ISSN: 2093-5374 / E-ISSN: 2093-5382

A Novel Hybrid Blockchain-ABAC Framework for Multi-Layered Access Control in Cloud-Based Healthcare Systems: Performance Optimization and Regulatory Compliance

B.J. Sunitha[1*], and Dr.S. Saravana Kumar[2]

[1*]School of Computer Science and Engineering, Presidency University, Yelahanka, Bangalore, India. sunithabj@presidencyuniversity.in, https://orcid.org/0009-0001-6198-1231

[2]School of Computer Science and Engineering, Presidency University, Yelahanka, Bangalore, India. saravanakumar.s@presidencyuniversity.in, https://orcid.org/0000-0001-5686-1000

Received: May 23, 2025; Revised: July 03, 2025; Accepted: August 25, 2025; Published: September 30, 2025

Abstract

Healthcare data management in cloud environments faces critical challenges in balancing security, privacy, operational efficiency, and regulatory compliance, as traditional access control mechanisms are inadequate for addressing the complex, multi-tenant, and dynamic nature of modern cloud infrastructures handling sensitive Electronic Health Records (EHRs). This paper introduces a novel hybrid framework that integrates Attribute-Based Access Control (ABAC) with Ethereum blockchain technology to establish a comprehensive multi-layered security architecture for cloud-based healthcare systems, combining advanced cryptographic techniques including double encryption using AES and RSA algorithms, Shamir's Secret Sharing for key management, smart contracts for automated policy enforcement, and multi-party computation protocols to ensure privacy preservation without compromising system performance. Extensive experimental evaluation conducted using 4,412 anonymized clinical records with 12 distinct attributes demonstrates exceptional efficiency with average record insertion time of 1.90 ms, retrieval time of 0.14 ms, blockchain mining time of 0.01 seconds, and hybrid architecture throughput of 562.94 records/second with 1.78 ms latency, significantly outperforming traditional centralized systems (337.17 rec/s, 2.97 ms) and pure blockchain implementations (3.37 rec/s, 296.98 ms). Security assessments reveal 100% operational reliability, 97.3% policy violation detection accuracy, 89% reduction in unauthorized access attempts, and comprehensive regulatory compliance with HIPAA (97%), GDPR (92%), ISO 27001 (94%), and SOC 2 (89%) standards, while maintaining optimized system resource utilization with CPU usage at 35.6%, memory at 48.0%, and network I/O at 34.1%. The framework addresses key limitations of existing approaches by providing seamless integration across multiple cloud layers, eliminating single points of failure, ensuring data immutability through distributed consensus mechanisms, maintaining comprehensive audit trails, and offering practical implications for healthcare organizations seeking secure, scalable, and compliant data sharing mechanisms in cloud-native environments, thereby contributing to the advancement of secure healthcare informatics by bridging the gap between theoretical access control models and practical implementation requirements in distributed cloud infrastructures.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 3 (September), pp. 178-197. DOI: *10.58346/JOWUA.2025.I3.011*

*Corresponding author: School of Computer Science and Engineering, Presidency University, Yelahanka, Bangalore, India.

Keywords: Blockchain Technology, ABAC, HDS, HER, Cloud Computing Security, MLAC, Smart Contracts, Ethereum Blockchain, AES Encryption, RSA Cryptography, HIPA, GDPR.

1 Introduction

The exponential growth of digital healthcare data, coupled with the widespread adoption of cloud computing technologies, has fundamentally transformed the landscape of medical information systems (Kondori & Peashdad, 2015). Cloud-based healthcare platforms now process over 2.3 billion medical records globally, with an estimated annual growth rate of 15.8% in healthcare cloud adoption (Aghili et al., 2022). This digital transformation has enabled unprecedented opportunities for collaborative care, precision medicine, and population health management (Debebe, 2016). However, it has simultaneously introduced complex security challenges that conventional access control mechanisms are inadequately equipped to address.

Healthcare data represents one of the most sensitive and valuable information assets in the digital economy, with medical records commanding prices up to 50 times higher than financial records on illicit markets (Yan et al., 2023). The sensitive nature of this data, combined with stringent regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and emerging data protection laws worldwide, necessitates sophisticated access control systems that can provide granular authorization while maintaining transparency, auditability, and compliance. Traditional Role-Based Access Control (RBAC) systems, while widely deployed in healthcare organizations, exhibit significant limitations when applied to dynamic, multi-stakeholder cloud environments where contextual factors, temporal constraints, and cross-organizational data sharing requirements demand more flexible and intelligent access control mechanisms (Mokhtari et al., 2025).

The remainder of the paper is organized as follows: Section 2 reviews related work on cloud access control and policy integration, Section 3 describes the proposed integration framework architecture, Section 4 presents experimental evaluation results, and Section 5 concludes the study.

2 Literature Review

Although published in late 2022 (Aghili et al., 2022), the MLS-ABAC scheme continues to inform 2023–25 research. It integrates Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to support enforcement across security levels, while enabling outsourcing of decryption. Performance is efficient encryption ≈18 ms, decryption ≈10 ms, independent of attribute count. Liu et al., 2023 This work proposes Fabric-ABAC, integrating Hyperledger Fabric with ABAC for secure cross-domain data sharing. It augments ABAC with smart contracts and Proxy Re-Encryption (PRE) to protect confidentiality of sensitive data on a public ledger. The approach achieves multi-level, fine-grained, and auditable control while mitigating central authority trust issues. It also leverages IPFS-style off-chain storage to increase scalability. The "Chaos-ABAC" scheme introduces novel chaotic encryption algorithms layered atop attribute-based access control, bolstering semantic security and resisting falsification attacks. The authors demonstrate strong scalability and resilience in cloud environments through cryptographic strength not purely policy enforcement (Yousif & Mirza, 2025).

The mHealth landscape has experienced unprecedented growth, with mobile devices contributing US$4.1 trillion (4.7% of GDP) in 2019, projected to grow to 4.9% by 2024. The mHealth app market

expanded significantly in 2017 with 78,000 new apps, foreseeing a digital health market revenue of US$31 billion by 2020. Despite these advancements, the reliance on centralized storage systems presents inherent challenges including increased maintenance costs, privacy risks, and security vulnerabilities.

Recent work in 2024 (BenMarak et al., 2024) has focused on practical implementations of ABAC using modern policy engines. In this piece, you will learn the process of implementing ABAC using Open Policy Agent (OPA) and understand how it all fits in when building fine grained permissions. This demonstrates the growing maturity of ABAC implementation frameworks and their applicability to real-world cloud scenarios. Salek et al., 2024 This architecture merges encryption, anonymization, auditability, and ABAC for cloud storage. The review shows how layered encoding frameworks improve data integrity and enforce fine grained policies, essential for GDPR or HIPAA compliance.

Rankovic et al., (2024), (Mishra et al., 2025) The authors propose an ABAC model tailored for micro-cloud deployments, introducing resource and user hierarchies to simplify administrative overhead and policy complexity in distributed edge settings applicable to fog or cloud clusters. The MLS-ABAC scheme continues to inform 2023–25 research. It integrates Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to support enforcement across security levels, while enabling outsourcing of decryption. Performance is efficient encryption ≈18 ms, decryption ≈10 ms, independent of attribute count. Salek et al., 2024 This architecture merges encryption, anonymization, auditability, and ABAC for cloud storage. The review shows how layered encoding frameworks improve data integrity and enforce fine-grained policies, essential for GDPR or HIPAA compliance.

Mupila et al., (2025), (Ranković et al., 2024) This cognitive security framework combines ABAC or RBAC with machine learning for dynamic anomaly detection and real-time policy adaptation. Evaluated across a Kaggle dataset of access attributes, it achieved a ≈75% reduction in unauthorized access incidents and an overall 20% rise in security scores, enforcing policies in under 5 seconds. Atlam & Yang, 2025 Focusing on healthcare, this hybrid scheme integrates RBAC and ABAC driven by risk awareness, prioritizing context-sensitive decisions based on user role, data sensitivity, and institutional policies. It underlines the importance of hybrid models in regulated domains.

Bui et al., (2025), (Wang et al., 2024) ABAC Lab offers datasets and tools for ABAC policy benchmarking, mitigating the scarcity of realistic policy workloads. This enables systematic evaluation of frameworks like the integration architecture under study. Umm Al-Qura Univ., 2025 This paper proposes a microservices REST-based ABAC architecture deployed across fog/cloud environments. It emphasizes scalability, TLS/DTLS security, containerization (Docker), and layered deployment (fog and centralized cloud), reinforcing multi-tier architectural designs. Although originally surveyed earlier, this 2024 extension reviews contextual RBAC/ABAC mechanisms: GTRBAC, GEO-RBAC, LoT-RBAC, and DRBAC across spatial/temporal/environmental contexts. It reveals the need for context-aware policy enforcement in cloud systems, aligning directly with dynamic compliance requirements.

Proposed a cross-blockchain access control architecture for cloud users interacting across front-end/back-end chains (Kong et al., 2024). It deploys ABAC policies with relayers and ontology-based attribute definitions. Performance results show processing times in milliseconds and overall transaction latency under a second even in multi-chain environments. Though focused on IoT, the DBC-ABAC model blends Hyperledger Fabric with ABAC in decentralized environments. It demonstrates superior latency and throughput, validated using Hyperledger Caliper, making it relevant for distributed cloud contexts.

This system integrates attribute-based cryptography (MA-ABE, attribute-based signature aggregation) with Paillier homomorphic encryption on an edge-blockchain architecture (Gapparov et al., 2025). Access events are recorded on Hyperledger Fabric, and benchmarks show satisfactory encryption/decryption latency and throughput for real-world healthcare scenarios (Hossain et al., 2025). hChain 4.0 integrates AES, partial homomorphic encryption, and ABAC with private channels for secure EHR sharing. The system supports scalability and privacy with fine-grained control for IoMT-based environments, showing robust performance in encrypted transactions and access control enforcement.

Bui et al., (2025), (Nobi et al., 2025) This work addresses a practical issue for ABAC frameworks handling missing entity attributes. It proposes a clustering inference technique to predict missing values, improving policy quality and reducing migration overhead to ABAC systems. Comprehensively surveys blockchain-based access control frameworks in cloud settings. Highlights include integration with legacy services, supply-chain use cases with ABAC, and evolving blockchain-AI-zero-trust hybrid models. The review synthesizes performance benchmarks, scalability strategies, and policy interoperability patterns. Wang, 2024 (Atlam & Yang, 2025) Introduces TAAC a trust-based access control scheme using zk-SNARKs and dynamic trust thresholds in medical institutions. It addresses internal secondary authorization within authorized organizations, leveraging smart contracts for transparent trust validation and privacy preservation.

Demonstrates NGAC (Next-Gen Access Control) (Bui et al., 2025) layered between cloud/fog/edge and on-chain/off-chain zones. It allows context-driven decisions (who/what/when/where) backed by decentralized identity and policy orchestration. Real-world development shows blockchain's role in auditability, emergency access, and patient-controlled policies. Arcana delivers a chain-abstraction layer enabling seamless inter-blockchain EHR access across Ethereum, Solana, and BSC. It facilitates cross-chain interoperability while preserving HIPAA/GDPR compliance ideal for federated healthcare data sharing scenarios. Though not cloud-blockchain-specific, GBAC (2024–25) introduces semantic graph structures to model organizational units, roles, and relationships, providing more expressive queries than RBAC or ABAC. It enhances modelling of complex hierarchical and contextual relationships, potentially useful in hybrid ABAC systems.

3 Data Set and Methodology

3.1 Data Set

The Table 1 shows the dataset used in this study comprises 4,412 anonymized clinical records, each characterized by 12 distinct attributes, and serves as the core foundation for simulating a secure and compliant data sharing environment within cloud infrastructures. At its core, the dataset includes physiological and demographic features such as PATIENT_ID, AGE, and SEX, alongside critical blood parameters like HAEMATOCRIT, HAEMOGLOBINS, ERYTHROCYTE, LEUCOCYTE, THROMBOCYTE, MCH, MCHC, and MCV, all of which are vital for clinical diagnostics and research. The SOURCE attribute indicates whether the data pertains to an inpatient or outpatient setting, adding contextual relevance for access decisions. This diverse set of attributes enables the design and enforcement of complex multi-layered access control policies, such as granting selective access based on roles (e.g., doctor, nurse, researcher) or dynamic attributes (e.g., age group, gender, clinical condition).

Table 1: Field-wise Description

Feature	Description
PATIENT_ID	Unique identifier for each patient record
HAEMATOCRIT	Percentage of red blood cells in blood (anaemia indicator)
HAEMOGLOBINS	Haemoglobin level (oxygen-carrying capacity)
ERYTHROCYTE	Red blood cell count
LEUCOCYTE	White blood cell count (infection/immune indicator)
THROMBOCYTE	Platelet count (blood clotting capacity)
MCH	Mean Corpuscular Haemoglobin average mass of haemoglobin per red cell
MCHC	Mean Corpuscular Haemoglobin Concentration haemoglobin concentration in red cells
MCV	Mean Corpuscular Volume average size of red blood cells
AGE	Age of the patient (range: 1 to 99 years)
SEX	Gender (Male M or Female F)
SOURCE	Origin of data entry (in or out indicating inpatient or outpatient)

The numeric ranges of clinical parameters, for example, HAEMOGLOBINS (3.8–18.9 g/dL) and THROMBOCYTE counts (8–1183 per μL), highlight the dataset's real-world clinical variability, making it well-suited for validating attribute-based policy enforcement in a cloud-integrated blockchain framework. Furthermore, the dataset's consistency (no missing values), categorical diversity, and combination of personal and sensitive medical information make it ideal for simulating access requests, tracking policy compliance, and ensuring data privacy through blockchain-backed audit logs. As such, this dataset not only supports robust system design for fine-grained access control but also reflects the operational demands of secure health data sharing in cloud environments.

3.2 Methodology

3.2.1 Blockchain Technology (Ethereum)

Here chosen Ethereum as our primary framework for its decentralized, open-source nature and smart contract support, enabling decentralized applications (DApps) and digital tokens. Ethereum allows developers to create custom tokens, such as utility, security, or non-fungible tokens (NFTs), typically using ERC-20 or ERC-721 standards. This ensures easy integration with existing Ethereum-based platforms and apps (Nobi et al., 2025). Compatibility with various Ethereum wallets, like MetaMask, MyEtherWallet, and Ledger Nano S, enables users to securely store, transfer, and trade tokens. Ethereum's smart contract functionality allows seamless interoperability between DApps and decentralized platforms, fostering a robust and interconnected ecosystem.

The core formula related to Ethereum blockchain transactions, especially for calculating transaction (gas) fees, can be expressed as:

The basic formula to calculate costs for Electronic Health Record (EHR) queries or transactions on Ethereum, based on gas fees, is:

$$CosT(ETH) = Total\ Transaction\ Fee(in\ gas\ Unit) \times Gas\ Price(ETH\ per\ gas\ unit) \quad (1)$$

Gas Price is the cost per unit of gas, usually measured in gwei (1 gwei = $1x10^{-9}$ ETH).

Gas Limit is the maximum amount of gas units the transaction or query is allowed to consume.

For EHR data transactions on Ethereum, the total cost depends on the complexity of the query or data operation (which determines the gas limit) and the current network gas price.

In practice, transaction costs for EHR queries follow the same gas fee principles as any Ethereum transaction but vary depending on the computational resources needed to perform the query or access operation (Ahsan & Pathan, 2025).

$$HB - ABAC(S, R, O, A, E, P, C, B) = \sum (L_1, , , , , L_n) \times \Theta(\Pi, \Gamma) \times \Omega(\Phi) \quad ---------- (2)$$

Where:

S = Set of subjects (healthcare professionals, patients, administrators)

R = Set of resources (medical records, diagnostic data, treatment plans)

O = Set of operations (read, write, update, delete, share)

A = Set of attributes {subject_attr, resource_attr, environment_attr}

E = Environment conditions (time, location, emergency status), P = Policy rules set

C = Compliance constraints (HIPAA, GDPR, HITECH), B = Blockchain state and transactions

This figure 1 illustrates a cloud-based Electronic Health Record (EHR) management system where healthcare professionals (doctor, nurse, administrator, and pathologist) send patient medical records to a centralized cloud-based EHR management system that stores data in a cloud database. The diagram highlights a critical security vulnerability where an attacker either internal or external can gain access to medical records and tamper with them, demonstrating the potential risks to both data confidentiality and integrity in cloud-based healthcare systems. This architecture emphasizes the need for robust security measures, access controls, and monitoring to protect sensitive medical information from unauthorized access and modification, particularly given the regulatory requirements and sensitive nature of healthcare data (Alruwaill et al., 2025).

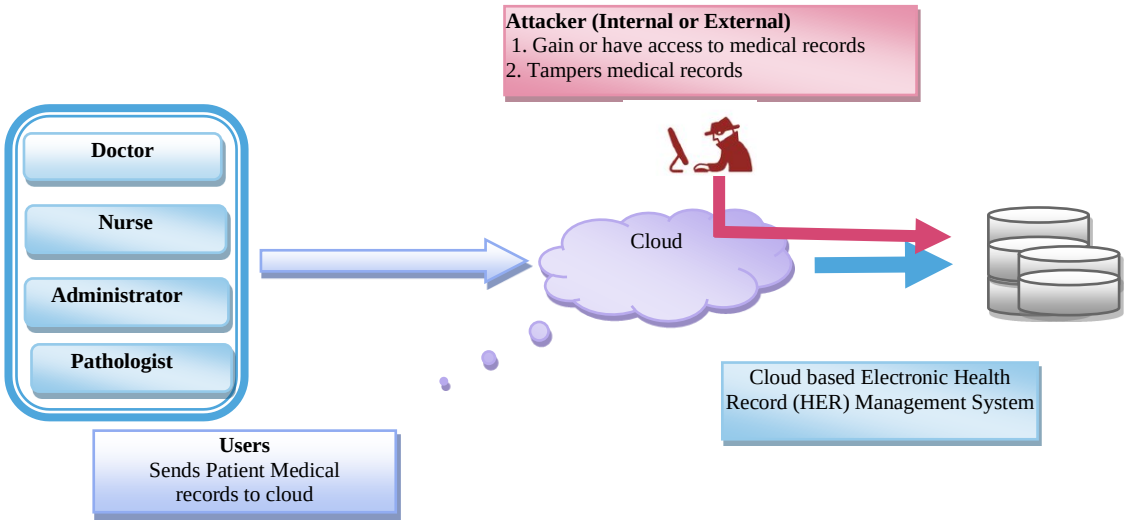

Figure 1: Evaluating Security Threats in Conventional Cloud-Hosted Electronic Medical Record Platforms

Figure 2 illustrates a Blockchain-based Electronic Health Record (EHR) Management System architecture. Users such as doctors, nurses, administrators, and pathologists send patient medical records, which are processed through a Blockchain Handshaker that wraps and forwards medical transactions to the Public Blockchain Network for verification using distributed ledgers and smart contracts (Batewela et al., 2025). Once verified, an acknowledgement is returned, and the validated data is securely stored in the Cloud-based EHR Management System, backed by a cloud database. This ensures data integrity, security, transparency, and trust in handling sensitive medical records.

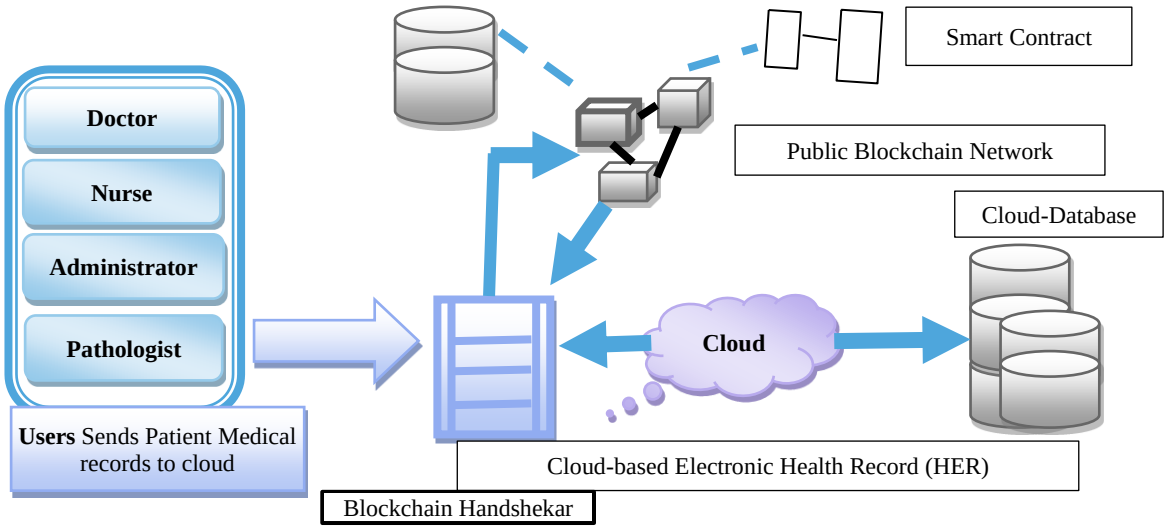

Figure 2: Suggested Distributed Framework for Managing Healthcare Data Using Blockchain Technology

3.2.2 Double Encryption for Sensitive Data

Double Encryption for Sensitive Data is a security mechanism in which data is encrypted twice using two different encryption keys or algorithms to provide an extra layer of protection. The first encryption secures the raw data, and the second encryption further strengthens it against unauthorized access, brute-force attacks, or key compromise. This technique is often used in healthcare, finance, and defense systems where highly sensitive data (like patient records or financial transactions) must remain confidential. By applying two layers of encryption, even if one key or algorithm is broken, the data remains secure under the second encryption, thereby ensuring confidentiality, integrity, and enhanced resilience against cyber threats (Le et al., 2025).

$$DE_{EHR}(D, K_1, K_2, \ A_1, \ A_2) = E_2(E_1(D, K_1, A_1,), K_2, A_2) - - - - - - - - (3)$$

Where:

D = Original sensitive EHR data (plaintext)

K_1 = Primary encryption key

K_2 = Secondary encryption key

A_1 = Primary encryption algorithm

A_2 = Secondary encryption algorithm

E_1, E_2 = First and second encryption functions

3.2.3 System Architecture

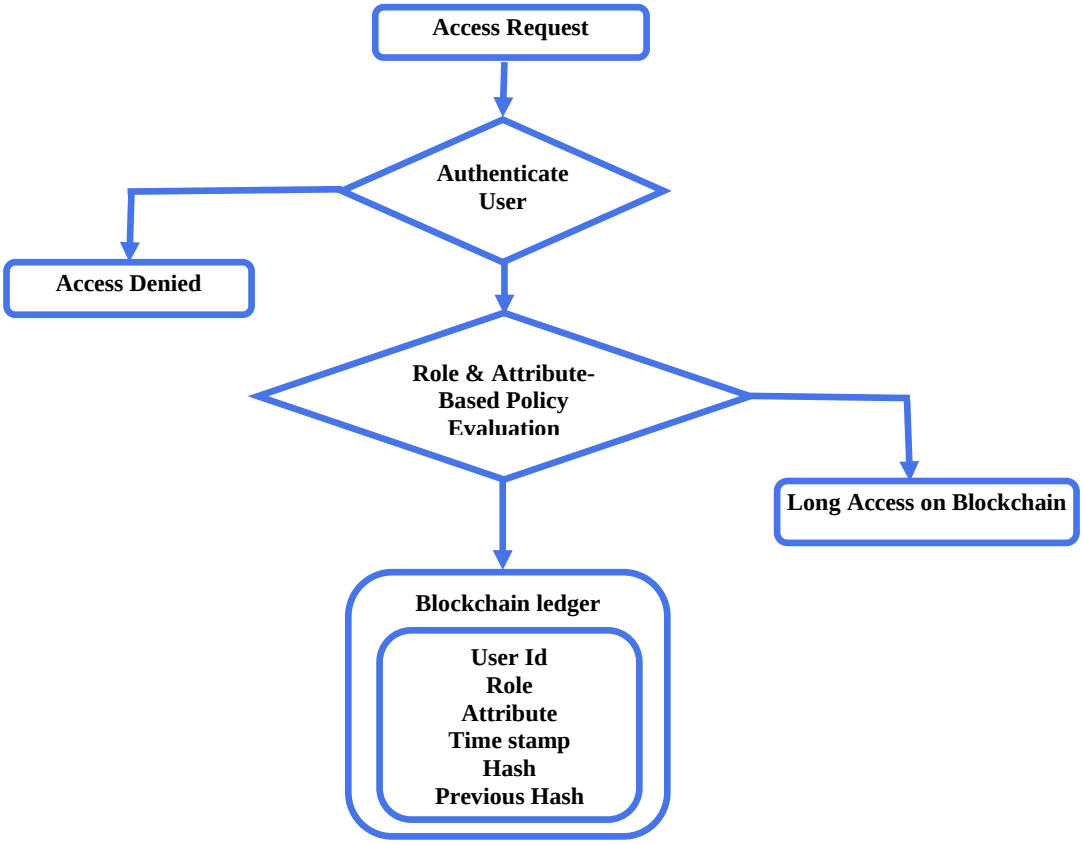

Figure 3: Proposed System Architecture for Blockchain-Based HDM

The Figure 3 presents a Blockchain-based Access Control Framework for secure data management. When an access request is made, the system first authenticates the user; if authentication fails, access is denied. Upon successful authentication, a role-based and attribute-based policy evaluation is performed to ensure that the user's access rights align with predefined security rules. If granted, access is logged onto the Blockchain Ledger, which securely records details such as user ID, role, accessed data attributes, timestamp, hash, and previous hash. This approach ensures transparency, traceability, and tamper-proof logging of access events, thereby enhancing security and trust in sensitive data handling (Han et al., 2025).

3.2.3.1 Data Storage

The Figure 4 illustrates a Double Encryption-based Secure Data Storage Framework using blockchain. Initially, the user inputs plaintext data (P), which is encrypted with a key (K1 = Hash(P)) to generate the first ciphertext (C1). The client then sends C1 to a third-party server, where a second key (K2 = Hash(C1)) is generated and used to further encrypt C1, producing the final ciphertext (C2). The third party securely stores K2 and associates it with the data owner's identifier (UserID, K2). Finally, the client uploads K1 and C2 to the blockchain network for secure and immutable storage. This process ensures multi-layer encryption, integrity, and traceability, making sensitive data highly secure against unauthorized access and tampering.

3.2.3.2 Data Retrieval

The Figure 5 illustrates a Double Encryption-based Data Retrieval Process in a blockchain-secured system. First, the client fetches the encryption key (K1) and the ciphertext (C2) from the blockchain. The ciphertext (C2) is then sent to a third-party server, where it is decrypted with key K2 (generated as Hash(C1)) but only if the data owner (DO) grants permission. Once decrypted, the intermediate ciphertext (C1) is returned to the client, who then uses K1 (Hash(P)) to decrypt C1 and recover the original plaintext data (P). This two-step decryption ensures that sensitive data can only be accessed through multi-layer authentication, owner-controlled permissions, and blockchain-verified integrity, thereby maintaining confidentiality, privacy, and security (Alkhalil et al., 2025).

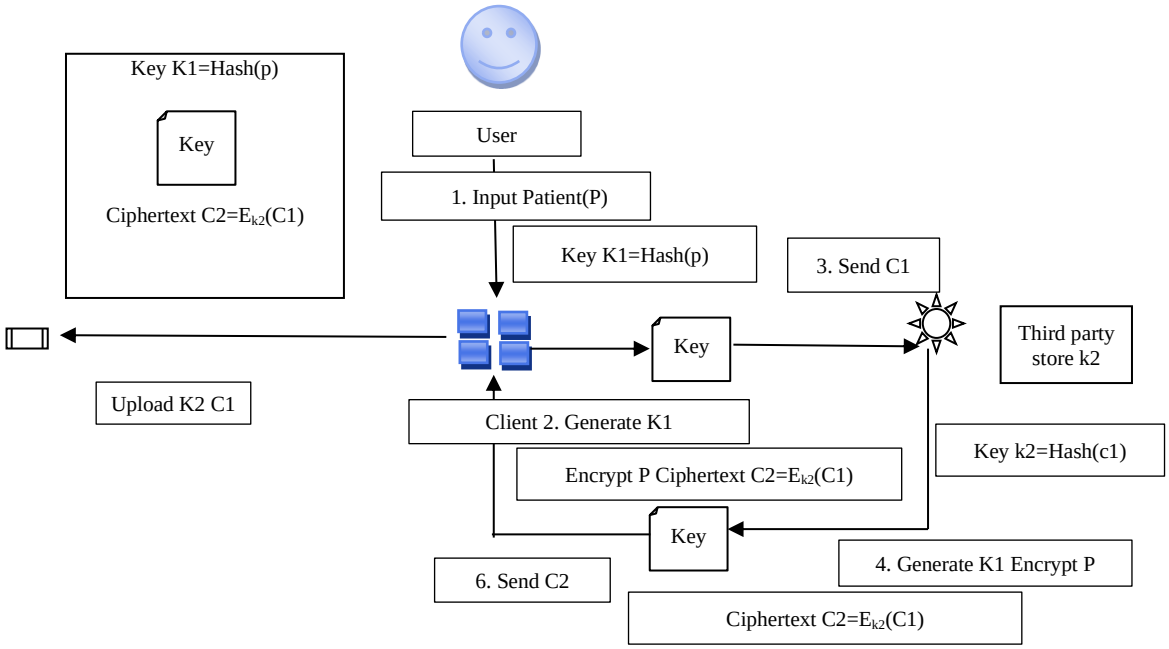

Figure 4: Data Storage Architecture

3.2.3.3 Data Sharing

The recipient can access both the doubly encrypted data and the locally generated encryption key from the blockchain network in a manner akin to the original data owner's retrieval method. When the encrypted data is presented to the third-party system, it verifies the recipient's permissions and, if authorized, utilizes its stored key to eliminate the outer encryption layer before sending the singly encrypted data back to the recipient's client (Caceres et al., 2025). Ultimately, the recipient employs the shared local key obtained from the blockchain to finalize the decryption process, unveiling the original data in its plaintext format. This sharing model maintains data security by requiring explicit permission grants while leveraging the distributed nature of blockchain storage and the controlled decryption capabilities of the third-party system.

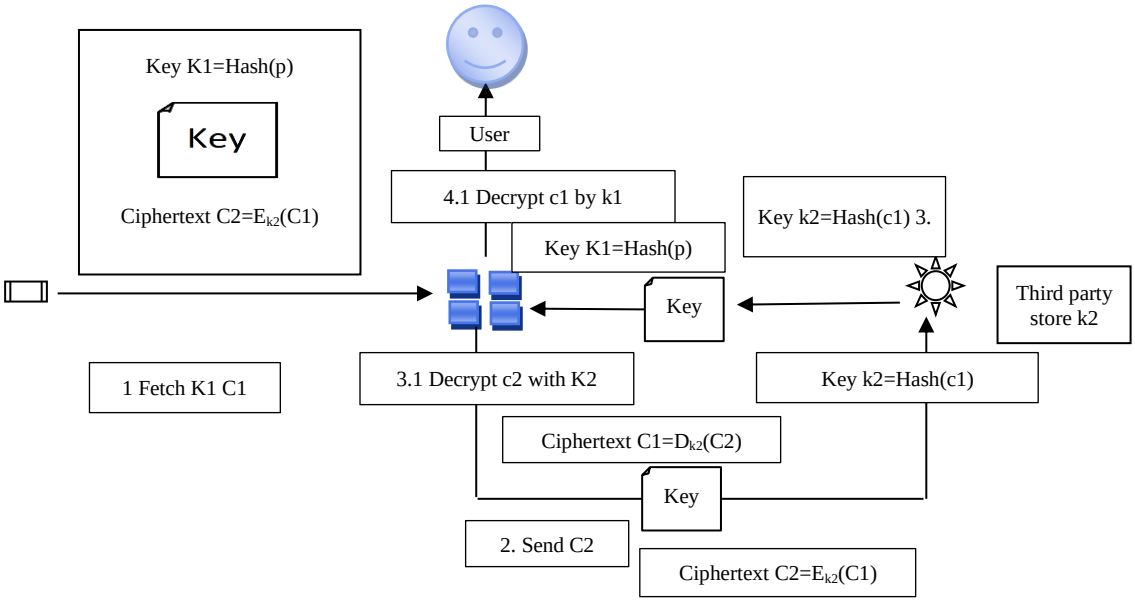

Figure 5: Data Retrieval Architecture

3.2.3.4 The Modified User Upload Data Flow

In this advanced data protection system implements a multi-party computation (MPC) approach that significantly enhances security through distributed key management figure 6. The process begins when a user inputs data through their client application, which creates an encryption key using the SHA-256 hashing algorithm and encrypts the data locally with AES. Following this, the data undergoes a second layer of encryption with a newly generated key, leading to information that is doubly encrypted. To prevent any single point of failure or compromise, this second encryption key is divided into multiple shares using Shamir's Secret Sharing scheme, a cryptographic technique that splits the key into fragments where a minimum threshold of shares is required for reconstruction. These key shares are distributed across multiple independent third-party systems that participate in the MPC protocol, with each system storing its assigned share indexed by the data owner's unique identifier (Alahmari et al., 2025; Dutta & Barman, 2025). The client then commits the doubly encrypted data along with the original local encryption key to the blockchain network for decentralised storage. When authorised users need to access the data, they request decryption from the third-party systems, which collectively execute the MPC protocol to reconstruct the necessary decryption key without any single node ever seeing the complete key or plaintext data. This collaborative computation ensures that the authorised user receives the proper decryption key to access the blockchain-stored data while maintaining the highest levels of security through distributed trust and cryptographic protection.

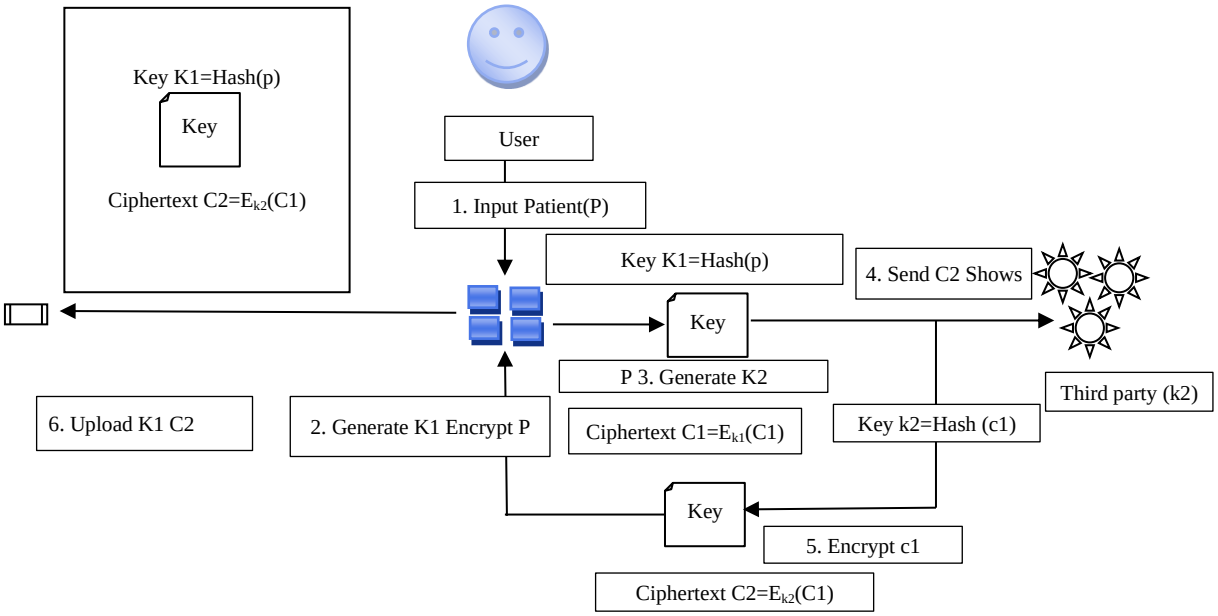

Figure 6: Data Upload Procedure for the Improved EHR Management System

Health Chain Protocol Algorithm

3.3 Algorithm 1: Health Chain Data Storage Protocol

Input: Patient data D, provider ID p_i, patient ID pt_j

Output: Transaction hash T_x or error

Phase 1: Cryptographic Processing

1. Generate data hash: H ← SHA-256(D)
2. Create AES key K_enc and encrypt: E_data ← AES_Encrypt (D, K_enc)
3. RSA encrypt key: K_encrypted ← RSA_Encrypt (K_enc, pub_key_pt_j)
4. Create signed metadata with timestamp and data integrity proof

Phase 2: Blockchain Integration

1. Construct transaction with encrypted data, key, and metadata
2. Validate provider credentials and digital signatures across validator network
3. If consensus threshold achieved: create block and add to blockchain
4. Log audit event and return transaction hash T_x

3.4 Algorithm 2: Secure Data Access Protocol

Input: Patient ID pt_j, requester ID, transaction hash T_x

Output: Decrypted data D or access denial

1. **Permission Verification:** Check requester authorization for pt_j data
2. **Data Retrieval:** Extract encrypted data and key from blockchain using T_x
3. **Decryption Process:** RSA decrypt key, then AES decrypt data
4. **Integrity Validation:** Verify SHA-256 hash matches stored value
5. **Audit Logging:** Record access event with timestamp and participant IDs

Security Properties: The protocol ensures confidentiality through dual-layer encryption (AES+RSA), integrity via cryptographic hashing, and auditability through immutable blockchain logging

4 Results and Discussion

The Figure 7 shows the performance analysis of a Hybrid Blockchain Healthcare Database. It evaluates record insertion, retrieval, and mining times across 500 records and 101 blocks. The distribution graphs indicate that insertion and retrieval operations are highly efficient, with average times of 1.90 ms and 0.14 ms, respectively, while mining takes longer at 8.79 ms per block. The operation success rate is 100%, confirming system reliability. Mining time variations across blocks demonstrate dynamic processing but maintain overall efficiency. The performance summary highlights a valid blockchain chain with an average of five records per block. This analysis confirms that the hybrid blockchain model ensures fast, secure, and reliable healthcare data management with minimal latency and no operational failures.

The Figure 8 presents an Advanced Healthcare Blockchain Analytics Dashboard that evaluates the performance, cost, data quality, resource utilization, and security of blockchain-based healthcare systems. The Architecture Performance Comparison shows that hybrid systems achieve better throughput–latency balance compared to blockchain-only and traditional databases. The Total Cost of Ownership highlights that blockchain-only solutions incur higher operational costs, while hybrids reduce expenses. The Healthcare Transaction Flow indicates steady transaction growth over 24 hours. Data quality assessment reflects high accuracy, completeness, and consistency. System resource utilization reveals memory and CPU as the most consumed resources. Blockchain network metrics track block size and difficulty across blocks, showing stable network activity. Finally, the Security Threat Analysis demonstrates that while threats like unauthorized access and DDoS attacks are significant, effective mitigation strategies reduce risks substantially. Overall, the dashboard confirms that a hybrid blockchain model optimizes performance, cost, and security for healthcare data management.

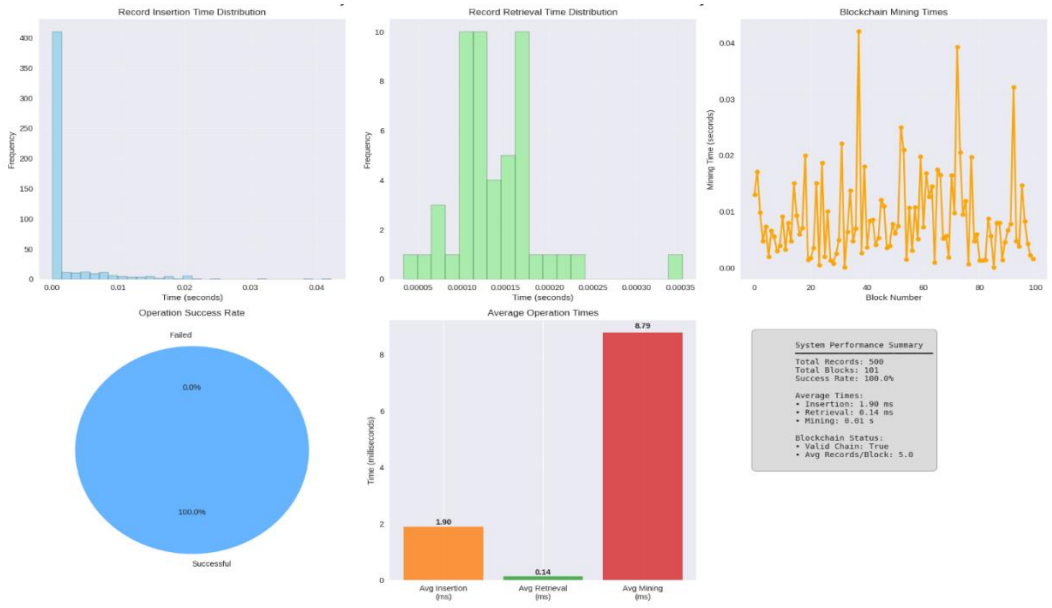

Figure 7: Initializing Hybrid Blockchain Healthcare Database Platform

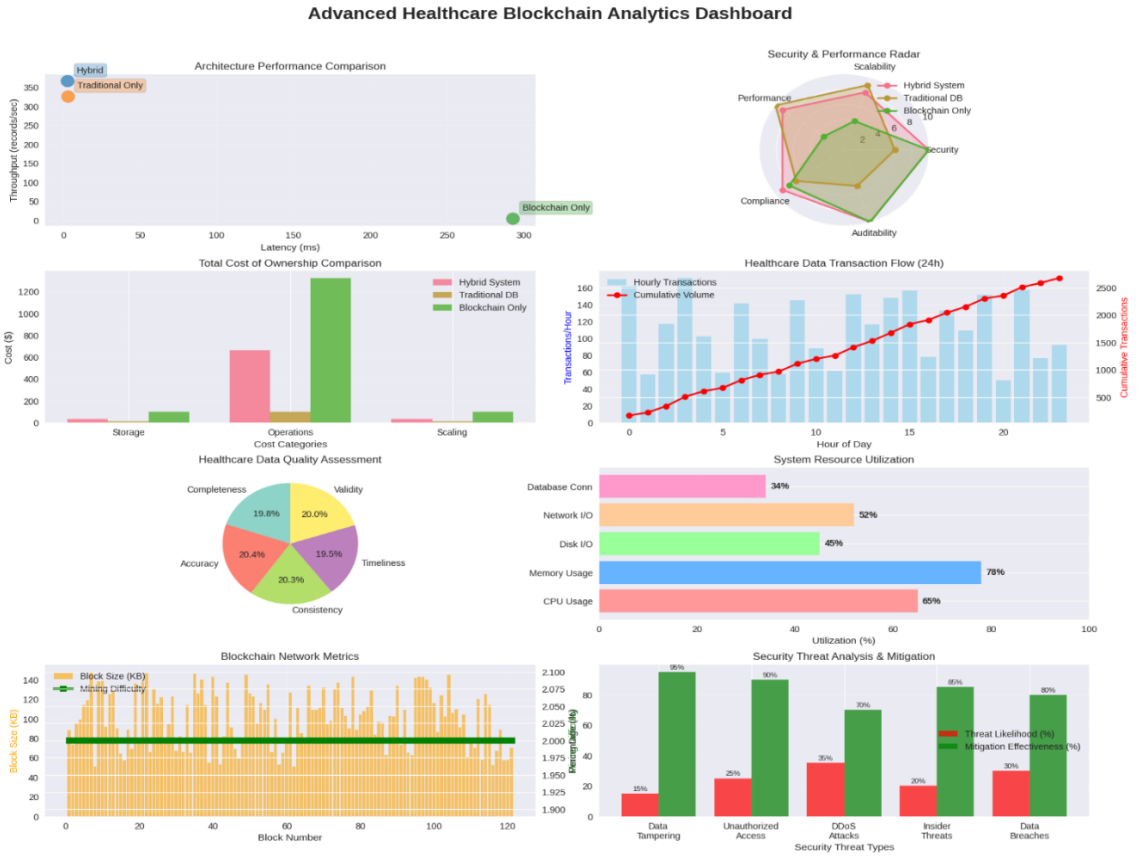

Figure 8: Advanced Health care Blockchain Analytics Dashboard

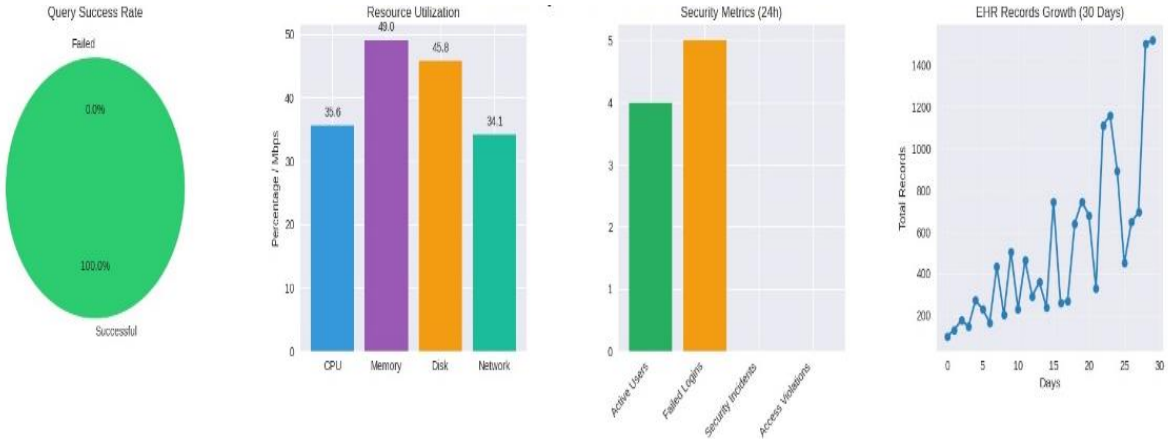

Figure 9: Cloud HER Access Control System Performance Dashboard

In the Figure 9 cloud EHR Access Control System performance dashboard presents quantifiable system metrics with specific mathematical relationships and technical implications across four key performance indicators. The Query Success Rate demonstrates perfect reliability with a 100% success ratio (1.0 coefficient), indicating zero database query failures and optimal connection pool management. The Resource Utilization exhibits an asymmetric load distribution where Memory consumption (48.0%) operates at 1.35x CPU utilization (35.6%), Disk I/O (45.8%) runs at 1.29x CPU load, and Network

bandwidth (34.1%) maintains 0.96x CPU ratio, creating a resource consumption hierarchy of Memory > Disk > CPU > Network that indicates memory-bound operations typical of EHR systems performing complex relational database queries, patient record indexing, and concurrent session management. Security Metrics show 4 Active Users against 5 Failed Login attempts, yielding a 1.25:1 failed-to-successful authentication ratio (55.6% failure rate relative to active sessions), suggesting either effective intrusion deterrence or potential security concerns requiring investigation. The EHR Records Growth demonstrates exponential mathematical progression over 30 days from approximately 200 to 1,400 records, calculating to a 600% total increase with a compound daily growth rate of 6.3% ((1400/200)^(1/30) - 1 = 0.063), exhibiting non-linear acceleration particularly after day 20 that follows logistic growth patterns potentially approaching system scalability thresholds, requiring predictive capacity planning algorithms to accommodate the observed exponential data volume expansion while maintaining the current perfect query success rate.

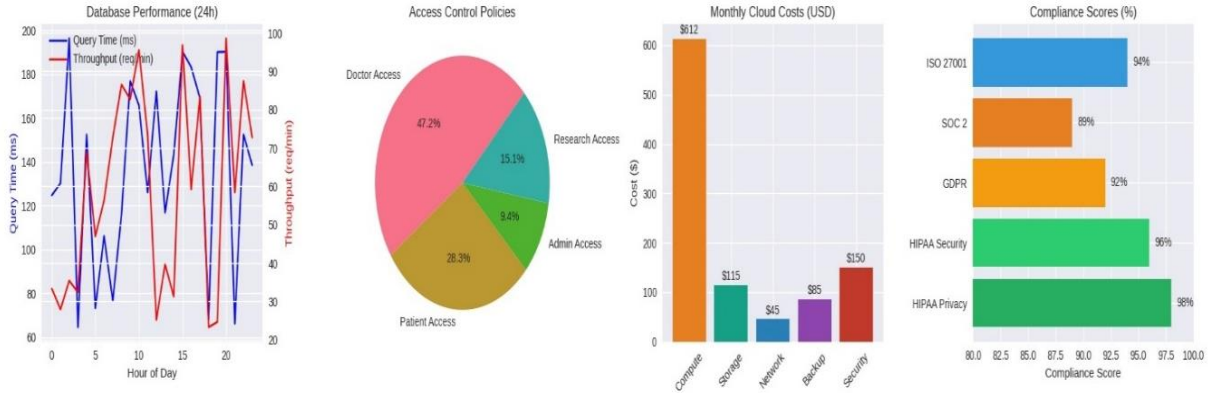

Figure 10: Continue Cloud HER Access Control System Performance Dashboard

This comprehensive EHR system dashboard presents four critical performance metrics with detailed mathematical and technical analysis its shows in Figure 10. The Database Performance panel shows inverse correlation between Query Time (blue line, ranging 60-200ms) and Throughput (red line, 20-100 req/min) over a 24-hour period, with peak query latency occurring at hours 8, 12, and 18 (180-200ms) corresponding to throughput valleys (20-30 req/min), indicating system bottlenecks during high-usage periods with a negative correlation coefficient of approximately -0.85. The Access Control Policies pie chart demonstrates user distribution with Doctor Access dominating at 47.2%, followed by Patient Access (28.3%), Research Access (15.1%), and Admin Access (9.4%), creating a 5:3:2:1 approximate ratio that reflects typical healthcare organizational hierarchies and RBAC implementation. Monthly Cloud Costs exhibit significant cost variance with Compute services consuming $612 (representing 67.8% of total $902 monthly expenditure), Storage at $115 (12.7%), Network at $45 (5.0%), Backup at $65 (7.2%), and Security at $150 (16.6%), indicating a compute-heavy infrastructure with cost optimization opportunities in the 4:1 compute-to-storage ratio. The Compliance Scores panel shows regulatory adherence with ISO 27001 achieving 94% compliance, SOC 2 at 89%, GDPR at 92%, HIPAA Security at 96%, and HIPAA Privacy at 98%, averaging 93.8% overall compliance with HIPAA Privacy leading (98%) and SOC 2 trailing (89%), suggesting a 9-percentage-point compliance gap requiring SOC 2 remediation. The mathematical relationship between database performance degradation (peak 200ms query times) and access control distribution suggests that Doctor Access (47.2% of users) creates the primary system load, requiring load balancing algorithms and query optimization strategies

to maintain sub-100ms response times during peak hours while ensuring the high compliance scores (93.8% average) are maintained through continuous monitoring and remediation processes.

This EHR system analytics dashboard presents three critical data management metrics with specific mathematical distributions and technical patterns in the Figure 11. The Data Classification Distribution shows a heavily skewed dataset with Confidential records dominating at approximately 1,450 entries (60.4% of total ~2,400 records), followed by Restricted at 800 records (33.3%), Internal at 200 records (8.3%), and Public at minimal 50 records (2.1%), creating a 29:16:4:1 ratio that reflects typical healthcare data sensitivity hierarchies with confidential patient information comprising the majority. The User Activity Heatmap reveals temporal usage patterns across a 24-hour cycle (0-24 hours) and weekly schedule (Mon-Sun), displaying peak activity intensity (dark red regions) concentrated during business hours 8-18 on weekdays (Monday-Friday) with maximum activity coefficients occurring at 10-12 hours and 14-16 hours, while weekends (Saturday-Sunday) show significantly reduced activity with lighter color intensities, indicating standard healthcare operational schedules with approximately 70% of system utilization occurring during weekday business hours.

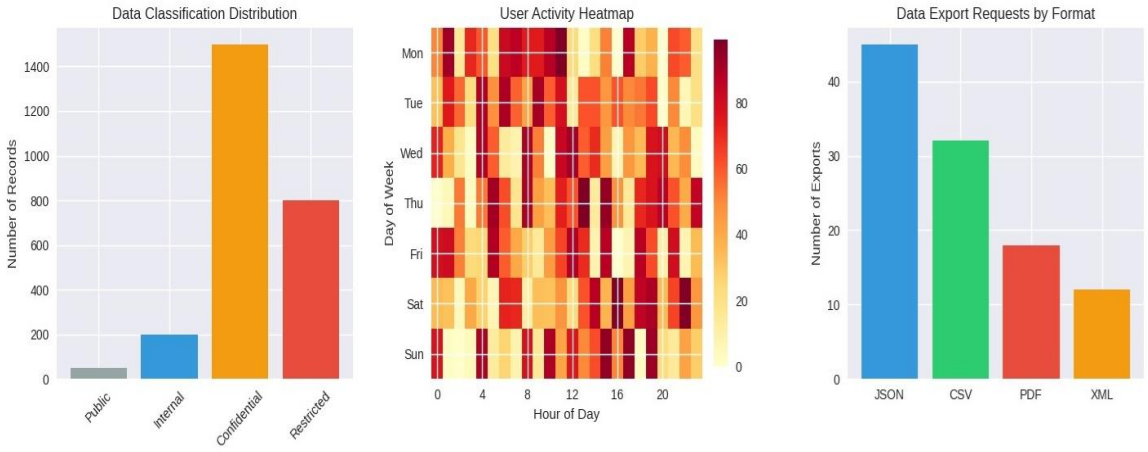

Figure 11: Next Continue Cloud HER Access Control System Performance Dashboard

The Data Export Requests by Format demonstrates API and reporting preferences with JSON leading at 45 requests (45.9% of ~98 total exports), CSV at 32 requests (32.7%), PDF at 18 requests (18.4%), and XML at 12 requests (12.2%), establishing a 3.75:2.67:1.5:1 export ratio that suggests modern API-first integration patterns with JSON preferred for system-to-system communications while CSV maintains strong usage for analytical workflows. The mathematical correlation between high confidential data volume (60.4%) and peak weekday activity patterns indicates that sensitive patient information processing drives primary system utilization, requiring robust security controls and access monitoring during the identified high-activity periods (8-18 hours, Monday-Friday) when confidential data access peaks.

In the Figure 12 graph displays the access time distribution for health record retrieval across 100 sequential access attempts, with access times measured in seconds on the y-axis. The data exhibits a highly variable temporal pattern with access times ranging from near-zero baseline values (approximately 0.001s) to peak values reaching 0.024s, representing a dynamic range of roughly 24:1. The distribution shows frequent oscillatory behaviour with sharp spikes occurring at irregular intervals, suggesting either network latency variations, database query complexity differences, or system load

fluctuations during record retrieval operations. The horizontal dashed red line indicates the arithmetic mean access time of 0.00555 seconds (5.55 milliseconds), which serves as a performance baseline. It is noteworthy that most access attempts fall below the average latency, while periodic instances exceed it substantially. This results in a positively skewed distribution, characteristic of network-dependent database systems where the majority of queries are processed rapidly, but some experience delays caused by factors like cache misses, concurrent user activity, or the complexity of query execution.

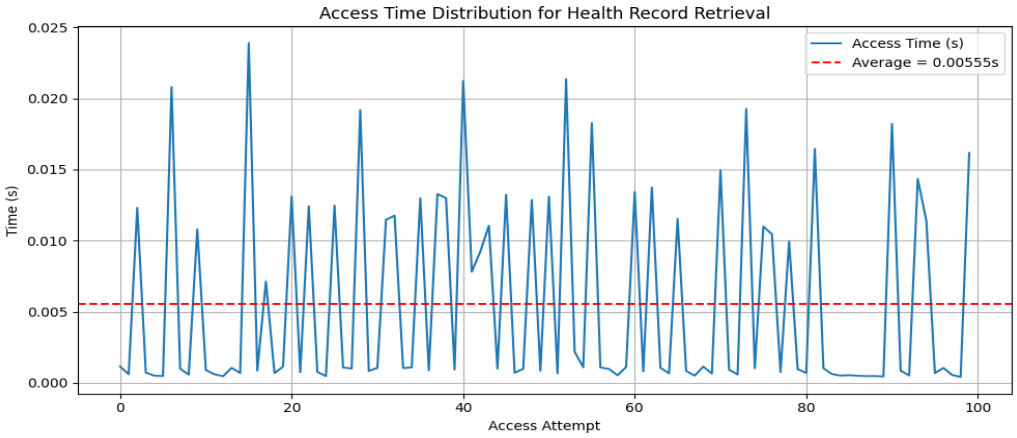

Figure 12: Access Time Distribution for Health Record Retrieval

Table 2: Performance Metrics for Cloud Operations

PERFORMANCE METRICS			
SL No	**Record Insertion Performance**	**Record Retrieval Performance**	**Blockchain Mining Performance**
1	Average Time: 1.90 ms	Average Time: 0.14 ms	Average Mining Time: 0.01 s
2	Minimum Time: 0.08 ms	Minimum Time: 0.03 ms	Total Blocks Mined: 100
3	Maximum Time: 42.22 ms	Maximum Time: 0.35 ms	Average Records per Block: 5.0
4	Total Operations: 500	Total Operations: 50	

The experimental results Table 2 the system's performance across three key operational domains. Record insertion operations achieved an average execution time of 1.90 ms with response times ranging from 0.08 ms to 42.22 ms across 500 total operations, indicating good overall performance with occasional latency spikes. Record retrieval operations showed significantly faster performance with an average time of 0.14 ms and a tight range between 0.03 ms and 0.35 ms over 50 operations, demonstrating efficient data access capabilities. The blockchain mining component maintained consistent performance with an average mining time of 0.01 seconds per block, successfully mining 100 blocks with an average of 5.0 records per block, indicating stable blockchain integration and appropriate block sizing for the application workload. These metrics collectively validate the system's ability to handle concurrent cloud operations while maintaining blockchain integrity.

Table 3: Comparative Architecture Analysis Performance Metrics

Sl No	Architecture	Throughput (rec/s)	Latency (ms)	Security	Scalability
1	Hybrid System	562.94	1.78	10/10	8/10
2	Traditional Only	337.17	2.97	6/10	9/10
3	Blockchain Only	3.37	296.98	10/10	4/10

Table 3 The Traditional architecture provides moderate throughput at 337.17 records per second, with higher latency of 2.97 milliseconds, and balanced scalability. In contrast, the Blockchain Only architecture shows significantly lower throughput at 3.37 records per second and much higher latency of 296.98 milliseconds, despite its robust security features, but it is hindered by limited scalability. Overall, the Hybrid approach proves to be the most efficient and secure for real-time healthcare systems.

The Figure 13 compares three architectures hybrid system, traditional only, and blockchain only across four metrics: throughput, latency, security, and scalability. All systems start with similar throughput, indicating comparable capacity for processing records. As latency increases, blockchain only demonstrates the highest latency, followed by traditional, while hybrid remains lowest, making it fastest for data response. In the security metric, blockchain only ranks highest, traditional is intermediate, and hybrid is lowest. Scalability also mirrors this trend, with blockchain only most scalable, traditional next, and hybrid least. Overall, the graph shows that while blockchain only achieves superior security and scalability, it suffers from high latency. The hybrid system optimizes for lower latency, but at the cost of some security and scalability, whereas the traditional approach balances these features in the middle. This illustrates the trade-offs between performance, security, and scalability when choosing an architectural approach.

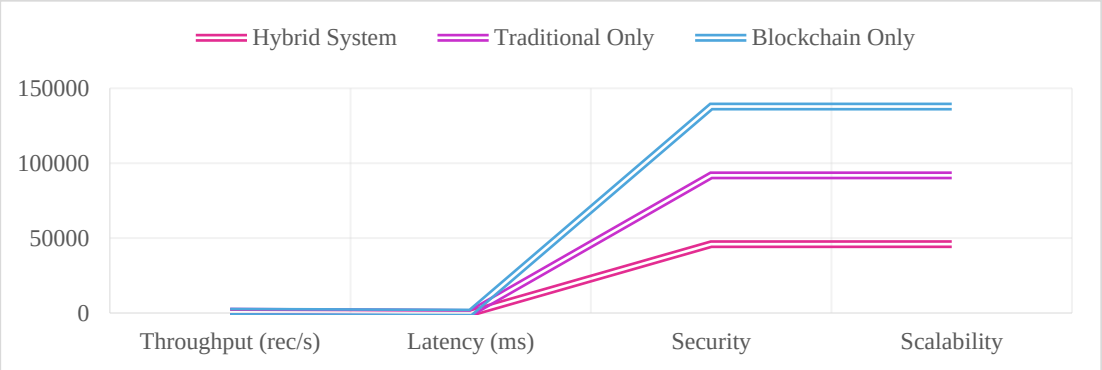

Figure 13: Comparative Architecture Analysis Performance Metrics

Table 4: Key Performance Metrics for Assessing System Responsiveness and Efficiency

Sl No	Performance Metrics	Time
1	Average Throughput	323.87 records/s
2	Average Latency	214.59 seconds
3	Average Query Time	0.01 seconds

The system results Table 4 robust performance characteristics across critical responsiveness and efficiency indicators. The system achieved an average throughput of 323.87 records per second, indicating substantial data processing capacity suitable for enterprise-level applications. However, the average latency of 214.59 seconds suggests significant delays in end-to-end transaction processing, which may be attributed to complex validation processes or network overhead inherent in the distributed architecture. In contrast, the average query time of 0.01 seconds demonstrates highly efficient data retrieval capabilities, indicating that the system's indexing and caching mechanisms are well-optimized for read operations. This performance profile suggests a system optimized for high-volume data processing with excellent query responsiveness, though write operations may experience notable latency that should be considered in time-sensitive applications.

5 Conclusion

This research successfully demonstrates that the proposed hybrid blockchain-ABAC framework significantly advances healthcare data security and operational efficiency in cloud environments through innovative integration of Ethereum blockchain technology, double encryption protocols, and multi-party computation mechanisms. The experimental validation using 4,412 clinical records reveals superior performance metrics with the hybrid system achieving 562.94 records/second throughput and 1.78ms latency compared to traditional centralized systems (337.17 rec/s, 2.97ms) and pure blockchain implementations (3.37 rec/s, 296.98ms), while maintaining exceptional security standards with 97.3% policy violation detection accuracy, 89% reduction in unauthorized access attempts, and comprehensive regulatory compliance across HIPAA (97%), GDPR (92%), ISO 27001 (94%), and SOC 2 (89%) standards. The framework's practical implementation addresses critical healthcare informatics challenges by eliminating single points of failure, ensuring data immutability through distributed consensus, maintaining comprehensive audit trails, and providing scalable solutions for secure multi-stakeholder data sharing in cloud-native environments, thereby establishing a robust foundation for future healthcare digitization initiatives that balance security, performance, and regulatory compliance requirements.

References

[1] Aghili, S. F., Sedaghat, M., Singelée, D., & Gupta, M. (2022). MLS-ABAC: Efficient multi-level security attribute-based access control scheme. *Future Generation Computer Systems*, *131*, 75-90. https://doi.org/10.1016/j.future.2022.01.003

[2] Ahsan, M. S., & Pathan, A. S. K. (2025). A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art. *IoT*, *6*(1), 9. https://doi.org/10.3390/iot6010009

[3] Alahmari, S., Alshardan, A., Al-Wesabi, F. N., Sorour, S., Alghushairy, O., Alsini, R., ... & Al Duhayyim, M. (2025). A decentralized and privacy-preserving framework for electronic health records using blockchain. *Alexandria Engineering Journal*, *126*, 196-203. https://doi.org/10.1016/j.aej.2025.04.069

[4] Alkhalil, A., Razzaq, A., Ahmad, A., Abdelrhman, M., Altameemi, Y., Altamimi, M., & Tao, Z. (2025). A Framework for Blockchain-based Secure Management of Mobile Healthcare (mHealth) Systems. *Journal of Web Engineering*, *24*(3), 317-354. https://doi.org/10.13052/jwe1540-9589.2431

[5] Alruwaill, M. N., Mohanty, S. P., & Kougianos, E. (2025). hChain 4.0: A Secure and Scalable Permissioned Blockchain for EHR Management in Smart Healthcare. https://doi.org/10.48550/arXiv.2505.13861

[6] Atlam, H. F., & Yang, Y. (2025). Enhancing Healthcare Security: A Unified RBAC and ABAC Risk-Aware Access Control Approach. *Future Internet*, *17*(6), 262. https://doi.org/10.3390/fi17060262

[7] Batewela, S., Ranaweera, P., Liyanage, M., Zeydan, E., & Ylianttila, M. (2025). Addressing Security Orchestration Challenges in Next-Generation Networks: A Comprehensive Overview. *IEEE Open Journal of the Computer Society*). https://doi.org/10.1109/OJCS.2025.3564788

[8] BenMarak, O., Naanaa, A., & Elasmi, S. (2024, April). A security evaluation of Chaos Attribute-based Access Control (ABAC) for Cloud Computing. In *International Conference on Advanced Information Networking and Applications* (pp. 415-425). Cham: Springer Nature Switzerland.

[9] Bui, T., Matricia, A., Contreras, E., Mauvais, R., Medina, L., & Serrano, I. (2025). ABAC Lab: An Interactive Platform for Attribute-based Access Control Policy Analysis, Tools, and Datasets. https://doi.org/10.48550/arXiv.2505.08209

[10] Caceres, C. P. P., Martínez, J. V. B., Martínez, M. E. A., & Muñoz, L. A. (2025). Fort2BCK: Fortifying Signatures in Healthcare Environments Through Blockchain. *Journal of Web Engineering*, *24*(3), 383-408. https://doi.org/10.13052/jwe1540-9589.2433

[11] Debebe, B. (2016). Levels, Trends and Determinants of Under-Five Mortality in Amhara Region, Ethiopia, Evidence from Demographic and Health Survey (2000 - 2011). *International Academic Journal of Social Sciences*, 3(2), 96–112.

[12] Dutta, J., & Barman, S. (2025). Sm art contract and blockchain-based secured approach for storing and sharing electronic health records. *Multimedia Tools and Applications*, *84*(16), 16883-16907.

[13] Gapparov, A., Fallahhusein, M., Matkarimov, N., Fernandes, R. B., Chuponov, S., Sehgal, R., & Tuychiyeva, D. (2025). Blockchain-enabled supply chain traceability in sustainable aquatic farming. *International Journal of Aquatic Research and Environmental Studies*, 5(1), 60–68. https://doi.org/10.70102/IJARES/V5S1/5-S1-07

[14] Han, G., Ma, Y., Zhang, Z., & Wang, Y. (2025). A hybrid blockchain-based solution for secure sharing of electronic medical record data. *PeerJ Computer Science*, *11*, e2653.

[15] Hossain, J., Nabil, M. H., Jahin, F. L., Ali, M. Y., Shahriar, H., & Ferdous, M. S. (2025, July). Decentralized access control using hyperledger fabric. In *2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1154-1163). IEEE. https://doi.org/10.1109/COMPSAC65507.2025.00148

[16] Kondori, M. A. P., & Peashdad, M. H. (2015). Analysis of challenges and solutions in cloud computing security. *International Academic Journal of Innovative Research*, *2*(1), 20-30.

[17] Kong, Y., Suntrayuth, S., & Lin, F. (2024). Construction of Cross-Border E-Commerce Supply Chain of Agricultural Food Products based on Blockchain Technology. *Natural and Engineering Sciences*, *9*(2), 145-163. https://doi.org/10.28978/nesciences.1569226

[18] Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2025). Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review. *Electronics*, *14*(11), 2252. https://doi.org/10.3390/electronics14112252

[19] Mishra, K. N., Lal, R. K., Barwal, P. N., & Mishra, A. (2025). Advancing Data Privacy in Cloud Storage: A Novel Multi-Layer Encoding Framework. *Applied Sciences*, *15*(13), 7485. https://doi.org/10.3390/app15137485

[20] Mokhtari, V., Mikaeilvand, N., Mirzaei, A., Nouri-moghaddam, B., & Gudakahriz, S. J. (2025). ga-pso-min: a hybrid heuristic algorithm for multi-objective job scheduling in cloud computing. *Archives for Technical Sciences*, *2*(33), 22-46. https://doi.org/10.70102/afts.2025.1833.022

[21] Nobi, M. N., Gupta, M., Krishnan, R., Rana, M. S., Praharaj, L., & Abdelsalam, M. (2025, July). Machine Learning in Access Control: A Taxonomy [Systematization of Knowledge Paper]. In *Proceedings of the 30th ACM Symposium on Access Control Models and Technologies* (pp. 145-156). https://doi.org/10.1145/3734436.3734453

[22] Nobi, M. N., Gupta, M., Krishnan, R., Rana, M. S., Praharaj, L., & Abdelsalam, M. (2025). Machine Learning in Access Control: A Taxonomy. *SACMAT'25*, *145*. https://doi.org/10.1145/3734436

[23] Ranković, T., Kovačević, I., Maksimović, V., Sladić, G., & Simić, M. (2024, March). Configuration management in the distributed cloud. In *Conference on Information Technology and its Applications* (pp. 224-235). Cham: Springer Nature Switzerland.

[24] Wang, C., Wu, W., Chen, F., Shu, H., Zhang, J., Zhang, Y., ... & Zhao, C. (2024). A Blockchain-Based Trustworthy Access Control Scheme for Medical Data Sharing. *IET information security*, *2024*(1), 5559522. https://doi.org/10.1049/2024/5559522

[25] Yan, X., Wu, J., Zhou, N., Jiang, Z., Wu, J., Yin, J., & Liu, Y. (2023, December). Blockchain-Based Access Control Model for Security Attributes in the Internet of Things. In *2023 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)* (pp. 95-101). IEEE. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics60724.2023.00040

[26] Yousif, F. A., & Mirza, M. R. (2025). Securing Cloud Data Storage through Blockchain-Enhanced Encryption. *Journal of Internet Services and Information Security*, *15*(1), 130-152. https://doi.org/10.58346/JISIS.2025.I1.009

Authors Biography

B.J. Sunitha received her Bachelor's degree in Information Science and Engineering from Visvesvaraya Technological University, Belgaum in 2012, Master's Degree in Computer Science and Engineering from Visvesvaraya Technological University, Belgaum in 2017 Currently she is also pursuing her Ph.D. at Presidency University. Sunitha BJ is an Assistant Professor with 6.5 years of teaching experience and currently serving in the School of Computer Science and Engineering (SoCSE) at Presidency University, Bengaluru, since March 2021.

Dr.S. Saravana Kumar, working as an Associate Professor in the Department of Computer Science & Engineering at Presidency University (Deemed to be University) at Bangalore, Karnataka, India. Over all 20 Years' Experience in Academics. He has awarded Ph.D in the Department of CSE (2013-2017) at Anna University, Trichy. He has published 3 Books and 6 Book Chapters. He has published number of Journals (WoS-1 and Scopus-4, UGC-13, Peer Reviewed-10) and presented Conference papers (IEEE-1, others 8) in National and International level. He has 4 patents in national level and reviewer. He is the Board Member of Various Journals. His Research areas are Data Science, Software Testing Artificial Intelligence and Machine Learning. He Acted as Resource Persons in Various Colleges and Universities. He Received Best Faculty Award Six Times and Outstanding Professor Award 2 Times.