ISSN 2277-2685
IJESR/Jan-Mar. 2026/ Vol-16/Issue-1/445-452
B.Mahesh *et. al.*, / International Journal of Engineering & Science Research
Full Length Article

Secure And Private Analytics Of Healthcare Records In Multi-Tenant Cloud Environments Using Blockchain

P.Jayaraju[1],B.Mahesh[2],G.Aravind[3],K.Adithya[4]
[1]Assistant Professor; Department Of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad, India.
[2,3,4]B.Tech Students; Department Of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad, India.
Mail Id; adithya9391@gmail.com[4]
Accepted 26-03-2026

Abstract
The growing volume of digital healthcare data and increasing incidents of data breaches have intensified concerns regarding the protection of sensitive patient information. Healthcare analytics systems must therefore balance privacy preservation with the ability to generate meaningful insights. This paper presents a secure framework that integrates privacy-preserving mechanisms, zero-knowledge proofs (zk-SNARKs), blockchain technology, and a multi-tenant cloud architecture to address these challenges. The proposed approach safeguards healthcare records during analytical computations by applying advanced cryptographic techniques, enabling verification without revealing underlying data.Within the framework, anonymized healthcare datasets are processed by a privacy-preserving analytics engine that generates zk-SNARK proofs to validate computations. These proofs are recorded on a blockchain network, creating a transparent and tamper-resistant ledger that enhances trust and security in healthcare data transactions. Such a mechanism is particularly beneficial in telemedicine scenarios, where secure sharing and processing of patient information are critical. The implementation of the proposed model in a telemedicine application demonstrates its scalability, reliability, and effectiveness. Overall, the framework provides a practical solution for secure healthcare analytics while maintaining strict privacy guarantees.

Keywords— *Healthcare Data Security, Privacy-Preserving Analytics, Zero-Knowledge Proofs (zk-SNARKs), Blockchain Technology, Cloud Computing, Data Privacy.*

INTRODUCTION

Healthcare analytics has transformed modern medical decision-making by enabling the extraction of meaningful insights from large-scale clinical datasets. However, the growing use of digital health records and cloud-based platforms has intensified concerns regarding the privacy and security of sensitive patient information. Protecting healthcare data while maintaining its analytical usefulness remains one of the most critical challenges in collaborative healthcare environments.

Healthcare records contain highly confidential information, including patient identities, diagnoses, treatment histories, and financial details. Traditional encryption techniques primarily safeguard data during storage and transmission, but they often require decryption before analytics operations. This exposure creates potential vulnerabilities, particularly in shared cloud infrastructures where multiple organizations operate simultaneously. Therefore, a robust mechanism is required to enable secure analytics without revealing raw patient data.

To address these concerns, this work proposes a privacy-preserving healthcare analytics framework that integrates zero-knowledge proofs, specifically zk-SNARKs, blockchain technology, and a multi-tenant cloud architecture. Zero-knowledge proofs allow verification of computation correctness without disclosing underlying data, thereby preserving confidentiality during analytics processes. This capability is particularly valuable in telemedicine platforms and collaborative research environments where data sharing is essential but privacy must remain intact.Blockchain technology complements this approach by providing an immutable and decentralized ledger for storing verification proofs and transaction records. The integration ensures transparency, accountability, and tamper-resistant audit trails for healthcare analytics operations. By combining zk-SNARKs with blockchain, the framework establishes trust among participating entities without compromising data privacy.The proposed framework also supports multi-tenant cloud environments, where healthcare providers, research institutions, and telemedicine platforms share computing resources. Strong tenant isolation mechanisms and cryptographic verification techniques are employed to prevent unauthorized access and cross-tenant data leakage. Additionally, anonymization techniques are incorporated to

ensure that meaningful insights can be derived without exposing personally identifiable information.The importance of privacy preservation in healthcare analytics is further emphasized by the increasing number of global data breaches affecting healthcare organizations. These incidents not only compromise patient confidentiality but also lead to financial losses, legal penalties, and erosion of public trust. As telemedicine and remote healthcare monitoring continue to expand, the need for secure analytics solutions becomes even more urgent.

Moreover, regulatory requirements such as HIPAA and GDPR demand strict data protection measures, auditability, and accountability. The proposed framework addresses these requirements by offering cryptographic verification, secure data sharing, and immutable audit logs. By decoupling data ownership from computation, healthcare providers can collaborate securely while maintaining control over sensitive information.

This study introduces and evaluates the proposed privacy-presing analytics model using a telemedicine application use case. The implementation demonstrates how secure analytics can be performed in real-world healthcare scenarios without exposing raw data. The contributions of this work include enhanced privacy protection, improved scalability, and verifiable computation integrity for distributed healthcare systems.

Overall, this research aims to provide a secure and scalable foundation for collaborative healthcare analytics. By combining zero-knowledge proofs, blockchain technology, and cloud computing, the proposed framework advances privacy-preserving analytics and supports innovation in modern healthcare ecosystems.

Scope of the Project

The scope of this project involves designing and implementing a secure analytics framework for healthcare data within a multi-tenant cloud environment. The system focuses on preserving patient privacy while enabling efficient data analysis. Zero-knowledge proofs are incorporated to verify computations without revealing sensitive medical records.Blockchain technology is integrated to provide immutability, transparency, and tamper-proof logging of analytics proofs and healthcare transactions. The framework also supports anonymized data processing and secure data sharing among authorized entities. Multi-tenant isolation mechanisms ensure that data belonging to different organizations remains strictly separated.

The project further evaluates system performance, scalability, and security using a telemedicine application scenario. It examines how the framework protects healthcare data during storage, transmission, and computation while maintaining efficiency. Additionally, the study identifies vulnerabilities in conventional cloud-based healthcare analytics systems and demonstrates how the proposed solution mitigates these risks.

Objective

The primary objective of this project is to develop a secure and privacy-preserving healthcare analytics framework using advanced cryptographic techniques. The system aims to protect sensitive medical data throughout processing, sharing, and analysis in multi-tenant cloud environments.

Another key objective is to implement zero-knowledge proofs, particularly zk-SNARKs, to verify analytics computations without exposing raw patient information. The project also seeks to integrate blockchain technology to provide an immutable and transparent ledger for storing verification proofs and secure transactions.

additional objectives include preventing unauthorized access, eliminating cross-tenant data leakage, and supporting anonymized analytics. The framework aims to enhance trust among patients, healthcare providers, and telemedicine platforms by providing verifiable computation integrity.

The project further demonstrates practical applicability through a telemedicine use case. By combining cloud computing, blockchain, and cryptographic verification, the system aims to deliver a scalable and secure solution for next-generation healthcare analytics.

Problem Statement

Healthcare organizations increasingly rely on cloud-based analytics to extract insights from large volumes of medical data. However, this shift introduces significant privacy and security challenges. In multi-tenant cloud environments, multiple entities share computational resources, increasing the risk of unauthorized access and data leakage.Traditional encryption techniques protect data at rest but fail to secure information during computation. Data must often be decrypted before analysis, exposing it to potential threats. Furthermore, existing systems lack mechanisms to verify analytics computations without revealing underlying data, leading to trust issues among participating organizations.Another limitation is the absence of transparent and tamper-proof logging mechanisms. Without secure audit trails, ensuring integrity and accountability becomes difficult. The rapid growth of telemedicine also demands secure data sharing between patients and healthcare providers, which conventional systems cannot guarantee at scale.Therefore, a robust framework is required to enable privacy-preserving analytics while ensuring transparency, security, and scalability. This project addresses these challenges by integrating zk-SNARKs, blockchain technology, and multi-tenant cloud security mechanisms.

Existing System

Current healthcare analytics systems rely on centralized cloud architectures and traditional encryption techniques. Although these approaches provide basic data protection, they do not adequately secure information during analytics computations. Blockchain-based models improve data integrity but often suffer from scalability and performance limitations.Several existing solutions incorporate encryption and access control mechanisms; however, they lack cryptographic verification for computation correctness. Additionally, many frameworks do not provide efficient tenant isolation in shared cloud environments, increasing the risk of privacy breaches.

Proposed System

The proposed framework introduces a privacy-preserving analytics model that integrates zk-SNARKs, blockchain, and multi-tenant cloud computing. The system ensures that healthcare data remains confidential while enabling meaningful analytics. Zero-knowledge proofs verify computation correctness without exposing raw data, while blockchain provides tamper-proof logging and transparency.The architecture supports anonymized data processing, secure sharing, and strong tenant isolation. By combining these technologies, the framework delivers a scalable and secure solution for collaborative healthcare analytics.

PROJECT DESCRIPTION

This project introduces a secure and privacy-preserving framework designed for performing analytics on healthcare records within a multi-tenant cloud environment. The architecture combines blockchain technology with advanced cryptographic mechanisms to ensure that sensitive patient information remains protected during storage, transmission, and analytical processing. The central objective is to enable meaningful data analytics while maintaining strict confidentiality and data integrity.

A key feature of the proposed framework is the integration of zero-knowledge proofs, particularly zk-SNARKs. These proofs allow computational results to be verified without revealing the underlying healthcare data. Medical records are first anonymized and then processed by a privacy-preserving analytics engine. After computation, the system generates zk-SNARK proofs that confirm the correctness of the analytical results. These proofs are subsequently recorded on a blockchain ledger, providing an immutable and tamper-resistant history of all analytics operations.The use of blockchain technology enhances trust and transparency among stakeholders, including healthcare providers, patients, researchers, and administrators. Each transaction, verification proof, and access request is logged securely, preventing unauthorized modifications. This approach is especially useful in telemedicine environments where secure data sharing and remote computation are essential.By combining cryptographic privacy, decentralized verification, and cloud scalability, the proposed framework offers a practical solution for modern healthcare analytics. The architecture ensures confidentiality of patient data while supporting collaborative analytics across multiple organizations.

Methodologies

Module Names

The system is divided into the following modules:

Module	Description
Blockchain	Maintains immutable and decentralized storage of healthcare transactions
Zero-Knowledge Proofs (zk-SNARKs)	Enables verification of computations without exposing sensitive data
Homomorphic Encryption	Allows computation directly on encrypted healthcare records
SHA-256	Ensures data integrity using cryptographic hashing
JSP Dashboard	Provides user interface for data visualization and system interaction
MySQL Database	Stores user details and supporting metadata

1. Blockchain Module

The blockchain module acts as the core infrastructure for secure data storage and transaction management. It maintains a distributed ledger where healthcare transactions such as record uploads, analytics requests, and verification results are stored. Each block contains encrypted data, timestamps, and hash values linked to the previous block. This chaining mechanism prevents unauthorized modifications and ensures data immutability. The decentralized structure eliminates single points of failure and provides transparency across multiple stakeholders.

2. Zero-Knowledge Proofs (zk-SNARKs) Module

This module enables verification of analytics computations without exposing sensitive medical information. When analytics are performed on anonymized or encrypted data, zk-SNARKs

generate mathematical proofs confirming the correctness of the results. These proofs are lightweight and efficient, making them suitable for cloud-based healthcare environments. Each proof is recorded on the blockchain, ensuring transparency and tamper-proof validation.

3. SHA-256 Module

The SHA-256 module ensures data integrity by generating unique hash values for files, identities, and transactions. Each uploaded record produces a 256-bit hash that serves as a digital fingerprint. Any modification to the data results in a completely different hash value, allowing the system to detect tampering. This mechanism supports secure identity management and data verification within the blockchain network.

4. Homomorphic Encryption Module

The homomorphic encryption module allows computations to be performed on encrypted healthcare data without decrypting it. Patient records remain encrypted throughout the analytics process, ensuring confidentiality even in untrusted cloud environments. After computation, encrypted results are returned to authorized users, who decrypt them locally. This method reduces data exposure risks and strengthens privacy protection.

REQUIREMENTS ENGINEERING

The proposed secure and privacy-preserving analytics framework is designed to integrate multi-tenant cloud computing with blockchain-based verification to enable protected healthcare data processing. The system incorporates advanced cryptographic mechanisms, including zero-knowledge proofs (zk-SNARKs), homomorphic encryption, and SHA-256 hashing, to safeguard sensitive patient information throughout the analytics lifecycle. These components collectively support encrypted computation, decentralized verification, tamper-proof storage, and integrity validation across healthcare transactions. By ensuring that raw medical data is never exposed during processing, the framework delivers scalable, transparent, and policy-compliant analytics suitable for telemedicine applications and distributed healthcare environments.

The hardware requirements define the computing infrastructure necessary for implementing and executing the proposed system efficiently. These requirements ensure that the cryptographic operations, blockchain processing, and cloud-based analytics perform smoothly. The system requires a minimum configuration consisting of an Intel Core i3 processor or higher, 4 GB DDR4 RAM, and at least 100 GB of storage capacity. A standard 15.6-inch LED monitor is sufficient for user interaction, while basic peripherals such as a keyboard and mouse are required. A webcam may optionally be included to support authentication features. These specifications provide a balanced environment for development, testing, and deployment of the framework.

The software requirements describe the platform dependencies required for system development and operation. The proposed system uses Java EE technologies, including JSP and Servlets, for the front-end interface, while Maven is used for project management and build automation. The backend database is implemented using MySQL version 5.5 or higher to manage user data and metadata. The system is designed to operate on Windows 10 or Windows 11 environments, with Apache Tomcat 9.0 serving as the web server. The application supports modern browsers such as Google Chrome and Mozilla Firefox for user interaction. Development is carried out using Eclipse IDE or IntelliJ IDEA, which provide efficient coding, debugging, and deployment capabilities.

The functional requirements define the operations performed by each module of the system. The blockchain module is responsible for secure storage and verification of healthcare transactions. When encrypted medical data is uploaded, the system creates a blockchain transaction, generates metadata, and stores the information in an immutable ledger. Authorized users can view healthcare transactions and access prescription or report references through validated block identifiers. This module ensures transparency and prevents unauthorized modifications.

DESIGN ENGINEERING

Design engineering focuses on defining the structural and behavioral aspects of a system using Unified Modeling Language (UML) diagrams. These diagrams provide a conceptual blueprint that helps visualize system functionality, specify relationships among components, and document interactions during development. In this project, design engineering is applied to model the communication between actors, system modules, encryption mechanisms, and secure data flow.

The proposed system, titled *Secure and Private Analytics of Healthcare Records in Multi-Tenant Cloud Environments Using Blockchain*, integrates multiple modules that collaboratively collect, encrypt, store, and analyze healthcare data. UML diagrams are employed to represent these interactions clearly:

- **Use Case Diagrams** illustrate interactions between actors such as Patient, Doctor, Authority, Pharmacy, and Insurers. These interactions include registration, authentication, report upload, encrypted data processing, analytics execution, prescription generation, insurance claims, and blockchain-based verification.
- **Class Diagrams** define the structural components including Patient, Doctor, Medical Record, Blockchain, zk-SNARKs module, Homomorphic Encryption module, SHA-256 hashing unit, Smart

Contract, Cloud Storage, Prescription, and Insurance Claim.

- **Sequence Diagrams** describe step-wise communication. For instance, a patient uploads medical data, the encryption module secures the information, analytics are performed on encrypted data, zk-SNARKs generate verification proofs, blockchain validates results, and doctors access verified outcomes.
- **Activity Diagrams** represent workflows such as authentication, encrypted upload, privacy-preserving computation, blockchain validation, prescription creation, and claim processing.
- **Component Diagrams** show system modules including interfaces for patients and doctors, analytics engine, encryption modules, blockchain services, and cloud storage.

Use Case Diagram – Explanation

The use case diagram illustrates the interactions among five primary actors: Patient, Doctor, Authority, Pharmacy, and Insurers. Patients register, log in, upload medical records, request consultations, access prescriptions, and initiate insurance claims. Doctors, after approval by the authority, review patient data, provide medical advice, and generate prescriptions. The authority validates both patient and doctor registrations to maintain trust within the system.

Pharmacies access prescriptions, update medication status, and communicate details to patients. Insurers verify submitted claims using prescription and treatment information. All healthcare data is protected using cryptographic mechanisms, and blockchain technology ensures immutability and transparency. Role-based access control restricts operations to authorized users, enabling secure collaboration among stakeholders.

Class Diagram – Explanation

The class diagram defines the structural relationships among Doctor, Patient, Pharmacy, Authority, Insurers, and Database entities. The Doctor class includes operations such as registration, login, viewing reports, and sharing prescriptions. The Patient class supports functionalities including registration, login, uploading reports, viewing prescriptions, and submitting insurance claims.

The Pharmacy class handles prescription viewing and updates, while the Authority class manages approvals and authentication. The Insurers class validates insurance claims. The Database class stores system records and user data. These interconnected classes facilitate secure communication and controlled data access, ensuring modularity and data confidentiality.

Object Diagram – Explanation

The object diagram provides a runtime snapshot of system entities interacting within the blockchain-based healthcare environment. Instances of Doctor, Patient, Authority, Pharmacy, Insurers, and Database collaborate to perform system operations. The patient uploads records to the database, which are reviewed by the doctor. The authority validates entities, pharmacies update prescription details, and insurers verify claims. The database acts as a centralized repository ensuring data consistency. This representation highlights real-time collaboration among objects while maintaining secure communication.

State Chart Diagram – Explanation

The state chart diagram describes the dynamic behavior of system modules. The process begins with user authentication. Patients then submit consultation requests and upload reports. These reports transition into storage states within the database. Doctors review reports and generate prescriptions. The authority supervises approval states, pharmacies update prescription details, and patients submit insurance claims. Insurers validate claims before final storage. Each transition ensures secure, role-based access and maintains data integrity.

Component Diagram – Explanation

The component diagram presents system modules and their dependencies. The Doctor and Patient components include submodules for registration, authentication, report management, and prescription handling. The database component stores all system information. Independent modules communicate with shared services, ensuring scalability and maintainability.

E-R Diagram – Explanation

The entity-relationship diagram represents database structure and relationships among Doctor, Patient, Authority, Pharmacy, and Insurers. Entities store relevant attributes such as identification details, medical records, prescriptions, and insurance claims. Relationships define interactions including treatment, report upload, prescription generation, and claim verification. This design minimizes redundancy and supports efficient data management.

Data Flow Diagram – Explanation

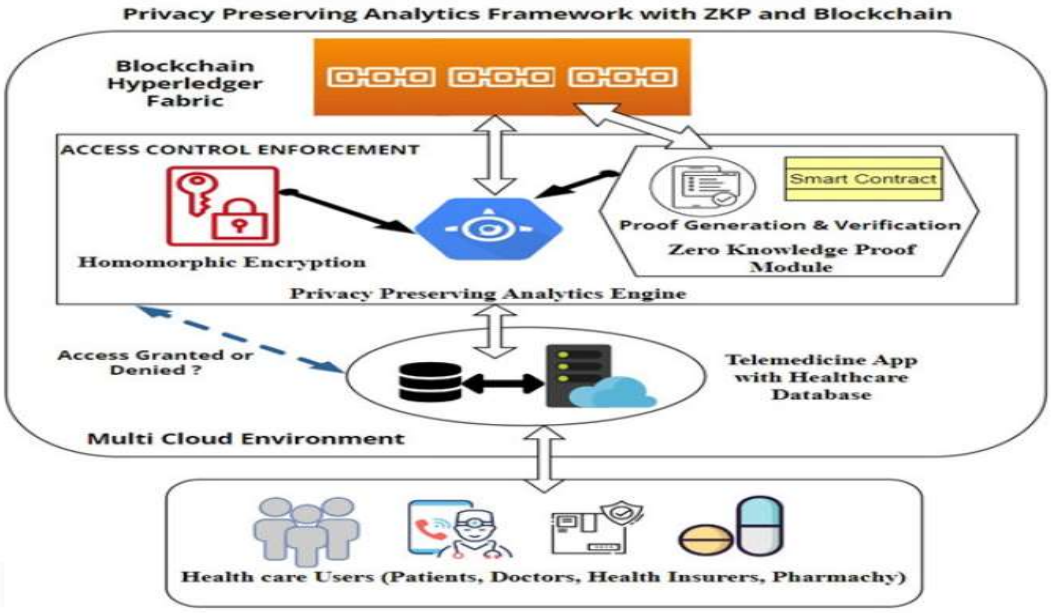
The data flow diagram illustrates secure information exchange among system modules. Patients upload reports, doctors analyze them, pharmacies update prescriptions, and insurers verify claims. The database manages storage and retrieval. Role-based access ensures confidentiality and integrity throughout the process.

Deployment Diagram – Explanation

The deployment diagram depicts physical distribution of system components. Patient devices provide user interfaces for uploading encrypted data. Doctor systems access verified information and generate prescriptions. Authority servers validate registrations. Blockchain-IPFS nodes maintain immutable records. Cloud storage provides backup and redundancy. Security modules including

homomorphic encryption, SHA-256 hashing, and zk-SNARKs ensure privacy and verification. Secure communication channels connect all nodes, forming a scalable healthcare infrastructure.

System Architecture



The system architecture is designed to support secure healthcare data management across multiple stakeholders. It integrates blockchain, zk-SNARKs, homomorphic encryption, and SHA-256 hashing to ensure confidentiality, integrity, and verifiable computation. The patient layer handles registration and encrypted uploads, while the doctor layer manages report analysis and prescription generation. The authority layer validates actions, and pharmacy and insurer layers process prescriptions and claims. Sensitive data is encrypted prior to storage, and blockchain ensures immutability. zk-SNARKs enable verification without exposing private information. Cloud storage provides redundancy, and secure communication channels enable reliable data exchange. The architecture therefore delivers a scalable, privacy-preserving, and tamper-resistant healthcare ecosystem.

DEVELOPMENT TOOLS

This chapter describes the programming languages, frameworks, and software tools used to implement the proposed healthcare security system. The development platform selected for this project is Java due to its portability, security features, and strong support for distributed applications. The implementation primarily utilizes Java technologies including Core Java and J2EE components. J2EE is adopted for developing enterprise-level modules such as web interfaces, server-side processing, and database connectivity. These technologies collectively provide a scalable and secure environment for handling healthcare data within a multi-tenant cloud architecture.

Features of Java

Java Framework

Java is a high-level programming language introduced by James Gosling at Sun Microsystems in 1995. It derives much of its syntax from C and C++ while simplifying memory management and reducing low-level dependencies. Java programs are compiled into bytecode, which executes on the Java Virtual Machine (JVM), allowing applications to run on different hardware platforms without modification. This platform independence supports the principle of "write once, run anywhere."

Java is designed as a general-purpose, object-oriented, and concurrent language. Its architecture-neutral nature, built-in security model, and extensive libraries make it suitable for network-based applications. Java is widely used in enterprise systems, web applications, mobile devices, and cloud environments. The flexibility and portability of Java enable developers to build applications that operate efficiently across diverse platforms ranging from personal computers to distributed cloud infrastructures.

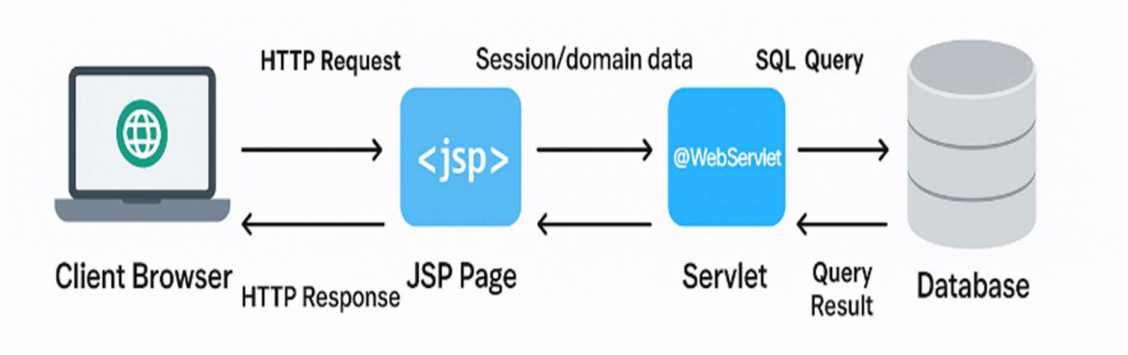
Apache Tomcat Server

Apache Tomcat is an open-source web server and servlet container used to deploy Java web applications. It supports Servlets, JSP, and HTTP protocols. Tomcat is lightweight compared to full Java EE servers and allows easy deployment of web applications. It integrates well with development

environments and is widely used for testing and production deployments.

Java provides a robust platform for developing secure and scalable applications. Its portability, object-oriented structure, and multithreading capabilities make it suitable for enterprise-level systems. The Java Database Connectivity (JDBC) API enables seamless interaction with relational databases, allowing applications to execute queries and manage data efficiently. Additionally, frameworks such as Hibernate support object-relational mapping, reducing manual database handling.

Java's strong exception handling, security mechanisms, and extensive libraries improve reliability and performance. The availability of web technologies such as Servlets, JSP, and Tomcat further enhances its suitability for distributed systems. Due to these features, Java serves as an effective development platform for implementing secure, database-driven healthcare applications.



SOFTWARE TESTING

Software testing is performed to identify defects and verify that the developed system satisfies specified requirements. It involves evaluating software components, subsystems, and the complete application to ensure that the product functions correctly and reliably. Testing helps determine whether the system behaves according to user expectations and prevents unacceptable failures during operation. Various testing approaches are applied, each targeting different aspects of functionality, performance, and integration.

Developing Methodologies

The testing process begins with the preparation of a structured test plan covering both general functionality and specialized features across multiple platform configurations. Standard quality assurance procedures are followed throughout the testing lifecycle. The objective is to confirm that the application complies with requirements defined in the system specification and operates without defects. Testing methodologies are designed to evaluate system performance, validate security mechanisms, and verify accurate interaction among modules.

Types of Tests

Unit Testing

Unit testing focuses on validating individual components of the application. Test cases are designed to verify that each module performs its intended function and produces expected outputs for given inputs. This testing approach examines internal logic, decision branches, and data flow within the code. Unit testing is conducted after completing each module and before integration with other components. It ensures that business logic and system configurations operate correctly, with clearly defined inputs and anticipated results.

Conclusion

The proposed framework for secure and privacy-preserving analytics of healthcare records in multi-tenant cloud environments demonstrates an effective approach for protecting sensitive medical information while enabling collaborative data analysis. By combining blockchain technology with zero-knowledge proof mechanisms, particularly zk-SNARKs, the system allows analytical computations to be verified without exposing raw patient data. This capability addresses major concerns related to privacy violations, unauthorized access, and data leakage in modern healthcare infrastructures.

The utilization of a multi-tenant cloud environment improves scalability and optimizes resource utilization, enabling multiple healthcare stakeholders to perform secure analytics concurrently. Blockchain integration provides an immutable and transparent ledger for storing verification proofs, ensuring data integrity, traceability, and trust among participants. This feature is particularly valuable in distributed healthcare services such as telemedicine, where secure information sharing is critical.

The architecture supports structured interactions among stakeholders including patients, doctors, pharmacies, insurers, and trusted authorities. The modular design enhances flexibility and allows secure computation across decentralized entities. Experimental evaluation indicates that the system

maintains strong security guarantees while handling anonymized datasets efficiently at scale. Furthermore, the integration of cryptographic techniques with decentralized storage improves reliability and auditability.

Overall, the proposed framework contributes to the advancement of privacy-preserving healthcare analytics by integrating cryptographic validation with decentralized cloud infrastructure. The approach establishes a foundation for future healthcare ecosystems that emphasize data confidentiality, interoperability, and transparency. Additionally, the framework can be extended to support emerging technologies such as artificial intelligence-based diagnostics, edge computing, and advanced zero-knowledge proof systems, thereby enabling next-generation secure healthcare platforms.

References

[1] H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, "A blockchain-based scheme for privacy-preserving and secure sharing of medical data," *Computer Security*, vol. 99, Dec. 2020.

[2] G. Xu et al., "A privacy-preserving medical data sharing scheme based on blockchain," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 698–709, Feb. 2023.

[3] Y. Piao, K. Ye, and X. Cui, "A data sharing scheme for GDPR compliance based on consortium blockchain," *Future Internet*, vol. 13, no. 8, Aug. 2021.

[4] R. Benaich, S. El Mendili, and Y. Gahi, "Advancing healthcare security using zero-trust blockchain solutions," *HighTech Innovation Journal*, vol. 4, no. 3, pp. 630–652, Sep. 2023.

[5] B. Sharma, R. Halder, and J. Singh, "Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption," in *Proc. COMSNETS*, Jan. 2020.

[6] L. Liu et al., "Dual blockchain-based data sharing mechanism with privacy protection for medical IoT," *Heliyon*, vol. 10, Jan. 2024.

[7] T. Bai et al., "Health-zkIDM: A healthcare identity system based on blockchain and zero-knowledge proof," *Sensors*, vol. 22, no. 20, Oct. 2022.

[8] A. Diro et al., "Leveraging zero-knowledge proofs for blockchain-based identity sharing," *Journal of Information Security and Applications*, vol. 80, Feb. 2024.

[9] X. Shang et al., "Newton-interpolation-based zk-SNARK for artificial Internet of Things," *Ad Hoc Networks*, vol. 123, Dec. 2021.

[10] R. Zhang, R. Xue, and L. Liu, "Security and privacy for healthcare blockchains," *IEEE Transactions on Services Computing*, vol. 15, no. 6, Nov. 2022.

[11] R. Shinde et al., "Securing AI-based healthcare systems using blockchain technology," *Transactions on Emerging Telecommunications Technologies*, vol. 35, 2023.

[12] G. S. Gaba et al., "Zero-knowledge proof-based authenticated key agreement protocol for healthcare," *Sustainable Cities and Society*, vol. 80, May 2022.

[13] J. Scheibner, M. Ienca, and E. Vayena, "Health data privacy through homomorphic encryption and distributed ledger computing," *BMC Medical Ethics*, vol. 23, 2022.

[14] O. Kocabas et al., "Assessment of cloud-based health monitoring using homomorphic encryption," in *Proc. IEEE ICCD*, 2013.

[15] K. Sinha, P. Majumder, and S. K. Ghosh, "Fully homomorphic encryption-based privacy-preserving computation," in *Proc. IEEE ANTS*, 2020.

[16] B. Wang et al., "Privacy-preserving federated learning with homomorphic encryption," *Applied Soft Computing*, vol. 146, Oct. 2023.

[17] X. Dong, D. Randolph, and C. Weng, "Secure multi-party computation protocols in healthcare," *AMIA Joint Summits*, 2021.

[18] A. V. Kumar et al., "Secure multiparty computation enabled e-healthcare system," *IOP Conference Series*, 2020.

[19] U. Kose et al., *Interpretable Cognitive Internet of Things for Healthcare*, Springer, 2023.

[20] P. Jangde and D. K. Mishra, "Secure multiparty computation solution to healthcare frauds," in *Proc. ISMS*, 2011.

[21] S. Vijayalakshmi, "Attribute-based encryption in healthcare applications," in *Proc. ICACRS*, 2022.

[22] H. Wang et al., "Ciphertext-policy attribute-based encryption for smart health," *Computer Standards & Interfaces*, vol. 84, Mar. 2023.

[23] S. Roy et al., "Multi-authority hierarchical attribute-based encryption for secure EHR sharing," *Cluster Computing*, vol. 27, 2024.

[24] N. Ni and Y. Zhu, "Accelerating zk-SNARK kernels on GPU," *Journal of Parallel and Distributed Computing*, vol. 173, Mar. 2023.

[25] K. Zala et al., "Enhanced anonymity model for privacy protection in e-health," *Social Network Computing Sciences*, vol. 5, 2024.

[26] A. Sharma, S. Kaur, and M. Singh, "Review on blockchain and IoT in healthcare," *Transactions on Emerging Telecommunications Technologies*, vol. 32, 2021.