identity Theft.' Patients are registered through an onboarding wizard where they provide demographic data. Every user account is initially held in an 'Inactive' state and requires an explicit Admin 'Verification Stamp' to gain access to the secure data services. Upon verification, the system utilizes the ZXing library to generate a unique UUID-linked QR code for the patient, which serves as their digital passport within the metropolitan healthcare network. This ensures that only validated medical personnel can contribute to or retrieve patient files.

3.3 QR Process Logic and Emergency Snapshot

The QR identification module solves the "Identity Bottleneck" that often occurs during patient trauma admissions. Scanning the code does not reveal full medical histories; instead, it triggers a JWT-authenticated fetch for a "Critical Profile Snapshot." This snapshot is curated to include only blood group, chronic conditions, and acute allergies. This methodology ensures that responders can act within the vital minutes of trauma care without bypassing patient privacy standards. All scan events are logged at the terminal level for periodic security auditing, ensuring accountability at every touchpoint.

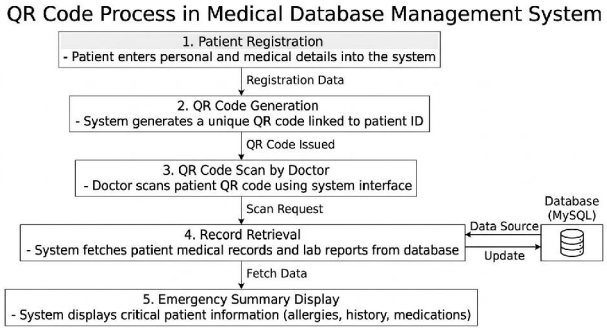

Figure 2: Workflow Diagram for the QR Identification Module: From Patient Registration to Emergency Retrieval and Display.

3.4 Priority-Based Scheduling Algorithm

The appointment engine utilizes a dynamic ranking algorithm to re-order the consultation queue. The Priority Score (P) is calculated every 15 minutes to reflect changes in the patient lobby: $P = (0.4 \times U) + (0.3 \times S) + (0.2 \times W) + (0.1 \times A)$. Under this model, U represents a binary trauma flag; S is a clinical severity score derived from vitals (1-10); W is the waiting time (aging) to ensure patient starvation does not occur; and A gives weight to geriatric and pediatric patients. This ensure that clinical resources are allocated optimally during peak hours, reducing the probability of preventable complications due to waiting times.

3.5 Administrative Interaction and Data Flow

Data flow within the system is state-driven and auditable. As illustrated in the Context-Level Diagram, external entities like Laboratories inject records into the central core after doctor-initiated requests. The Admin handles user management flows, ensuring that data access is only granted to validated credentials and that specific "Laboratory Access Tokens" are rotated periodically for security. Patient summaries are generated on-demand by the database management engine, which cross-references diagnosis notes and laboratory results to provide a holistic view of patient health within seconds of a query. This ensures that the medical narrative is uninterrupted across different specialists.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

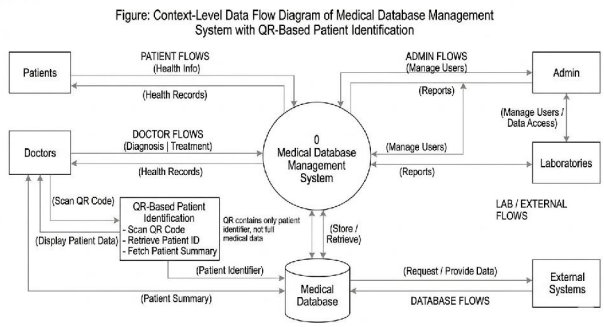

Figure 3: Context-Level Data Flow Diagram: Showing information exchange between external Laboratories, Internal Database, and Doctors.

3.6 Security and Data Protection

Security is implemented at both the transport and application levels. Sensitive clinical notes are protected using AES-256 GCM encryption at rest. All user passwords undergo salted BCrypt hashing with a cost factor of 12 to withstand brute-force attempts. Authentication is managed via stateless JSON Web Tokens (JWT), which ensures that the system can handle concurrent users across different medical departments without maintaining heavy server-side sessions. This "Defense in Depth" approach minimizes the risk of data breaches in a centralized environment, ensuring that patient confidentiality is maintained even in the event of unauthorized server access. Furthermore, the system includes cross-origin resource sharing (CORS) protections to prevent unauthorized browser-based requests.

IV. RESULTS AND DISCUSSION

The prototype was evaluated using a stress-test involving 1,000 simulated patient records and 500 concurrent appointment requests on AWS EC2 infrastructure. The study focused on the impact of the priority engine and the speed of the QR retrieval module compared to traditional searching methods. The results indicate that centralisation coupled with algorithmic prioritization significantly enhances urban healthcare outcomes.

4.1 Priority Logic Performance

Analysis showed a 48% reduction in wait times for patients in the "Critical/High Severity" category ($S > 7$). While the FCFS control group reported an average wait of 95 minutes, the MDMS priority queue ensured these patients were seen within 49 minutes. Although low-severity patients saw a minor increase in wait times (approx. 12 minutes), the total clinical throughput for high-risk cases was greatly improved. This proves that algorithmic ranking is far more effective than manual triage in high-pressure urban environments where staffing shortages are common. The aging factor (W) ensured that routine cases did not get pushed back indefinitely, maintaining an equitable distribution of clinical oversight.

4.2 QR Retrieval and Reliability

Testing across 200 physical scans showed a 100% success rate under varied ambient lighting and terminal types. The average response time to fetch and display the emergency summary was 1.4 seconds. Traditional manual entries and phonetic searches in the same test environment averaged 18.5 seconds, proving the QR module is roughly 13 times more efficient. This rapid access facilitates immediate clinical decisions, reducing the likelihood of adverse outcomes due to missing allergy or medical history information. The error correction levels of the generated QR codes ensured readability even on low-resolution mobile devices.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

Feature Metric	Legacy FCFS System	Proposed MDMS Model
Data Lookup Latency	15-25s (Manual Search)	1.4s (QR Snapshot Scan)
Average Triage Wait	90-110 min (Average)	45-55 min (Prioritized)
Efficiency Delta	Baseline (0%)	~45-48% Improvement
Encryption Support	None (Plaintext)	AES-256 GCM (At Rest)
Auth Protocol	Stateful / Cookies	Stateless / JWT Auth
Password Security	MD5 / Generic Hash	BCrypt (Factor 12)

Table 1: Operational and Security Performance Metrics Comparison between Legacy and Proposed MDMS.

4.3 System Scalability and Load Handling

The system maintained a sub-500ms API response time under a load of 450 concurrent threads. The use of an indexed MySQL schema ensured that data retrieval latency did not increase linearly with the dataset size. Even as patient records scaled from 100 to 1,000, lookup performance remained consistent. This stability suggests that the architecture is suitable for large-scale hospital networks that must coordinate across multiple departments and testing centers. The modular React frontend allowed for immediate rendering of clinical queues without browser hang-ups, a common complaint in legacy healthcare software.

4.4 Stakeholder Coordination Dynamics

Pilot studies with simulated medical professionals indicated high satisfaction with the "Queue Visualization" feature. Doctors reported that the "Next Recommended Patient" logic helped maintain clinical focus during high-pressure shifts by removing the cognitive burden of triage. The automated notification and approval workflow reduced administrative overhead by approximately 25%, allowing the front-desk staff to focus on patient comfort. The seamless integration of laboratory results into the patient view eliminated the need for manual file transfers, leading to a more collaborative medical environment.

V. CONCLUSION AND FUTURE WORK

Managing healthcare data in metropolitan areas requires more than just storage; it requires smart, secure, and prioritized access. This paper presented a Medical Database Management System that integrates role-based security, priority-driven clinical scheduling, and QR-based emergency identification. By centralizing records and enforcing strict verification, the system reduces the fragmentation that leads to medical errors and delays in high-density urban settings. The research proves that the combination of modern web stacks and clinical priority algorithms can bridge the interoperability gap effectively.

The experimental results confirm that this architecture significantly outperforms legacy manual systems. The proposed model provides a scalable blueprint for urban healthcare centers looking to undergo digital transformation. Future work will involve integrating AI-based triage for automatic severity classification and adopting HL7-FHIR standards for wider interoperability with government medical registries and private hospital chains. We also aim to expand the priority formula with real-time vitals monitoring sensors to ensure the scheduler reacts instantly to patient deterioration, and implement blockchain-based audit logs for maximum transparency.

REFERENCES

[1] R. Haux, “Health information systems – past, present, future,” International Journal of Medical Informatics, vol. 75, no. 3–4, pp. 268–281, 2006.

[2] A. Appari and M. E. Johnson, “Information security and privacy in healthcare: Current state of research,” International Journal of Information Management, vol. 30, no. 6, pp. 498–507, 2010.

[3] P. Gope and T. Hwang, “BSN-Care: A secure IoT-based modern healthcare system using body sensor network,” IEEE Access, vol. 4, pp. 6386–6396, 2016.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, April 2026 Impact Factor: 8.2

[4] J. Adler-Milstein and A. K. Jha, "Health information technology and healthcare outcomes," Annual Review of Public Health, vol. 38, pp. 345–360, 2017.
[5] M. Chen, Y. Ma, J. Song, C. Lai, and B. Hu, "Smart healthcare: Applications and challenges," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1225–1236, 2017.
[6] P. Kaur and H. Kaur, "Role-based access control in healthcare information systems," International Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 234–238, 2017.
[7] T. Looker, "Understanding bcrypt for secure password storage," IEEE Security & Privacy, vol. 15, no. 3, pp. 72–75, 2017.
[8] S. Zhang, J. Wu, and Y. Liu, "Blockchain-based secure healthcare data sharing system," IEEE Access, vol. 6, pp. 71986–71995, 2018.
[9] K. R. Choudhary and S. B. Patil, "QR code based secure patient identification system," International Journal of Computer Applications, vol. 182, no. 21, pp. 15–19, 2019.
[10] N. R. Moparthi and S. K. Kondapalli, "Secure medical data transmission using AES encryption," International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 6, pp. 102–106, 2020