

---

# Decentralized Data Integrity: Integrating MySQL with Blockchain for Resilient Healthcare Systems

---

Deepak Chandra Uprety<sup>1</sup>, Kamal Upreti<sup>2,\*</sup>, Pravin R. Kshirsagar<sup>3</sup>,  
Tan Kuan Tak<sup>4</sup>, Shitiz Upreti<sup>5,\*</sup>, Ganesh V. Radhakrishnan<sup>6</sup>  
and Ajay Kumar<sup>7</sup>

<sup>1</sup>*Dept. of Computer Science and Engineering, Noida Institute of Engineering and Technology, Greater Noida, India*

<sup>2</sup>*Dept. of Computer Science, Christ University, Delhi NCR Campus, Ghaziabad, India*

<sup>3</sup>*Dept. of Electronics & Telecommunication, J D College of Engineering & Management, Nagpur, Maharashtra, India*

<sup>4</sup>*Engineering Cluster, Singapore Institute of Technology, Singapore*

<sup>5</sup>*School of Computer Science & Engineering (SCSE), IILM University, Greater Noida (UP), India*

<sup>6</sup>*Dept. of Economics and Finance, KIIT School of Management (KSOM), KIIT University, Bhubaneswar, India*

<sup>7</sup>*Inderprastha Engineering College, Ghaziabad, India*

*E-mail: deepak.glb@gmail.com; kamalupreti1989@gmail.com;  
pravinrk88@yahoo.com; kuantak.tan@singaporetech.edu.sg;  
upretiec@gmail.com; vrkris2002@gmail.com; ajayagrohi@gmail.com*

*\*Corresponding Author*

Received 02 February 2025; Accepted 08 May 2025

## Abstract

A transformational solution to the problems created by healthcare data management is presented by the integration of MySQL and blockchain technology, centered around security, scalability, and efficiency. This paper presents MBHA MySQL-Blockchain Healthcare Architecture combining the

*Journal of Mobile Multimedia, Vol. 21\_2, 275–306.*

doi: 10.13052/jmm1550-4646.2124

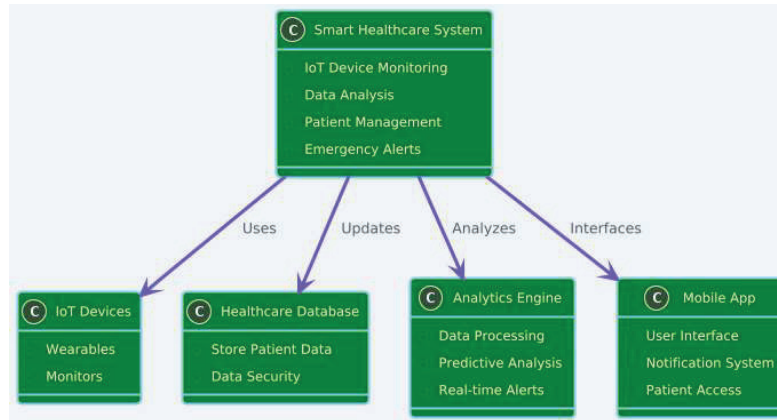
© 2025 River Publishers

structured data storage, querying capabilities of MySQL with the decentralized, tamper-proof framework of blockchain. The system shows impressive performance metrics with an average API response time of 1.54 seconds for user registration and 841 milliseconds for login. The database queries and data retrieval or insertion took less than 1 millisecond, and JWT tokens were generated for authentication in less than 50 milliseconds. Conclusion Results indicate an efficient real-time system to accomplish tasks with integrity in terms of data but also with safety in operations. This architectural model, discussed above, is issues regarding data security and access with a need to provide care-collaboration needs. Scalability would then be optimized while keeping down computational overhead; in fact, work toward readiness for adoption is mainly towards being more regulatory compliant.

**Keywords:** MySQL, blockchain, healthcare information systems, data security, data integration.

## 1 Introduction

**Background:** Data is a significant asset in the digital age, with different forms of data having distinct meanings. Healthcare data is especially valuable, yet cyber-attacks are targeting it to reap financial rewards. Data integrity security is critical because attackers utilize compromised data to execute subsequent assaults [1]. Countries are digitizing to enhance customer experience and minimize infrastructure requirements. For example, security professionals are under threats of breaches of confidentiality, violation of privacy, and credibility breaches [2, 3]. Parallely, digitization of healthcare systems has brought along revolutionary progress. The conventional healthcare systems are unable to fulfill the various needs of the patients, and inefficiencies crop up and suboptimal results occur. Instead, ML presents a paradigm shift in terms of individualized and data-driven care. Using patient data collected by advanced medical devices, predictive models developed by ML can drastically improve disease prediction and resource management [4]. The application of AI-based medicine, especially in cancer treatment, demonstrates the scope for customized treatment plans, real-time monitoring, and holistic treatment as shown in Figure 1. These changes together reflect a revolution in traditional healthcare systems toward efficiency, adaptability, and better patient care [5]. It opened up product innovation into convergence because it bases decisions on real evidence and caters towards personalized solutions for patient care [6]. Thousands of structured as well as unstructured



**Figure 1** Smart healthcare system components.

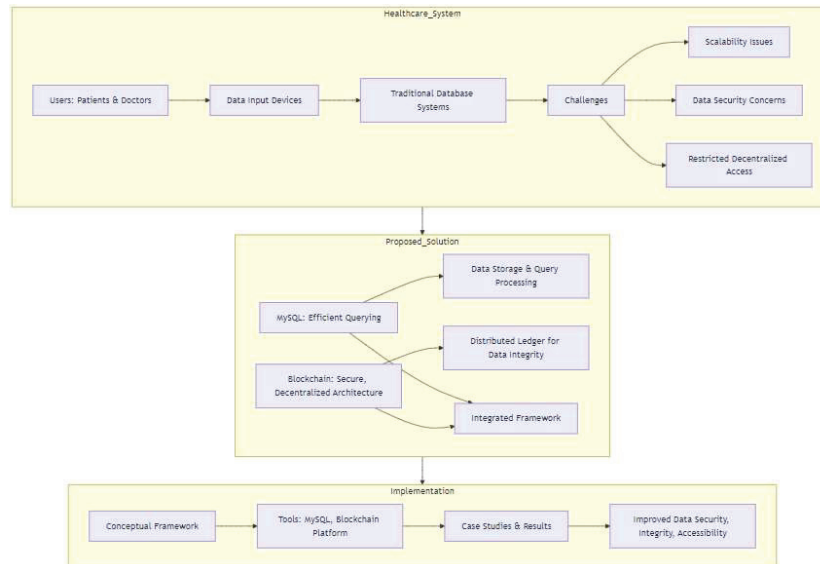
data can give an insight into the diseases, progress of the treatment, and preferences of the patients, hence enabling maximum personalization through preventive measures, predictive analysis, and machine learning in terms of finding susceptible groups and also optimizing the usage of resources. However, very important challenges include data privacy, security, and regulatory compliance [7].

To support this, a robust strategy for privacy-preserving data sharing is SMC, aligned with HIPAA and GDPR. SMC will ensure secure collaboration while protecting sensitive healthcare data and empowering patients for better healthcare outcomes. With increasing needs in effective monitoring healthcare systems, Ramani et al. in [8] proposed a scheme for optimized data management and secured federated learning named ODMSM-FL based on blockchain, thereby securely managing the data on decentralized IoMT systems and effectively managing problems concerning the performance metric and administrative data security issues with data privacy. Similarly, Chen et al. (2024) in [9] introduced Mobile AI-Generated Content (AIGC) to power Human Digital Twins (HDT), leveraging rare disease data modeling for tailored medication and virtual therapy platforms to enable personalized healthcare. This is innovative and transformative in transforming patients into the frontiers of healthcare solutions. Global acceptance and development of TCM (Traditional Chinese Medicine) is challenged by its growing safety concerns, such as unexpected toxicity issues including liver and kidney injuries. The approach in a “New Outlook on TCM Safety” has been emphasized in modernized approaches to toxicity evaluation, proactive risk management,

and safety strategies [10]. On the other hand, the merging of AI, ML, and blockchain technologies changes the business operations of an organization into efficiency, transparency, and effective decision-making [11]. There are fewer workers and rising chronic diseases against the healthcare sector. The health interventions by AI will hold promise for increasing patient outcomes and population health besides improving healthcare worker well-being. However, regulatory frameworks for many of these are presently quite inadequate since most AI technologies grow autonomously with little intervention to ensure their effectiveness and safety on a global plane [12]. Similarly, intelligent TCM employs sophisticated algorithms in remote diagnosis, like tongue image segmentation, to optimize health management [13]. A new segmentation algorithm aims to achieve improved accuracy for such complex, real-world conditions than traditional approaches while advancing TCM's capabilities for diagnosis. Heart disease continues to be a major challenge, largely contributing to morbidity and mortality due to coronary artery disease and heart failure. With this in mind, a novel prediction model has been developed for heart diseases integrating IoMT with state-of-the-art AI methods, such as TabNet and CatBoost [14]. IoMT empowers real-time data acquisition from wearables and sensors, TabNet processes tabular data efficiently for feature selection, and CatBoost promotes higher predictive accuracy as it manages complicated datasets. The model relies on different patient profiles to provide risk assessment in a personalized manner while allowing rapid predictions [15]. This is the future pathway toward transformative, preventive care strategies in cardiovascular health.

Unlike existing systems that rely solely on centralized SQL databases or off-the-shelf API integrations, the proposed MBHA (MySQL-Blockchain Healthcare Architecture) introduces a novel hybrid approach that ensures end-to-end data integrity through decentralized logging while retaining the performance benefits of structured SQL querying. The unique contribution lies in seamlessly embedding blockchain-backed validation into traditional SQL workflows, which is further enhanced by JWT-based stateless authentication for distributed healthcare platforms. This addresses real-world limitations of siloed data systems by enabling tamper-resistant, traceable interactions across stakeholders – a feature largely missing in existing healthcare frameworks.

Traditional database systems used in healthcare setups have numerous limitations since they cannot scale well. They also pose restrictions to data security and decentralized access. Such challenges make it difficult to handle sensitive and significant healthcare data, as typical healthcare operations



**Figure 2** Workflow of this research work.

require a substantial number of users with real-time accessibility and robust data integrity guarantees. The proposed paper, therefore, integrates MySQL with blockchain technology, where MySQL's excellent querying ability is combined with the benefits of a decentralized, highly secure architecture based on blockchain as shown in Figure 2. The integration seeks to overcome present constraints while further strengthening data security, integrity, and accessibility within the healthcare system. The paper will explore the challenges faced by traditional systems, the conceptual framework for MySQL and blockchain integration, and the methodologies used to implement the system. Through case studies and results, the paper will demonstrate the effectiveness of the proposed solution in real-world healthcare scenarios. Finally, it will discuss the broader implications of this integration, compare it with existing technologies, and highlight future research directions.

## 2 Literature Review

### 2.1 Blockchain Technology in Healthcare

Using the Integration of Fog Computing and Blockchain for Designing a Secure Healthcare Service for Predictive Analysis of Diabetes and Cardiovascular Diseases. On the basis of token generation through fog nodes, secure

storage by blockchain, and analysis using a feature selection-based neuro-fuzzy inference system, FS-ANFIS, more than 81% accuracy in prediction is reported in [16]. This approach may potentially demonstrate its prowess in supplementing healthcare applications through the efficient provision of disease-prediction services in a secure manner. The technology of blockchain is being explored in healthcare to enhance the security and integrity of electronic health records (EHR) [17, 18]. Its decentralized nature, tamper resistance, smart contracts, and consensus processes are some of the reasons that protect sensitive health data from misuse. Its usage, however, raises ethical concerns because it involves patients' privacy and personal information. An extensive literature review indicates that though blockchain technology is rapidly evolving, debates on the ethics of its use in healthcare are still emerging [19]. More research is required to resolve ethical issues with the adoption and use of blockchain technology [20]. A novel blockchain approach for secure management of healthcare information that reduces the communication and computational overhead costs compared to existing bitcoin networks and light-weight blockchain architectures. According to the experimental results of [21], the proposed solution accelerates ledger updates by 63% and reduces network traffic by tenfold with the increase in the number of nodes. The health care providers can now safely access and handle patients' health information, enhancing their ability to govern public health risks [22]. This solution addresses privacy, security, and interoperability issues within the ecosystem. This will help the health care system to react better to epidemics such as COVID-19. The Blockchain network improves data interchange between pharmacies and diagnostic laboratories, encouraging transparency while also improving performance, security, and accuracy in medical record management and analysis [23]. The study in [24] presents a novel blockchain architecture for improving security and privacy in EHR that uses decentralized databases like as OrbitDB and IPFS while displaying higher performance and metrics. The healthcare business is adopting blockchain technology to enhance decision-making processes [25]. The IP-HealthChain architecture is a complete solution that utilizes Ethereum blockchain 2.0 for fast data management and Elliptic Curve Cryptography for safe transaction verification [26]. This unique technique offers transparency, immutability, and decentralized control while solving issues like as scalability and storage capacity [27]. Blockchain technology has the potential to transform healthcare by allowing citizens to participate in health study programs, improving research, and creating a centralized database [28]. However, there are twelve challenges to its acceptability in GCC nations [29]. Rastogi et al.

(2024) in [30] show how blockchain-based IoT might enhance patient care while also lowering expenses by judiciously allocating medical resources. The suggested approach provides 96.123% more security. HealthRec-Chain is a patient-centric framework that uses IPFS to securely store and share medical reports and photos while protecting privacy and performance metrics with Java-enabled GPG encryption [31].

## **2.2 SQL Based Data Management in Healthcare**

The study in [32] discusses the issue of HIT tools, which integrates mobile agents and NoSQL technologies, to improve the efficiency of healthcare service. Mobile agents handle issues relevant to accessing distributed data, while NoSQL is designed to generate scalable applications with flexible structures. In this paper, the experimental setup had made use of Apache Jena Fuseki NoSQL server and the JAVA Agent Development Framework, commonly known as JADE. The growing use of digital technology in healthcare needs a thorough awareness of personal cybersecurity in order to preserve sensitive data and avoid risks [33]. Precision medicine and personalised therapies are increasingly reliant on the Multimodal Integration of Oncology Data System (MINDS). This paradigm combines approximately 41,000 instances from public sources, allowing for a patient-centered approach [34]. Its high compression ratio, query response times of less than 5 seconds, and interface enable researchers to unearth diagnostic and prognostic insights, resulting in evidence-based tailored therapy. The cloud-native design enables secure and efficient management of exponential data expansion. The study in [35] presents TinyML methods, such as TinyCleanEDF, EdgeClusterML, CompressEdgeML, CacheEdgeML, and TinyHybridSenseQ, to improve Big Data management in large-scale IoT systems. Edge AI-powered algorithms improve data processing, storage, and quality control. Experimental assessments yield encouraging outcomes, exceeding comparable procedures across a variety of parameters. The rising trends of network security risks require powerful evaluation systems that can be used to deal with vulnerabilities, viruses, and defects, especially in healthcare networks. Though the current systems are mainly designed for risk assessments, they usually do not include thorough security evaluations [36]. A practical simulation model for network security evaluation is required to enhance network protection through analysis and planning at various stages. Advancements in healthcare include an ontology-based model towards developing early detection for CVD, which is backed by AI-driven decision support systems [37]. This innovative model

will thus improve diagnostic accuracy and resource efficiency, providing scalable solutions towards early intervention and better patient outcomes. In the age of big data, informed decision-making is critical, and Large Language Models (LLMs) have transformed data management with in-context learning and enhanced reasoning capabilities [38]. Web-based technology provides a variety of online services, including medical and hospital processes, lowering prices and labor expenditures [39]. A web application that manages, communicates, stores, and updates patient data using bespoke programming may handle time-consuming tasks while improving patient information accessibility. The performance of this application is evaluated and compared to similar programming languages. EHR systems are widely employed in medical services, however they frequently fail to handle diverse data and sustain functionality. To overcome these difficulties, a novel graph-based EHR system is presented that combines Attribute-Based Encryption with Semantic Web Technologies [40]. This method uses semantic context to query a knowledge network while storing encrypted medical data in nodes. Cloud computing provides benefits to healthcare services, including on-demand service, high scalability, and virtualization. However, approaches like Deep Reinforcement Learning (Deep RL) and Kalman filtering have drawbacks such as high energy consumption, cost, and reaction time [41]. This unique layered technique uses Deep RL, Kalman filtering, and repeated training to identify the best service selection and composition solutions, providing acceptable results in terms of availability, reliability, energy consumption, and reaction time.

### **3 Methodology**

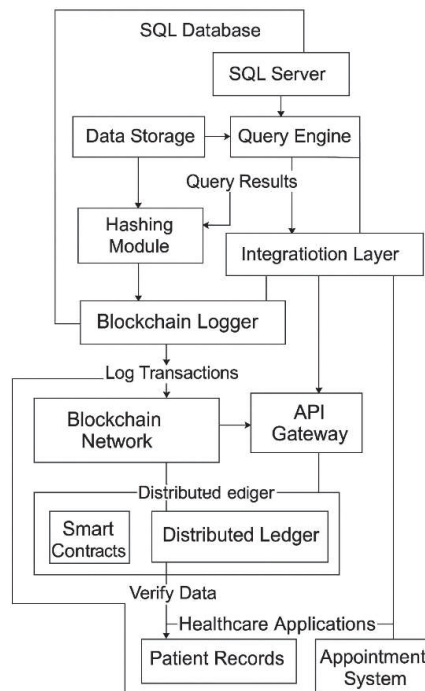
#### **3.1 Tools and Technologies**

The proposed system is a comprehensive suite of development tools ensuring effective secure, scalable and efficient management of the healthcare data. MySQL forms the backbone for structured data storage and retrieval giving real-time access to patient records, lab result and appointment details via optimized query execution process. Blockchain provides security, integrity, and transparency for data through a decentralized and tamper-proof framework, using Solidity-based smart contracts to automatically control access and validate transactions. Development tools like Apache servers, Python scripting, and blockchain APIs can be used to easily synchronize the SQL database with the blockchain ledger. All of these tools integrate into a workflow that ensures data consistency, secure interactions, and reliable performance in healthcare operations.

### 3.2 System Architecture

The system proposed architecture MBHA (MySQL-Blockchain Healthcare Architecture) brings together the strength of MySQL and blockchain technologies, giving a safe, decentralized, and efficient framework to handle healthcare data as shown in Figure 3. The rest of this section further elaborates on the architecture, its components and processes, while focusing on the layered structure and functionalities of this architecture.

The proposed MBHA architecture integrates traditional SQL-based data storage with blockchain technology to enhance the security, integrity, and traceability of healthcare information. At its core, the SQL Server manages structured data operations such as storage and querying, while the Integration Layer synchronizes these operations with other system modules. The Hashing Module generates cryptographic digests of critical data, which are passed to the Blockchain Logger for immutable registration on the blockchain. The Blockchain Network, governed by smart contracts, validates and logs these transactions into a Distributed Ledger. Meanwhile, the API Gateway



**Figure 3** Healthcare system integration with blockchain and SQL.

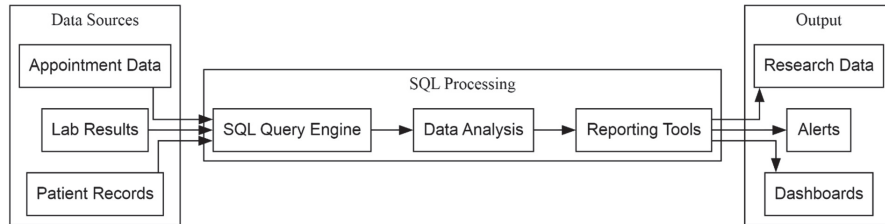
**Table 1** Functional overview of components in the MBHA blockchain-integrated healthcare architecture

<i>Component</i>	<i>Function</i>
<i>SQL Server</i>	Handles relational data storage and query processing
<i>Data Storage</i>	Stores structured healthcare data such as records and appointments
<i>Query Engine</i>	Executes SQL queries and fetches results
<i>Hashing Module</i>	Generates SHA-256 hashes of sensitive data for integrity verification
<i>Blockchain Logger</i>	Sends transaction hashes to the blockchain for immutable recording
<i>Blockchain Network</i>	Validates and confirms transactions using a consensus mechanism
<i>Smart Contracts</i>	Enforces automated rules for access, verification, and logging
<i>Distributed Ledger</i>	Maintains tamper-proof records of data access and changes
<i>API Gateway</i>	Serves as a communication interface between applications and backend
<i>Integration Layer</i>	Connects SQL query results with blockchain verification processes
<i>Patient Records</i>	Healthcare app for accessing validated patient information
<i>Appointment System</i>	Module for managing and verifying medical appointment data

acts as a unified interface between the backend and client-facing healthcare applications, including Patient Records and the Appointment System. These applications interact with both the SQL server and the blockchain to ensure that any accessed data is verified against the ledger, guaranteeing its authenticity and tamper-proof status. Table 1 provides a detailed overview of the core components within the MBHA architecture and their respective functions. Each module is designed to play a distinct role in ensuring the secure, verifiable, and efficient handling of healthcare data. The system combines a conventional SQL-based backend for high-performance storage and querying with blockchain-enabled modules that guarantee data immutability, access traceability, and decentralized validation. This modular design ensures that sensitive information is not only efficiently managed but also cryptographically protected and transparently audited through a distributed ledger. Together, these components create a cohesive infrastructure that addresses the critical challenges of trust, integrity, and interoperability in healthcare data systems.

### **A. SQL Database Layer**

The backbone of the architecture is where the SQL database layer comes in since it is capable of storing structured healthcare data with robust storage



**Figure 4** From data sources to outputs: SQL query engine in action.

and query processing capabilities that allow the efficient organization and accessibility of critical data in health care operations like patient records, lab results, and scheduled appointments (refer Figure 4).

### SQL Server

The structured healthcare data is stored in a central repository SQL Server. It supports optimized storage mechanisms for large-scale data, and this allows healthcare systems to effectively manage huge amounts of datasets. Low-latency response to real-time queries is ensured in the healthcare domain that is highly data-intensive. Mathematically, the SQL Server organizes data as:

$$HDS = \{P_i, L_j, A_k\}$$

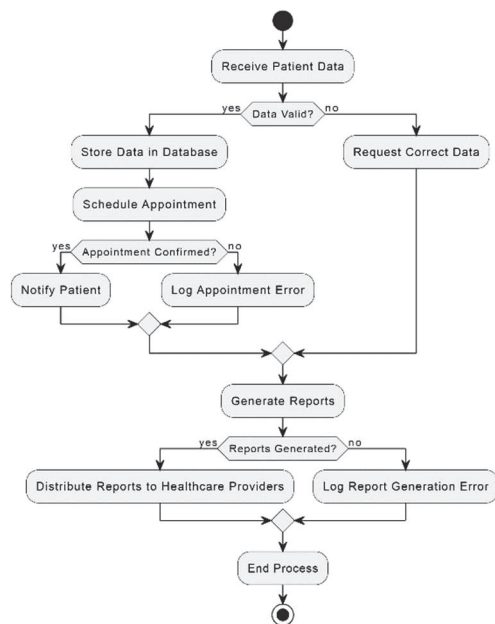
Where, HDS is denoted as Healthcare Data Set,  $P_i$  provides patient records,  $L_j$  represents lab records and  $A_k$  represents appointment data.

### Data Storage

The component for patient and doctor data storage holds all the data pertaining to them safely. This includes treatment records of the patients, prescriptions through doctors, and the logs for interactions between the doctors and their patients. This way, healthcare providers can have an overall record of care for every patient (refer Figure 5). For instance, doctors can avail prescription history or even some previous consultations straight from this system.

### Query Engine

The query engine supports complex queries that allow doctors to access and analyze patient data efficiently. Doctors can retrieve patient-specific data,



**Figure 5** End-to-end patient data handling flowchart.

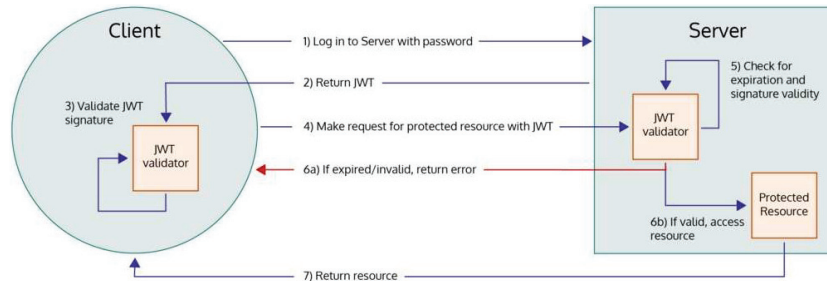
analyze trends in lab results, and review treatment efficacy over time. A typical query could be:

```
SELECT * FROM Patients WHERE PatientID = '12345';
```

This ensures doctors can make real-time, data-driven decisions based on accurate and up-to-date information.

## B. JWT tokens

A JSON Web Token, or JWT, is a compact, URL-safe means of representing claims between two parties, namely a client and a server. JWTs are used in distributed systems for authentication, data exchange, and access control. JWTs are encoded as JSON objects and can be digitally signed with algorithms such as HMAC or RSA to provide integrity and authenticity. JSON Web Tokens or JWTs are one of the widely used options for authentication and secure communication between a client and a server inside modern web and mobile applications as shown in Figure 6. This method facilitates a compact, URL-safe representation of claims, which are usually assertions



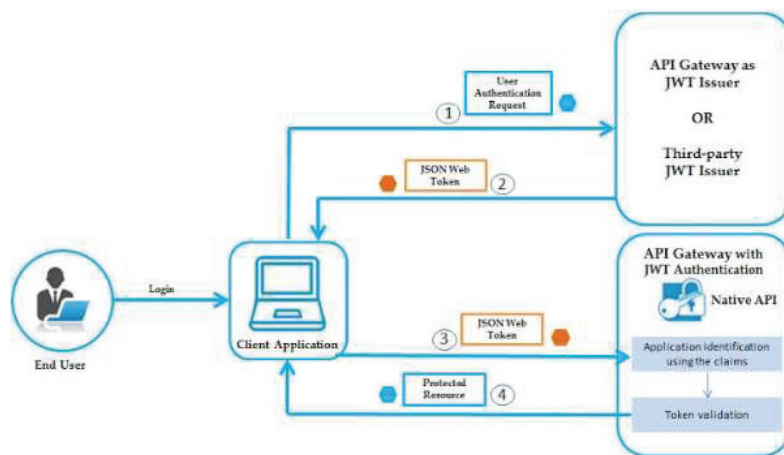
**Figure 6** JWT token lifecycle in client-server architecture.

made about some entity, like a user. These tokens ensure that they are self-contained; thus, the previous authentication systems are not required to be stateless, unlike the server-side session storage.

A JWT has three basic parts: header, payload, and signature. In the header, one defines the type of token-JWT and specifies which algorithm one intends to use to sign with for instance, HS256. Claims within a payload describe facts regarding an entity that include details on user details and role among other details. They are usually standardized in their own name (such as *iss*) and custom definition when specific applications so desire. The signature is achieved by using the header and payload, encoded and signed with a secret key or private key in the case of asymmetric encryption, ensuring the integrity of the token.

JWT tokens are the most useful for stateless authentication systems. The server checks their credentials, then creates a JWT containing all necessary claims for that user and sends it back to the client as a response, which will add this token in the Authorization header of each successive API call to the server, which then will be able to verify this token by decoding it and checking the signature without holding any session of the user as presented in Figure 7. Due to its stateless nature, JWT is highly scalable and suitable for distributed architectures.

JWTs are lightweight and efficient, especially for scenarios where low overhead is critical, such as mobile applications or microservices. They can be used not only for authentication but also for authorization. Access can be controlled based on roles and permissions encoded within the token. For instance, a token could include a claim stating that a user's role is "admin" to provision role-based access to certain resources. Security is one aspect of implementing JWT. Because a token can easily be intercepted through transmission, such tokens must be sent only on secure HTTPS. In addition to



**Figure 7** Secure authentication and authorization via API gateway using JWT.

this, the short exp attribute allows tokens to last for only as long as intended, limiting time exposure in the event of them being stolen. Long-lived tokens should be entirely avoided, and if not, refresh token mechanisms must exist to produce tokens when necessary. The payload should never store sensitive information like passwords or private keys because the token content can be decoded by anyone who has access to it. It's for this reason that they serve as the very core of today's modern identity management systems. However, it is their development that involves the best practice use of such items as the strength of the keys used to sign, setting the expiration date on tokens, and validating them carefully.

### C. Integration with Blockchain

For improvement in data security and trust, the SQL database is integrated smoothly with blockchain technology. This way, data that is shared among doctors, patients, and the healthcare system stays secure and tamper-proof.

### Data Synchronization

All data prescribed by doctors-whether prescriptions, diagnoses, or test results, for instance-can be updated directly in the blockchain as a form of immutability and accountability with regard to each doctor-patient interaction. A secure and clear record of communication between doctors and patients can no longer be doubted.

Mathematically, this can be expressed as:

$$B_i = Hash(HDS_i + D_i)$$

Where,  $B_i$  is Blockchain entry for the  $i$ th transaction,  $HDS_i$  is the Corresponding healthcare data for the  $i$ th record, and Log of actions performed by doctors (e.g., prescriptions, notes) are presented by  $D_i$ .

JWT is totally usable in the following manner before and after the blockchain, dependent on the use case and the flow of the system. Before adding blockchain, JWT could be the primary authentication method for user credentials and sessions between the client and servers. This step involves user authentication in terms of email and password, which are then verified against a MySQL database. Once verified, the backend will create a JWT containing claims such as user ID, roles, and the time to which it would expire. The JWT is then passed to the client and utilized for subsequent API requests by adding it to the Authorization header. This eliminates the requirement for server-side session storage, making the system stateless and scalable. For instance, in a healthcare application, a doctor logs in, and JWT ensures safe access to retrieve patient records or lab reports stored in the MySQL database.

### **API Gateway**

Doctors must first log into the gateway to interact with the system. Doctors can easily log in to locate patient data or update treatment history and analyze any historical trends for the treatment record. The gateway strictly adheres to the regulations; it also allows doctors to gain role-based access to sensitive information. The doctors would be an integral part of the proposed architecture; they would interact with the system in order to add value to patient care and provide sound data integrity. Doctors using the system would get healthcare data and update it with coherence regarding the retrieval, updating, and collaborative working of doctors. The system would allow doctors to obtain detailed medical histories of patients, lab results, and appointment schedules, thus enabling them to give accurate diagnoses and formulate appropriate treatment plans. Doctors can update the records of patients by using safe interfaces which update clinical notes, prescriptions, and outcomes of treatment. These will be copied automatically on the blockchain and all the changes can be accessed in a clear, secure, and immutably manner. Besides, a decentralized platform through blockchain empowers doctors belonging to different health care institutions for accessing the shared data of patients

**Table 2** Data-Level encryption techniques and implementation in the MBHA framework

Data Type	Encryption Technique	Key Handling	
		Mechanism	Tool/Library Used
Patient Personal Info	AES-256 (CBC mode)	Session key encrypted via RSA-2048	Java Crypto API + BouncyCastle
Authentication Tokens	JWT with HMAC-SHA256	Signed with server-side secret	JJWT (Java JWT) Library
Record Integrity Hash	SHA-256 Digest	Stored on Blockchain Ledger	Java MessageDigest + Web3j

if such consent is provided to that effect. It aligns with collaborative care practice in treating patients, continuing treatment while introducing a more integrated approach in handling patients, especially those with medical complexities. In this architecture, these features can be exploited in order to have doctors provide high-quality, patient-centered care.

### 3.3 Data Encryption and Security Module

To preserve confidentiality and ensure tamper-resistant handling of sensitive patient data, the proposed MBHA system integrates a dual-layered encryption protocol. The encryption pipeline operates in two stages: (i) symmetric encryption for data confidentiality, and (ii) asymmetric encryption for secure key distribution and access control. All healthcare data transmitted via the Java API is first encrypted using AES-256 (Advanced Encryption Standard) in CBC mode, providing high-speed encryption with strong security. Each encryption operation is initialized with a unique IV (Initialization Vector) and a secret key generated per session. These keys are never stored directly; instead, they are encrypted using RSA-2048 public-key cryptography, ensuring that only authorized healthcare personnel with the corresponding private key can decrypt the data. Furthermore, data hash values are generated using SHA-256 to ensure integrity. These hashes are logged on a private blockchain ledger (via the Blockchain Logging Module) to create an immutable audit trail that can detect any unauthorized modifications. For implementation, the system utilizes the Java Cryptography Architecture (JCA) with the BouncyCastle provider, allowing seamless integration of AES, RSA, and SHA functions within the backend logic.

To strengthen the privacy and integrity of healthcare data within the proposed framework, MBHA employs a layered encryption strategy

tailored to each data type and access mechanism. As outlined in Table 2, personal information is secured using AES-256 symmetric encryption, while key exchanges are managed through RSA-2048 to prevent unauthorized decryption. Additionally, authentication tokens are protected using industry-standard JWTs signed with HMAC-SHA256, and SHA-256 hashing is applied for immutable integrity verification. These encryption mechanisms are implemented using the Java Cryptography Architecture (JCA) along with trusted libraries like BouncyCastle and JJWT, ensuring compatibility with enterprise-grade security standards and offering verifiable, audit-friendly data protection throughout the system.

## **4 Results and Discussions**

The system, proposed in this research, was tested and validated as functional, secure, scalable, and performing well in a healthcare environment. There were multiple testing methodologies employed in the evaluation, aimed at validating the integration of MySQL and blockchain technologies, and overall performance.

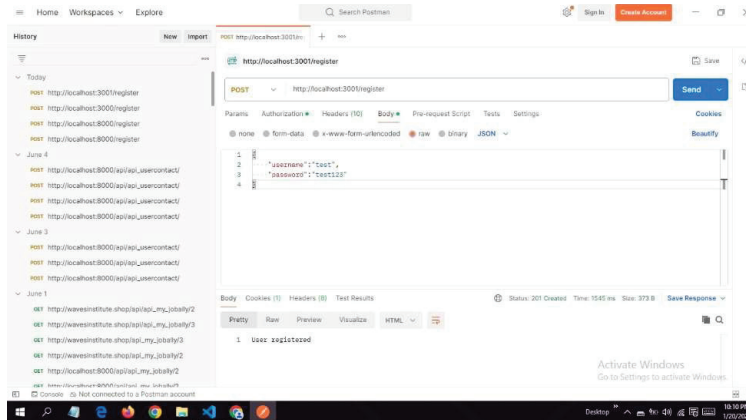
### **4.1 Functional Testing**

Functional testing is used to verify if each system feature works appropriately. All core functionalities like registration, login, retrieving data, and interaction with blockchain were executed through thorough tests. The data that is inserted while registering securely got stored into the MySQL server and ensured successful JWT token generation along with correct validation in case of a successful login. Besides that, blockchain-based interactions, including recording and retrieving immutable healthcare records, were tested to ensure that they met the expected requirements. All functionalities operated smoothly, making it user-friendly while maintaining backend efficiency.

### **2. API Functionality Testing with Postman**

This is done by using the tool called Postman. The most commonly used tool for testing APIs. These are the results recorded.

Registration Endpoint: It was observed that the POST request to the /register endpoint succeeded, thereby showing that a new user was registered with distinct credentials. As seen from the response message “User registered,” the API returned a successful status code of 201, meaning the user was successfully created.



**Figure 8** Postman API testing for user registration endpoint.

Login Endpoint: A POST request to the /login endpoint verified already existing user credentials. As soon as the authentication was successful, the server issued a JWT token for secure user sessions. The status code 200 and the message “Login successful” validate this, as depicted in Figure 8.

## 2. MySQL Database Check

The data persistence functionality was assessed using phpMyAdmin. User information (username, hashed password) was correctly stored into the MySQL database (refer Figure 9).

- Registration also hashed the user passwords before saving in the MySQL database, so no plaintext sensitive data was stored.
- Numerous registrations as multiple user entry in the user table indicated success in efficient acceptance of new registries.

## 3. Security Testing

To protect the critical healthcare information, security testing was conducted to test the system’s strength toward potential attacks. JWT tokens were tested in terms of integrity as well as expiration to avoid any kind of unauthorized access and session hijacking. The backend received tests for SQL injection to check for the strength of query database against malicious inputs. In addition, blockchain data immutability was proven by testing the execution of smart contracts and ensuring that stored transactions were tamper-proof. The system showed strong security features that effectively mitigated risks and ensured safe data exchange.

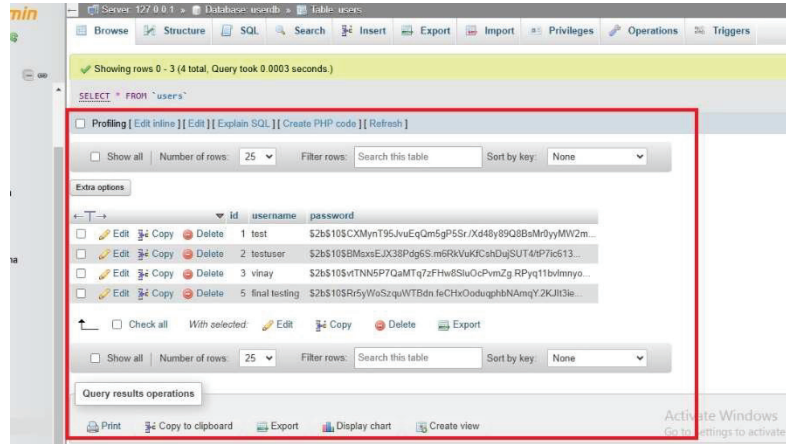


Figure 9 MySQL user table display in phpMyAdmin.

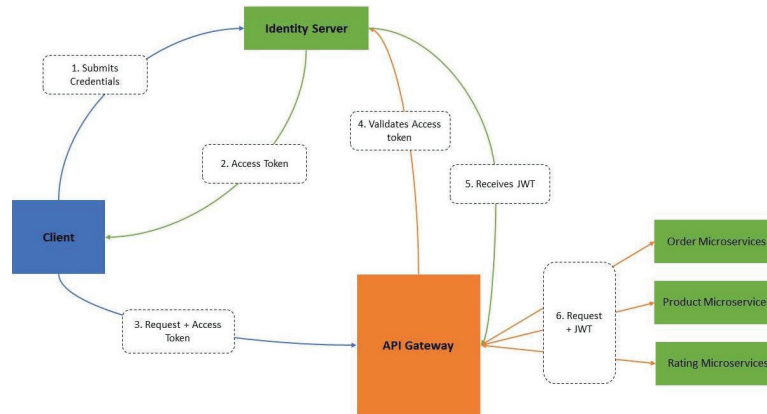


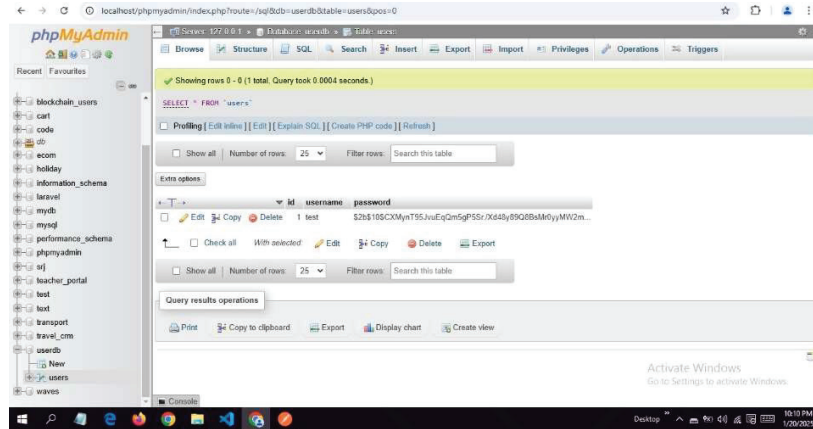
Figure 10 JWT authentication flow in a microservices architecture.

### JWT Token Authentication

We validated the integration of JWT tokens through a process as shown in Figure 10:

**Token Generation.** Once successfully logged in, a unique token was released to the user; such a token contains important user metadata, including an ID and roles.

**Token validation:** the token was used for further authentication to protected resources; expired or invalid tokens were not accepted to manage sessions strongly.



**Figure 11** MySQL database verification of user registration.

#### 4. System Workflow

Using process flow diagrams, the overall system workflow, from data input to output, was analyzed, as presented in Figure 11. The process comprised the following steps:

- Data Validation: It ensures that only valid inputs are processed.
- Database Interactions: Secure storage of user data and efficient querying.
- Report Generation: Notifications and reports generated based on user interactions.

#### 4.2 Performance Metrics

The proposed system was evaluated with critical performance indicators, including API response times, database query execution times, and JWT token generation efficiency. All these are significant metrics for establishing the appropriateness of the system in health care applications where robust and scalable data handling is required.

##### A. API Response Times

User registration and login API endpoints were extensively tested using Postman to determine their response times. The /register endpoint deals with user data validation, password hashing, and insertion into the database. It resulted in an average response time of 1.54 seconds compared to /login that went at 841 milliseconds since it just needed to authenticate the credentials,

generate a secure JWT, and return. These results indicate that the backend efficiently processes user authentication requests.

### B. Database Query Execution Times

It was analyzed how the MySQL database performs queries. Retrieving data-based queries, such as finding user information through an email address, took less than 1 millisecond (0.0004 seconds). Similarly, insert operations during user registration were almost at par. Thus, it can be said that the database schema and query optimization techniques employed have provided results effectively, and it can handle the large number of frequent reads and writes fast as shown in Table 3.

The proposed system, therefore, would meet critical needs in healthcare data management, though scalability, computational overhead, and synchronization delays as well as the compliance of regulations have to be considered. Subsequent versions of the system need to optimize its performance for a large-scale deployment, improve the security measures implemented, and adhere to regulations so that the system is practical and deployable.

### 4.3 Comparative Evaluation with Existing Healthcare Data Management Systems

To validate the effectiveness of the proposed MBHA framework, a comparative analysis was conducted against traditional SQL-based systems

**Table 3** Performance evaluation is summarized below

Metric	Endpoint/Operation	Average Time	Details
<b>API Response Time</b>	Registration (/register)	1.54 seconds	Includes user validation, password hashing, and database insertion.
<b>API Response Time</b>	Login (/login)	841 milliseconds	Covers user authentication and JWT token generation.
<b>Database Query Execution</b>	User Data Retrieval Query	< 1 millisecond	Query execution time for fetching user data from the users table.
<b>Database Query Execution</b>	Data Insertion (Registration)	< 1 millisecond	Includes insertion of new user data into the MySQL database.
<b>JWT Token Generation Time</b>	During Login	< 50 milliseconds	Time required to generate and validate JWT tokens for authenticated users.

**Table 4** Comparative performance and feature evaluation of MBHA with traditional and blockchain-based systems

Feature/Metric	Traditional System [32, 34]	Blockchain-Only SQL System [21,24]	MBHA (Proposed)
<b>Avg. API Response Time</b>	1.2 sec	3.5 sec	<b>0.84–1.54 sec</b>
<b>Query Execution Speed</b>	Fast	Slow	<b>Fast (&lt;1 ms)</b>
<b>Data Integrity &amp; Tamper Detection</b>	×	✓	✓ + <b>Blockchain Logs</b>
<b>JWT-Based Session Control</b>	Partial	Rare	<b>Full Integration</b>
<b>Smart Contract Automation</b>	×	Partial	<b>Fully Utilized</b>
<b>Scalability</b>	Moderate	Low	<b>High</b>

[32, 34] and standalone blockchain-based healthcare architectures [21, 24]. The comparison focused on key performance metrics and architectural capabilities, including API response times, data integrity, smart contract usage, and scalability. As presented in Table 4, MBHA outperforms existing systems by achieving faster response times, maintaining tamper-proof data integrity through blockchain logging, and offering comprehensive security features such as JWT-based session control and smart contract-driven automation. These results establish MBHA as a balanced and scalable solution that overcomes the limitations of both conventional and decentralized approaches.

## 5 Conclusions and Future Work

This study proposes the MySQL-Blockchain Healthcare Architecture, a system that combines the efficiency of MySQL data management with the security and decentralized framework of blockchain to eliminate traditional healthcare information systems' limitations. The performance metrics validate the efficiency and the suitability of this system for healthcare applications, which includes an API response time for registration in 1.54 seconds, login at 841 milliseconds, and database query times within 1 millisecond. JWT generation is accomplished within 50 milliseconds, which ensures that users are authenticated rapidly and securely. These results establish the system's ability to process real-time data while establishing secure communication in a scalable and reliable manner.

The proposed architecture highly improves health data management because of the features like integrity of data, transparency, and proper secure

access to sensitive information. The proposed system ensures collaborative care by the different health care providers in place with regard to issues related to privacy and security. But scalability and regulatory compliance need improvements. Optimization of system scalability and compliance of regulations related to health care remain in the research areas. The results of this research serve as a solid foundation for next-generation innovations in healthcare IT, offering a robust and effective solution for the secure management of data in this rapidly evolving domain.

### **Acknowledgment**

I sincerely thank Dr. Tan Kuan Tak, Engineering Cluster, Singapore Institute of Technology, Singapore, for his invaluable guidance and support during the successful completion of my postdoctoral fellowship (Remotely) at the Engineering Cluster, Singapore Institute of Technology, Singapore.

### **Funding**

No Funding support is provided for this paper publication.

### **Competing Interests**

No benefits in any form have been received or will be received from a commercial party related directly or indirectly to the subject of this article. All authors declare no conflict of interest for this article.

### **Author Contributions**

All authors have accepted responsibility for the entire content of this manuscript, and reviewed and approved its submission.

### **Ethics Approval and Consent to Participate**

No Participation of humans take place in this implementation process.

### **Consent to Publish**

All authors are showing their consent to publish this paper.

## Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

## References

- [1] Pandey, Abhishek Kumar, Asif Irshad Khan, Yoosef B. Abushark, Md Mottahir Alam, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. “Key issues in healthcare data integrity: Analysis and recommendations.” *IEEE Access* 8 (2020): 40612–40628.
- [2] Zarour, Mohammad, Mamdouh Alenezi, Md Tarique Jamal Ansari, Abhishek Kumar Pandey, Masood Ahmad, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. “Ensuring data integrity of healthcare information in the era of digital health.” *Healthcare Technology Letters* 8, no. 3 (2021): 66–77.
- [3] Vimalachandran, Pasupathy, Hua Wang, Yanchun Zhang, Ben Heyward, and Frank Whittaker. “Ensuring data integrity in electronic health records: A quality health care implication.” In *2016 International Conference on Orange Technologies (ICOT)*, pp. 20–27. IEEE, 2016.
- [4] Sarker, M. (2024). Revolutionizing healthcare: the role of machine learning in the health sector. *Journal of Artificial Intelligence General science (JAIGS)* ISSN: 3006-4023, 2(1), 36–61.
- [5] Rath, K. C., Khang, A., Rath, S. K., Satapathy, N., Satapathy, S. K., and Kar, S. (2024). Artificial intelligence (AI)-enabled technology in medicine-advancing holistic healthcare monitoring and control systems. In *Computer Vision and AI-Integrated IoT Technologies in the Medical Ecosystem* (pp. 87–108). CRC Press.
- [6] Ogundipe, D. O. (2024). The impact of big data on healthcare product development: A theoretical and analytical review. *International Medical Science Research Journal*, 4(3), 341–360.
- [7] Ahammed, M. F., and Labu, M. R. (2024). Privacy-Preserving Data Sharing in Healthcare: Advances in Secure Multiparty Computation. *Journal of Medical and Health Studies*, 5(2), 37–47.
- [8] Ramani, R., Mary, A. R., Raja, S. E., and Shunmugam, D. A. (2024). Optimized data management and secured federated learning in the Internet of Medical Things (IoMT) with blockchain technology. *Biomedical Signal Processing and Control*, 93, 106213.

- [9] Chen, J., Yi, C., Du, H., Niyato, D., Kang, J., Cai, J., and Shen, X. (2024). A revolution of personalized healthcare: Enabling human digital twin with mobile AIGC. *IEEE Network*.
- [10] Zhao, X., Bai, Z., Zhan, X., Wang, J., Cheng, Y., and Xiao, X. (2024). Safety evaluation of traditional Chinese medicine: New era, new strategy. *Acupuncture and Herbal Medicine*, 4(2), 171–175.
- [11] Chowdhury, R. H. (2024). The evolution of business operations: unleashing the potential of Artificial Intelligence, Machine Learning, and Blockchain. *World Journal of Advanced Research and Reviews*, 22(3), 2135–2147.
- [12] Palaniappan, K., Lin, E. Y. T., and Vogel, S. (2024, February). Global regulatory frameworks for the use of artificial intelligence (AI) in the healthcare services sector. In *Healthcare* (Vol. 12, No. 5, p. 562). MDPI.
- [13] Song, D., Zhang, H., Shi, L., Xu, H., and Xu, Y. (2024). S5Utis: Structured State-Space Sequence SegNeXt UNet-like Tongue Image Segmentation in Traditional Chinese Medicine. *Sensors*, 24(13), 4046.
- [14] Baseer, K. K., Sivakumar, K., Veeraiah, D., Chhabra, G., Lakineni, P. K., Pasha, M. J., ... and Harikrishnan, G. (2024). Healthcare diagnostics with an adaptive deep learning model integrated with the Internet of medical Things (IoMT) for predicting heart disease. *Biomedical Signal Processing and Control*, 92, 105988.
- [15] Raman, R., Verma, M. A., Kumar, V., Rastogi, S., Pillai, B. G., and Meenakshi, R. (2024, May). Fog Computing Integrated with and Blockchain Technology for Accurate Disease Prediction. In *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 677–682). IEEE.
- [16] Kasula, B. Y. (2023). The Role of Blockchain Technology in Securing Electronic Health Records. *Transactions on Latest Trends in Artificial Intelligence*, 4(4).
- [17] Thatikonda, R., Vaddadi, S. A., and Dash, B. (2024). Applications of blockchain technology in healthcare. In *Research Advances in Network Technologies* (pp. 189–205). CRC Press.
- [18] Hyrynsalmi, S., Hyrynsalmi, S. M., and Kimppa, K. K. (2021). The state of the art of the blockchain ethics in healthcare: A systematic literature review. *Finnish Journal of eHealth and eWelfare*, 13(3), 193–206.
- [19] Dubey, S., and Tiwary, A. K. (2023, June). Smart Education based on Blockchain Technology. In *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)* (pp. 1485–1490). IEEE.

- [20] Kumar, A., Singh, A. K., Ahmad, I., Kumar Singh, P., Anushree, Verma, P. K., ... and Tag-Eldin, E. (2022). A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. *Sensors*, 22(15), 5921.
- [21] Healthcare database technologies with blockchain.
- [22] Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, 15(1), 70–83.
- [23] Haleem, A., Javaid, M., Singh, R. P., Suman, R., and Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, 2, 130–139.
- [24] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., and Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks*, 200, 108500.
- [25] Hussien, H. M., Yasin, S. M., Udzir, N. I., Ninggal, M. I. H., and Salman, S. (2021). Blockchain technology in the healthcare industry: Trends and opportunities. *Journal of Industrial Information Integration*, 22, 100217.
- [26] Al-Marridi, A. Z., Mohamed, A., and Erbad, A. (2024). Optimized blockchain-based healthcare framework empowered by mixed multi-agent reinforcement learning. *Journal of Network and Computer Applications*, 224, 103834.
- [27] Alijoyo, F. A., Prabha, B., Aarif, M., Fatma, G., and Rao, V. S. (2024, July). Blockchain-Based Secure Data Sharing Algorithms for Cognitive Decision Management. In *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1–6). IEEE.
- [28] Hakimi, N., Fathi, Z., and Pourbahrami, B. (2024). Application of Metacombination Technique in the Financial Flow Based on Blockchain Technology in the Hospital Ecosystem. *Dynamic Management and Business Analysis*, 2(4), 74–93.
- [29] Mutambik, I., Lee, J., Almuqrin, A., and Alharbi, Z. H. (2024, January). Identifying the Barriers to Acceptance of Blockchain-Based Patient-Centric Data Management Systems in Healthcare. In *Healthcare* (Vol. 12, No. 3, p. 345). MDPI.
- [30] Rastogi, P., Singh, D., and Bedi, S. S. (2024). An improved blockchain framework for ORAP verification and data security in healthcare. *Journal of Ambient Intelligence and Humanized Computing*, 1–16.
- [31] Kumari, D., Parmar, A. S., Goyal, H. S., Mishra, K., and Panda, S. (2024). Healthrec-chain: patient-centric blockchain enabled ipfs for privacy preserving scalable health data. *Computer Networks*, 241, 110223.

- [32] SQL based data management in healthcare.
- [33] Kotsilieris, T. (2021, March). An efficient agent based data management method of NoSQL environments for health care applications. In *Healthcare* (Vol. 9, No. 3, p. 322). MDPI.
- [34] Sharma, D. P., Lashkari, A. H., and Parizadeh, M. (2024). Understanding Cybersecurity Management in Healthcare. *Progress in IS*.
- [35] Tripathi, A., Waqas, A., Venkatesan, K., Yilmaz, Y., and Rasool, G. (2024). Building flexible, scalable, and machine learning-ready multi-modal oncology datasets. *Sensors*, 24(5), 1634.
- [36] Karras, A., Giannaros, A., Karras, C., Theodorakopoulos, L., Mammassis, C. S., Krimpas, G. A., and Sioutas, S. (2024). TinyML algorithms for Big Data Management in large-scale IoT systems. *Future Internet*, 16(2), 42.
- [37] Nagabhooshanam, N., Murthy, C. R., and CosioBorda, R. F. (2023). Neural network based single index evaluation for SQL injection attack detection in health care data. *Measurement: Sensors*, 27, 100779.
- [38] Doniec, R., Berepiki, E. O., Piaseczna, N., Sieciński, S., Piet, A., Irshad, M. T., ... and Glinkowski, W. (2024). Cardiovascular Disease Preliminary Diagnosis Application Using SQL Queries: Filling Diagnostic Gaps in Resource-Constrained Environments. *Applied Sciences*, 14(3), 1320.
- [39] Zhang, M., Ji, Z., Luo, Z., Wu, Y., and Chai, C. (2024, May). Applications and challenges for large language models: From data management perspective. In *2024 IEEE 40th International Conference on Data Engineering (ICDE)* (pp. 5530–5541). IEEE.
- [40] Kathiravan, M., Lakshmi, I., Durga, V. S., Saravanan, S., Vijayakumar, M., and Bharathiraja, N. (2024, February). Java-Powered Digital Healthcare Management: innovating Medical Administration Systems. In *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)* (Vol. 5, pp. 1333–1338). IEEE.
- [41] Walid, R., Joshi, K. P., and Choi, S. G. (2024). Leveraging semantic context to establish access controls for secure cloud-based electronic health records. *International Journal of Information Management Data Insights*, 4(1), 100211.
- [42] Zhong, C., Darbandi, M., Nassr, M., Latifian, A., Hosseinzadeh, M., and Navimipour, N. J. (2024). A new cloud-based method for composition of healthcare services using deep reinforcement learning and Kalman filtering. *Computers in Biology and Medicine*, 172, 108152.

## Biographies



**Deepak Chandra Uprety** is an Associate Professor in the Department of Computer Science at Noida Institute of Engineering & Technology, 19, Knowledge Park-II, Institutional Area, Greater Noida, India. He has B. Tech, M. Tech, and PhD degree in Computer Science & Engineering. Mobile computing is one of the interesting fields and also has publications and papers in other areas such as Big Data, AI & ML, etc. His areas of specialization include Data mining, and Computer graphics, in addition to Artificial Intelligence and Machine Learning.



**Kamal Upreti** is currently working as an Associate Professor in Department of Computer Science, CHRIST (Deemed to be University), Delhi NCR, Ghaziabad, India. He completed is B. Tech (Hons) Degree from UPTU, M. Tech (Gold Medalist), PGDM (Executive) from IMT Ghaziabad and PhD in Department of Computer Science & Engineering. He has completed Postdoc from National Taipei University of Business, TAIWAN funded by MHRD.

He has published 50+ Patents, 32+Magazine issues and 154+ Research papers in in various reputed Journals and international Conferences. His areas of Interest such as Modern Physics, Data Analytics, Cyber Security, Machine

Learning, Health Care, Embedded System and Cloud Computing. He has published more than 45+ authored and edited books under CRC Press, IGI Global, Oxford Press and Arihant Publication. He is having enriched years' experience in corporate and teaching experience in Engineering Colleges.

He worked with HCL, NECHCL, Hindustan Times, Dehradun Institute of Technology and Delhi Institute of Advanced Studies, with more than 15+ years of enrich experience in research, Academics and Corporate. He also worked in NECHCL in Japan having project – “Hydrastore” funded by joint collaboration between HCL and NECHCL Company. Dr. Upreti worked on Government project – “Integrated Power Development Scheme (IPDS)” was launched by Ministry of Power, Government of India with the objectives of Strengthening of sub-transmission and distribution network in the urban areas. Currently, he has completed work with Joint collaboration with GB PANT & AIIMS Delhi, under funded project of ICMR Scheme on Cardiovascular diseases prediction strokes using Machine Learning Techniques from year 2017–2020 of having fund of 80 Lakhs. He got 5 Lakhs fund from DST SERB for conducting International Conference, ICSCPS-2024, 13–14 Sept 2024. Recently, he got 10 Lakhs fund from AICTE – Inter-Institutional Biomedical Innovations and Entrepreneurship Program (AICTE-IBIP) for 2024–2026. He has attended as a Session Chair Person in National, International conference and key note speaker in various platforms such as Skill based training, Corporate Trainer, Guest faculty and faculty development Programme. He awarded as best teacher, best researcher, extra academic performer and Gold Medalist in M. Tech programme.



**Pravin R. Kshirsagar** presently serving as a Professor at Electronics & Telecommunication Engineering, J D College of Engineering & Management, Nagpur India. Previously, he served as a HOD, Vice Principal,

Dean R&D, Head-ETC in the in prominent Institute of India. Under his Supervision Three scholars awarded the Ph.D thesis. He is Recognized Post-Doc supervisor in many countries also guiding four Post-doc fellow. He has achieved Hon. D.Eng for outstanding contribution in artificial neural modeling in neuroscience from Shiraz university of medical sciences in May 2022. He has vast experience of 22 years in teaching. He has served as reviewer in many international journals such as Inderscience, Spinger, Elsevier and IEEE Transaction. He has also delivered special talks in National & International conferences and chaired various technical sessions in International conferences. He has published various research papers in reputed journals. He has published more than 120 paper in National & International levels. He has 40 Indian Patent in his credential and 20 International Patent, He has 10 books in his credential. He is profoundly engrossed in the area of Data Science, Machine Learning, Artificial Intelligence, and Computer Networks.



**Tan Kuan Tak** is currently an Associate Professor at the Singapore Institute of Technology (SIT). He is registered as Chartered Engineer with Engineering Council, UK and Certified Energy Manager with The Institution of Engineers, Singapore. He is also a Specialist Adult Educator registered with the Institute for Adult Learning, Singapore. Dr Tan has several years of teaching experience in the engineering field. Prior to joining SIT, he has worked as a research fellow in NTU, as an engineer at SP PowerGrid, and as a lecturer at Ngee Ann Polytechnic, Singapore. His research interests include smart grids and microgrids, power distribution systems and protection, advanced electrification for transportation and buildings and energy management.



**Shitiz Upreti** is an Assistant Professor and Researcher at IILM University, Greater Noida, in the School of Computer Science and Engineering. With over 12 years of experience in academia, research, and workshop facilitation, he brings extensive knowledge to the classroom and beyond. His specialisations include Artificial Intelligence (AI), Machine Learning (ML), Business Analytics, and Cloud Computing. He is committed to promoting innovation and analytical thinking and actively participates in value-added courses and multidisciplinary research. His dedication to excellence in teaching and mentoring helps develop future-ready workers in the ever-changing tech industry. He continues to make valuable contributions to both academics and industry.



**Ganesh V. Radhakrishnan** is a Senior Professor at the KIIT School of Management, with over 30 years of experience in military service, industry leadership, and academia. He holds a Ph.D. from IIM Ahmedabad and an MBA from IIM Kozhikode. His primary research focuses on port economics and public systems. His current research examines the economic impacts of supply chain optimization, port efficiency, sustainability, and the application of AI in management. A prolific scholar, Dr. Radhakrishnan has published extensively in peer-reviewed journals and presented at leading

international conferences. He has held significant academic leadership roles, advancing research and fostering interdisciplinary collaborations with global institutions.



**Ajay Kumar** obtained his B.Tech (Industrial Engineering) from NIT, Jalandhar, M.Tech (Mechanical Engineering) from IIT Roorkee, Ph.D. (Mechanical Engineering) from NIT, Kurukshetra and completed six months course on Data Science and Machine Learning from IIT Delhi and Post doctorate Researcher/ Remote from Singapur institute of Technology. Prof. Kumar has a rich experience of over twenty-Six years of teaching undergraduate and postgraduate Engineering students.

Presently, he is serving as Director, Inderprastha Engineering College, Ghaziabad. Prior to this he had worked with many reputed private institutions and university. His areas of interest include Industrial Engineering, Modeling & Simulation Manufacturing Engineering (especially in Advanced Welding processes) and Data Science & Machine Learning.

He has published more than thirty research papers in national and international Journals of repute and conferences as well. He has published three patents in the area of Mechanical Engineering. Moreover, he has also guided seven M.Tech Dissertations, and guided three Ph.D. candidates as well.

He is also a Fellow Member of Institution of Engineers, India and IEEE Life member of Indian Society for Technical Education (I.S.T.E.); Senior Individual Member of Indian National Academy of Engineering (INAE). He had been the member in Board of Study (BOS) & Academic Council for many reputed Universities.