International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

SECURING CLOUD INFRASTRUCTURE THROUGH HYPERLEDGER FABRIC-BASED ACCESS MANAGEMENT

Ashvini K. Butani[1*], Dr. Ravirajsinh S. Vaghela[2]

[1*]Research Scholar, Department of Computer Science, Gujarat Technological University, Ahmedabad-382424-Gujarat, India, ashbhatti47@gmail.com, 0009-0002-5656-9741

[2]Assistant Professor, School of Cybersecurity and Digital Forensics, National Forensic Sciences University, Gandhinagar, Gujarat, India, ravirajsinh.vaghela@nfsu.ac.in, 0000-0002-6303-9450

Abstract

Cloud infrastructure refers to the dynamic provisioning of computing resources over the internet, enabling scalable and flexible enterprise operations. However, such environments face significant security challenges, particularly in access management. Cloud infrastructure delivers scalable computing resources, yet traditional Identity and Access Management (IAM) mechanisms face challenges such as centralized control, misconfigurations, and limited auditability. This study addresses these challenges by proposing a Hyperledger Fabric-based decentralized access control framework integrated with Amazon Web Services (AWS) for healthcare data security. The framework employs Zero Knowledge Proof (ZKP) for identity validation, Ciphertext Policy Attribute Based Encryption (CP-ABE) with Proxy Re-Encryption (PRE) for fine-grained data access, and machine learning driven anomaly detection for continuous monitoring. Experimental evaluation achieved throughput of 15000 transactions per second, latency of 350 milliseconds, privacy preservation up to 99.1 percent, and anomaly detection accuracy of 99.63 percent, surpassing prior models significantly. Storage analysis demonstrated predictable scalability with encrypted medical records up to 20 MB, while token revocation time remained within 1.9 seconds under network stress. The results confirm that blockchain-based access control enhances security, privacy, and auditability while maintaining operational efficiency. This research establishes a scalable and tamper-resistant model for secure healthcare data management in cloud environments.

Keywords: Amazon Web Services, Hyperledger Fabric, Blockchain, Access Management, Cloud Security.

1. Introduction

Cloud computing has completely revolutionized how companies manage and provide IT services since it provides internet-based computing services on scale, on demand, and at a low cost [1,2]. These services are offered in the form of AWS, Microsoft Azure, and Google Cloud Platform (GCP), on which users run applications without any physical maintenance of infrastructures [3,4]. Moreover, apart from supporting these services, these infrastructures provide a mature ecosystem of complementary services like virtual machines, data storage facilities, analytics, Artificial Intelligence (AI), Machine Learning (ML) facilities, and integration with Internet of Things (IoT) [5]. Organizations' increasing trend of trusting sensitive workloads and data into the cloud makes governing non-derivable resource access to cloud-based systems core to information security, privacy, compliance, and trust [6-8].

Cloud ecosystems possess a very distributed and dynamic nature, such that IAM must deliver security. IAM prescribes controls, policies, and processes for dealing with user identities and how they utilize resources, granting access subject to some stipulations [9–11]. It is critical in large enterprise environments with disparate roles and services. Still, traditional IAM remains centralized and often resides with providers or administrators, creating risks due to misconfigurations, insider threats, and a lack of insight [12–15].

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Blockchain technology addresses these limitations through a decentralized and tamper-resistant design. As a distributed ledger, it records transactions securely and transparently across multiple nodes [16,17]. Originally developed for cryptocurrencies, it is now applied in supply chains, healthcare, voting, and digital identity [18–20]. Its immutability, consensus validation, and traceability ensure trust, accountability, and data integrity [21,22]. Every transaction is validated by consensus and cannot be altered without network agreement, providing verifiable transparency [23].

Within this space, Hyperledger Fabric is a leading permissioned blockchain framework developed by the Linux Foundation [24]. Unlike public blockchains such as Bitcoin or Ethereum, it restricts participation to authenticated members, making it suitable for enterprise applications requiring privacy, compliance, and controlled access [25,26]. Its modular design allows customization of consensus, membership, and smart contract logic (chaincode) [27,28]. Fabric further supports private channels, role-based policies, and cryptographic signing, ensuring non-repudiation and traceability [29,30]. By removing single points of failure and offering scalability, fabric addresses the shortcomings of centralized IAM, providing secure, auditable, and compliance-ready access management for cloud environments [31].

This research addresses the risks to AWS cloud infrastructure arising from unauthorized access and data breaches, which result from the shortcomings of the system's IAM consolidated interfaces in enforcing adequate security controls. Although AWS incorporates IAM and CloudTrail, these features might not sufficiently safeguard enterprises requiring enduring access control systems that are secure, auditable, and resistant to tampering. The approach taken in this study is to integrate the permissioned blockchain framework, Hyperledger Fabric, into AWS to build a system for access management that is decentralized, transparent, and immutable. This integration improves compliance and security of access control through the use of smart contracts, consensus mechanisms, and encryption. The singularity of the approach is the application of decentralized consensus and immutability of blockchain technology, together with the scaling ability of AWS infrastructure. This combination fundamentally changes the paradigm for cloud security access control mechanisms.

Identified deficiencies in the IAM system within the AWS cloud framework served as a key motivator for this research. The traditional approaches to IAM become problematic when an organization's sensitive workload is shifted to the cloud, due to misconfigurations, insider attacks, and a lack of visibility in tenant services and compliance-driven environments. Proprietary AWS security offerings, including IAM and CloudTrail, also suffer from a lack of distributed control, immutable logging, and auditable access management. This study was motivated by the purpose of achieving a transparent and decentralized access management system for AWS, integrating Hyperledger Fabric, a permissioned blockchain framework, into AWS's infrastructure. This research seeks to bridge this gap by proposing and evaluating a blockchain-based access control framework built on Hyperledger Fabric, aimed at enhancing the security, transparency, and auditability of AWS cloud-hosted healthcare systems. The framework is designed to complement, rather than replace, existing cloud services by offering an added layer of cryptographic assurance, traceability, and user-controlled data access. The approach addresses the shortcomings of centralized IAM by introducing decentralized policy enforcement, cryptographically signed access logs, and patient-centric access governance. The contributions of this study are threefold:

- A comprehensive analysis and study of limitations in conventional IAM systems deployed in cloud-based healthcare platforms.
- The design of a decentralized access management architecture using Hyperledger Fabric, enabling policy immutability, decentralized verification, and auditable recordkeeping.
- A performance evaluation comparing the proposed framework with traditional IAM models in terms of throughput, latency, and security guarantees under real-world constraints.

By situating blockchain at the intersection of security, compliance, and operational scalability, this research aims to

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

establish a robust foundation for future-proof access control systems tailored for privacy-critical cloud environments.

This proposed research study provides an overview of the topic in Section 1. Several researchers have made important contributions, which are highlighted in Section 2. Section 3 outlines the suggested method and the associated algorithm. Hypotheses of the research are added in Section 4. Section 5 provides the results and discussion of the research in detail. Further, the conclusion and future work of the study are provided in Section 6.

2. Literature Review

Several recent studies have explored the integration of blockchain frameworks, particularly Hyperledger Fabric, within cloud infrastructures such as AWS to enhance IAM, data security, and operational scalability. Sutradhar et al. (2024) [32] introduced a scalable IAM system combining Hyperledger Fabric with OAuth 2.0, demonstrating secure patient identity management and access verification in healthcare systems, with empirical validation supporting its effectiveness in reducing fraud and enhancing interoperability. Elghoul et al. (2023) [33] developed a cost-effective, serverless Electronic Health Record (EHR) management architecture on AWS, incorporating multi-layered blockchain access control and role-based permissions to ensure secure record access. In a similar vein, Saah et al. (2023) [34] deployed Hyperledger Fabric over AWS to address data integrity challenges in the construction industry, validating system reliability using Hyperledger Explorer. Shammar et al. (2022) [35] proposed an Attribute-Based Access Control mechanism on Hyperledger Fabric (ABAC-HLFBC), which outperformed prior Fabric-IoT models in latency and throughput, as evaluated through Golang test suites and Hyperledger Caliper benchmarks. Shih et al. (2022) [36] extended blockchain access management to the Industrial Internet of Things (IIoT), designing smart contracts for policy enforcement and resource query through a dynamic and decentralized ABAC framework. Gohar et al. (2022)

[37] contributed a five-tiered Patient-Centric Healthcare (PCH) architecture integrating Blockchain, Cloud, and IoT for improved interoperability and secure data sharing, outperforming traditional healthcare data exchange models in terms of modularity and governance. Furthermore, Elghoul et al. (2022) [38] leveraged Amazon Managed Blockchain (AMB) to implement a cloud-based Hyperledger Fabric Blockchain Network (HFBN), achieving a 95.4% improvement in data integrity and a 28% reduction in transaction latency when compared to conventional EMR systems. Lastly, Iftekhar et al. (2021) [13] addressed Modbus IIoT security vulnerabilities by introducing a self-sovereign identity model based on Hyperledger Fabric, which eliminated single points of failure and improved system

responsiveness by 30% while reducing identity-related breaches by 40%. Collectively, these studies affirm the potential of blockchain-enhanced architectures to overcome the limitations of centralized IAM systems in cloud environments, while also establishing a foundation for secure, decentralized, and auditable access control across diverse application domains.

The following are the research gaps based on the previous research done by various authors. Limited studies have evaluated the scalability of Hyperledger Fabric under real-time, high-throughput workloads in cloud-native environments [38]. Existing models rarely address fine-grained, role-based access control with tamper-proof auditability in multi-tenant cloud systems [13]. Most studies lack empirical analysis on the latency-performance trade-off for access management using Hyperledger Fabric in distributed cloud settings [34,35].

The next section of this research provides the proposed methodology in detail, which helps to overcome the identified research gaps.

3. Hypothesis of research

H1: A blockchain-based access control framework combined with advanced cryptographic techniques can provide stronger security, privacy, and trust in cloud and IoT healthcare environments compared to traditional centralized models.

H2: Integrating optimization and anomaly detection into an access control system enhances its efficiency, scalability, and reliability, ensuring consistent performance even under high load and adverse network conditions.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4. Research Methodology

In this section, the proposed methodology for secure and auditable access control using Hyperledger Fabric in AWS cloud-based healthcare systems is provided in detail, outlining the techniques and sequential steps employed.

4.1 Patient Policy Setup and Zero-Knowledge Proof Validation

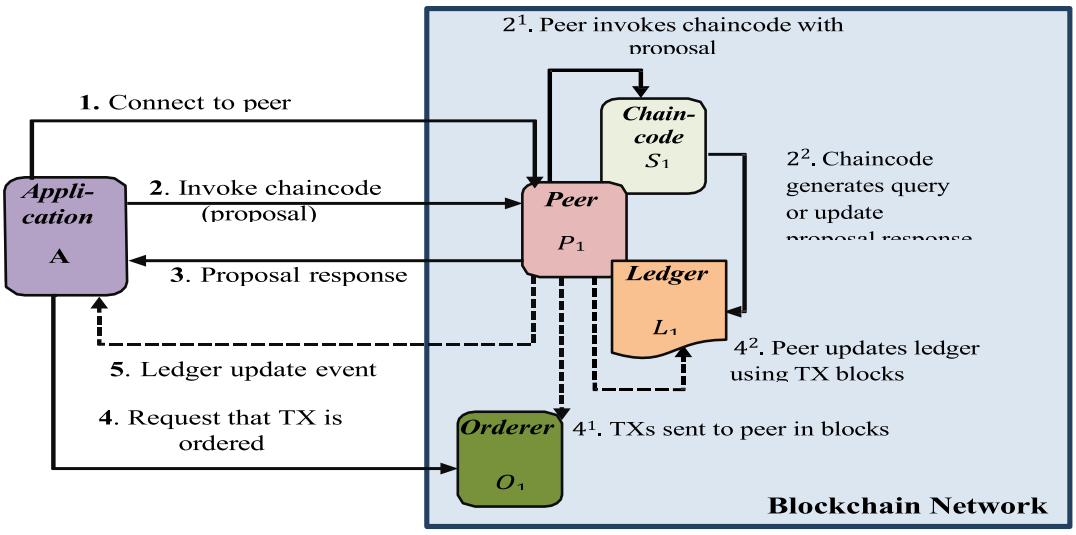
In the proposed framework, the access control process begins with patients configuring personalized access policies, which are stored immutably on the Hyperledger Fabric ledger using blockchain smart contracts. These policies define conditions under which specific user roles (e.g., doctors, specialists) can access Electronic Health Records (EHRs). When a doctor initiates a request, they must provide a ZKP to validate their identity and compliance with the defined access policy, without revealing sensitive credential details. The ZKP protocol ensures that a prover (doctor) can convince a verifier (ledger) that they possess valid credentials x, satisfying a certain predicate $P(x) = true$, without disclosing x itself. This is represented as:

$\exists x: P(x) = true$ but no information about x is revealed. (1)

The validation engine on Hyperledger Fabric checks whether the policy condition embedded in the chaincode aligns with the verified proof. Suppose the ZKP is invalid or the policy does not match the requester's attributes. In that case, the access is denied by default, thereby enforcing privacy-preserving, patient-controlled, and tamper-resistant policy enforcement at the access entry point. This initial step establishes the trust foundation for all subsequent access and auditing procedures in the system.

Hyperledger Fabric is a leading platform for permissioned blockchain networks, valued for its modular architecture and secure access control in cloud environments [39]. It includes peers, an ordering service, MSPs, and chaincode for executing business logic [40,41]. As illustrated in Figure 1, transactions are proposed, validated, ordered, and committed to the ledger by authenticated members. Its architecture ensures scalability, privacy, and enterprise-grade security [42].

Figure 1: Architecture of Hyperledger Fabric [43]



These policies are encoded and deployed as **Chaincode**, Hyperledger Fabric's smart contract mechanism, on the blockchain. In cloud computing, Chaincode refers to smart contracts used in permissioned blockchains like Hyperledger Fabric [13] (see Figure 1). It defines business logic for managing transactions in a decentralized manner, enhancing security and reducing the risk of fraud [44]. Chaincode enables automation and consistency across

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

distributed cloud applications [45]. In this framework, it validates Zero Knowledge Proofs (ZKPs), enforces patient access rules, and records decisions. Upon invocation, it checks policy compliance and triggers actions such as capability token issuance.

4.2 Capability Token Generation and Decision Receipt Signing

Once the ZKP is validated and the access policy conditions are met, the system proceeds to mint a short-lived capability token. This token includes an accumulator witness (for cryptographic verification of membership) and acts as a temporary, verifiable permission artifact. The system then writes a signed decision receipt, which serves as auditable proof that access was granted based on policy compliance.

- The capability token **'T'** is minted:

$$T = Sign_{Fabric}(ID_{doctor}, PolicyID, Witness, Timestamp) \quad (2)$$

- The accumulator witness ensures the token can be cryptographically verified later as part of the valid user set without revealing patient policy contents.

- The signed decision receipt logs the action and is stored immutably for auditability.

Once the capability token is verified, the system, through a secure Cloud Adapter interface, invokes the necessary decryption process. The cloud adapter mediates between the blockchain-based policy engine and the AWS cloud storage system that holds the encrypted EHR. It coordinates the application of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Proxy Re-Encryption (PRE) logic, ensuring that only policy-compliant users can retrieve and decrypt the AES key needed to access the data.

The AWS security architecture reinforces this process with a multi-layered defense framework ensuring resource availability, confidentiality, and integrity [46-48]. It incorporates tools like Amazon GuardDuty, WAF, KMS, and IAM for threat detection, encryption, and access control [49,50]. As illustrated in Figure 2, services such as ECS, EC2, and S3 operate within VPCs for isolated environments, with CloudTrail and CloudWatch supporting automated auditing [51]. This layered model ensures strong security, data governance, and regulatory compliance [52].

- User → WAF → EC2/RDS → GuardDuty/Shield: General formation of security architecture

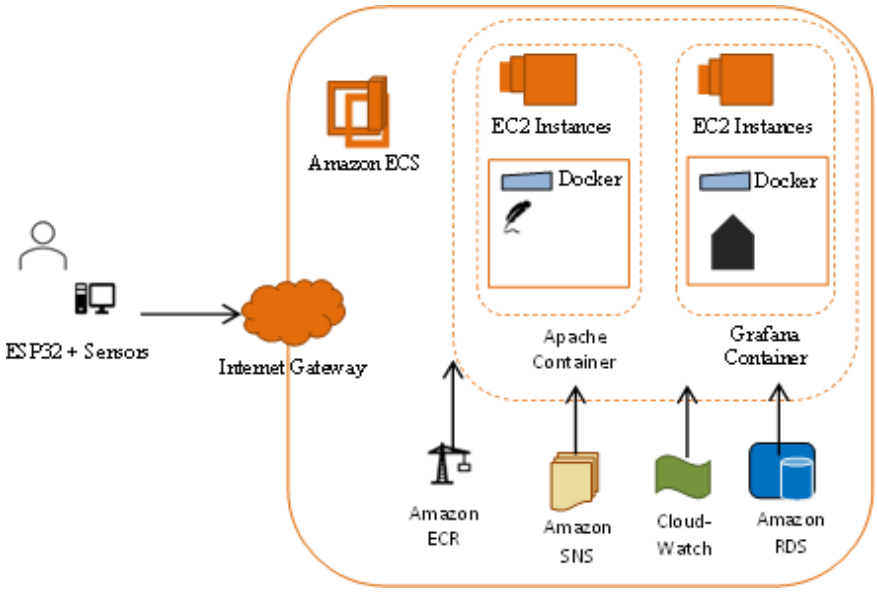


Figure 2: Architecture of Amazon Web Services [53]

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4.3 Token Validation and Encrypted EHR Access via CP-ABE and PRE

In this phase, the minted capability token is presented by the doctor and validated by the system to ensure it is untampered, valid within the access time window, and issued by a trusted authority. Upon successful validation, the system proceeds to unlock the symmetric AES key used to encrypt the patient's EHR. This is achieved using CP-ABE combined with Proxy Re-Encryption (PRE), which ensures that decryption can only occur if the user's attributes match the encryption policy set by the patient. The cryptographic process of this is as follows:

- **Access Policy Enforcement** using CP-ABE: Let M be the access matrix (policy) and γ be the user's attribute set. Decryption is allowed only if:

$$M \cdot \gamma^T \geq threshold \tag{3}$$

- **PRE** allows the cloud proxy to transform ciphertext CCC from encryption under the patient's public key pk_A to the doctor's key pk_B, without accessing the plaintext.

- **Final Decryption**: The re-encrypted symmetric key k is used to decrypt the AES-encrypted EHR:

$$EHR = Decrypt_{AES}(k, C_{EHR}) \tag{4}$$

This ensures fine-grained, policy-compliant access to sensitive health data, while maintaining patient privacy and avoiding direct data exposure on the blockchain or to intermediaries.

4.4 Auditing and Anomaly Detection using SIEM and Random Forest.

Security Information and Event Management (SIEM) is a security solution that collects, aggregates, and analyzes logs from multiple sources in real time. It helps organizations detect suspicious activities, ensure compliance, and respond to potential threats quickly [54]. By centralizing event data, SIEM provides visibility and enhances incident management.

Random Forest (RF) is a machine learning algorithm that builds multiple decision trees and combines their results for more accurate predictions. It is widely used for classification and anomaly detection due to its robustness and ability to handle large datasets [55]. The ensemble approach reduces errors and improves model reliability.

Once access to the EHR is granted and executed, the system proceeds to log the event immutably and monitor for abnormal activity. It is accomplished through the combination of SIEM technology and a trained RF predictive model against historical access logs. It serves to achieve post-access verification, detect insider threats, and thwart misuse.

- All access events E are logged as:

$$E = \{UserID, Timestamp, AccessType, ResourceID, DecisionReceipt, Location\} \tag{5}$$

- The SIEM engine aggregates logs in real-time and feeds them into the RF classifier:

$$y = f_{RF}(E) \in \{normal, anomaly\} \tag{6}$$

- If an anomaly is detected, the token's accumulator witness is revoked, and future access attempts are blocked.

The detection of anomalies using SIEM and RF ensures a highly reactive system response to misuse, enforces post-hoc accountability, and integrates machine learning-based behavioral analysis within access management.

4.5 Emergency Access via Break-Glass Mechanism

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In situations where urgent access to patient data is required, such as during medical emergencies, the system incorporates a break-glass mechanism. This process allows predefined stakeholders to override normal access controls temporarily, but only through a t-of-n multi-party approval system. The access is granted in a controlled, time-limited, and auditable manner, with encrypted justifications stored for post-event review.

- **Threshold Approval**:
- **Access is permitted only when at least t out of n trusted parties approve the override request:**

i=1

$$\delta i \geq t \ \ where \ \delta_i = \begin{cases} 1, & if\ approved\ by\ stakeholder\ i \\ 0, & otherwise \end{cases} \quad (7)$$

- **Encrypted Justification**: The reason for emergency access is encrypted and logged:

$$J = Encrypt_{pkAudit}(Justification) \quad (8)$$

- **Access Expiry**: The granted access is revoked automatically after a preset timeout window (e.g., 30 minutes).

This mechanism ensures that life-critical access is not obstructed, while still preserving security, accountability, and transparency in emergency data use.

4.6 Analytics Access with Differential Privacy (DP) Enforcement

In scenarios where healthcare data is requested for research, audit, or statistical analysis rather than direct patient care, the system enables privacy-preserving analytical access. This is executed through a DP layer that ensures statistical insights can be shared without exposing individual patient records. The system first verifies the legitimacy of the request using the signed decision receipt, then applies calibrated noise before releasing any output, thereby ensuring formal privacy guarantees. Given a query function f over database D, the DP mechanism releases:

$$f(D) = f(D) + N(0, \sigma^2) \quad (9)$$

Where $N(0,\ \sigma^2)$ is Laplace or Gaussian noise, and σ is calibrated to the desired privacy budget ε. The final analytics output is signed and issued along with a DP receipt, which includes:

$$R = \{Query_{ID}, \varepsilon, NoiseType, SignerID, Timestamp\} \quad (10)$$

DP ensures data utility is preserved for analytical use while preserving patient-level privacy intact and in accord with regulations like HIPAA and GDPR. It is a powerful, module-based, policy-driven mechanism for controlling access. By deploying a mix involving immutability in blockchain, ZKP, attribute-based encryption, anomalous detection, and differential privacy, it ensures scalable, transparent, and secure healthcare data access within cloud-based systems.

4.7 Proposed methodology

In this section, Figure 3 presents the suggested methodology providing secure access control within cloud-based healthcare systems while using Hyperledger Fabric. Patient-defined policies remain permanently on the blockchain, while doctors must provide ZKPs to be granted access. A verification that is successful yields a short-term ability token along with an accumulator witness, enabling EHRs to decrypt using CP-ABE and PRE. An Audit Manager logs

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

all access events, and anomaly detection is performed using SIEM and RF. In emergencies, a Break-Glass mechanism with t-of-n approvals allows temporary access, while analytics requests trigger Differential Privacy (DP) verification before issuing signed DP receipts. This framework ensures decentralized, privacy-preserving, and auditable access control in cloud environments.

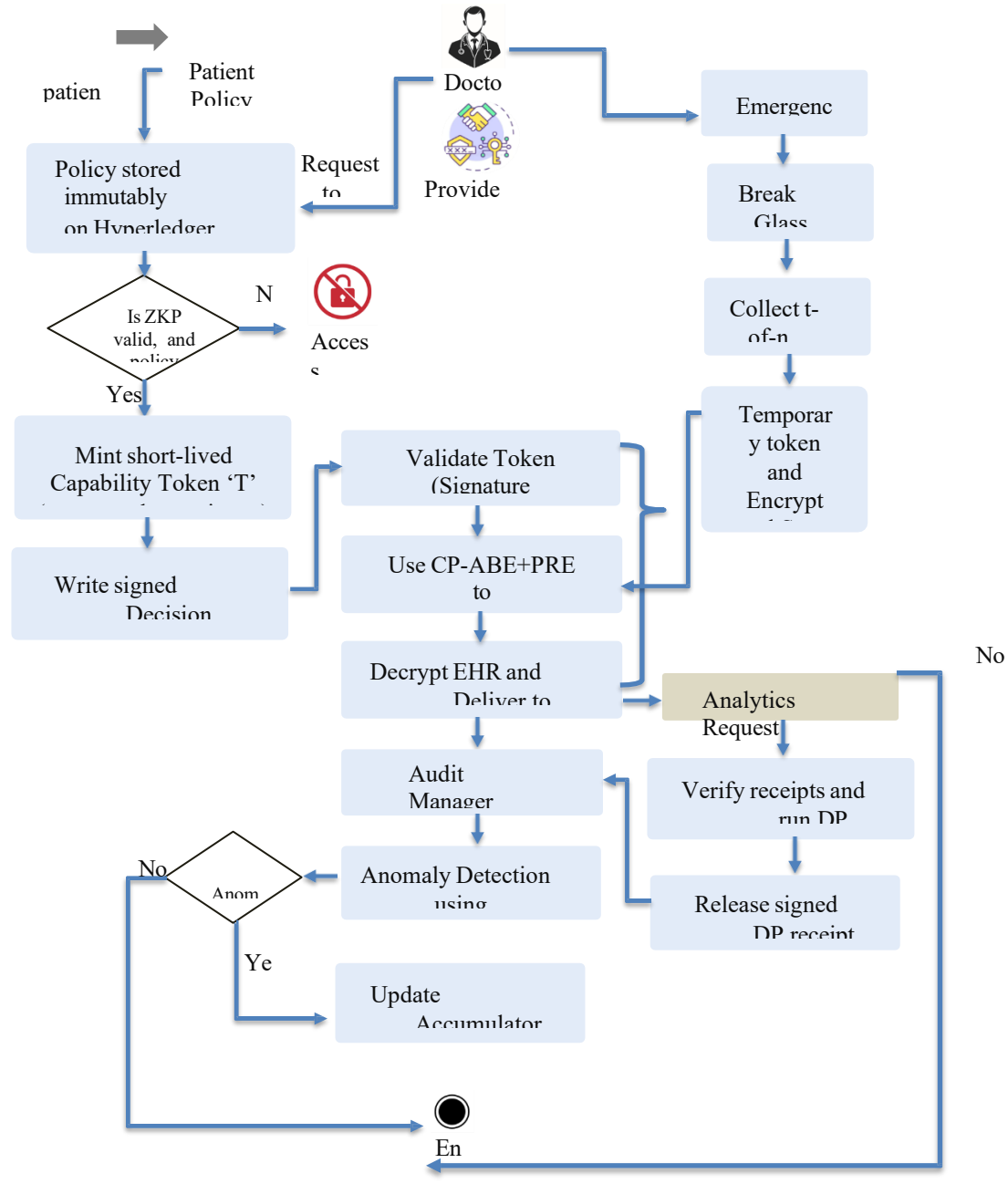


Figure 3: Flowchart for the proposed methodology

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4.8 Proposed Sequence Diagram

In Figure 4, the sequence diagram illustrates the end-to-end workflow of the proposed access management framework that integrates Hyperledger Fabric, Cloud Adapter, CP-ABE/PRE, Break-Glass, and SIEM/AI-driven monitoring. It shows the interactions between the main actors (Patient and Doctor) and the system components across three scenarios:
Normal Flow

- The doctor requests access to patient data.
- The patient policy, stored immutably on Hyperledger Fabric, is checked.
- The doctor provides a ZKP to prove identity without revealing credentials.
- If valid, the system mints a short-lived capability token and issues a signed receipt.
- The token is validated, and then CP-ABE + PRE decrypts the AES key.
- Finally, the EHR is delivered securely to the doctor.

Emergency Case

- When urgent access is required, the doctor initiates an emergency request.
- The Break-Glass Manager collects approvals (t-of-n consensus).
- A temporary access token is granted, with justification encrypted and logged.
- The access automatically expires after a time window to maintain accountability.

Audit & Security.

- Every transaction is immutably logged by the Audit Manager.
- SIEM + Random Forest models continuously analyze logs for anomalies.
- If suspicious activity is detected, the user's token is revoked and future access blocked.
- For analytics/research access, the framework applies Differential Privacy (DP) before releasing aggregate insights, protecting individual patient data.

Key Participants in the Diagram

Patient – Defines and owns the access policies for their Electronic Health Records (EHRs).

Doctor – Requests access to patient EHRs (normal, emergency, or analytics).

Hyperledger Fabric (Blockchain Layer) – Stores immutable access policies, executes smart contracts, validates Zero-Knowledge Proofs (ZKP), and issues capability tokens.

Cloud Adapter – Acts as a bridge between blockchain and AWS cloud storage.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cryptographic Modules (CP-ABE & PRE) – Enforce fine-grained policy-based encryption/decryption of EHRs.

SIEM + Random Forest (Anomaly Detection) – Monitors logs in real-time for misuse or insider threats. **Break-Glass Manager** – Provides controlled override for emergency access, with multi-party approval. **Audit Manager** – Logs and monitors all events for accountability.

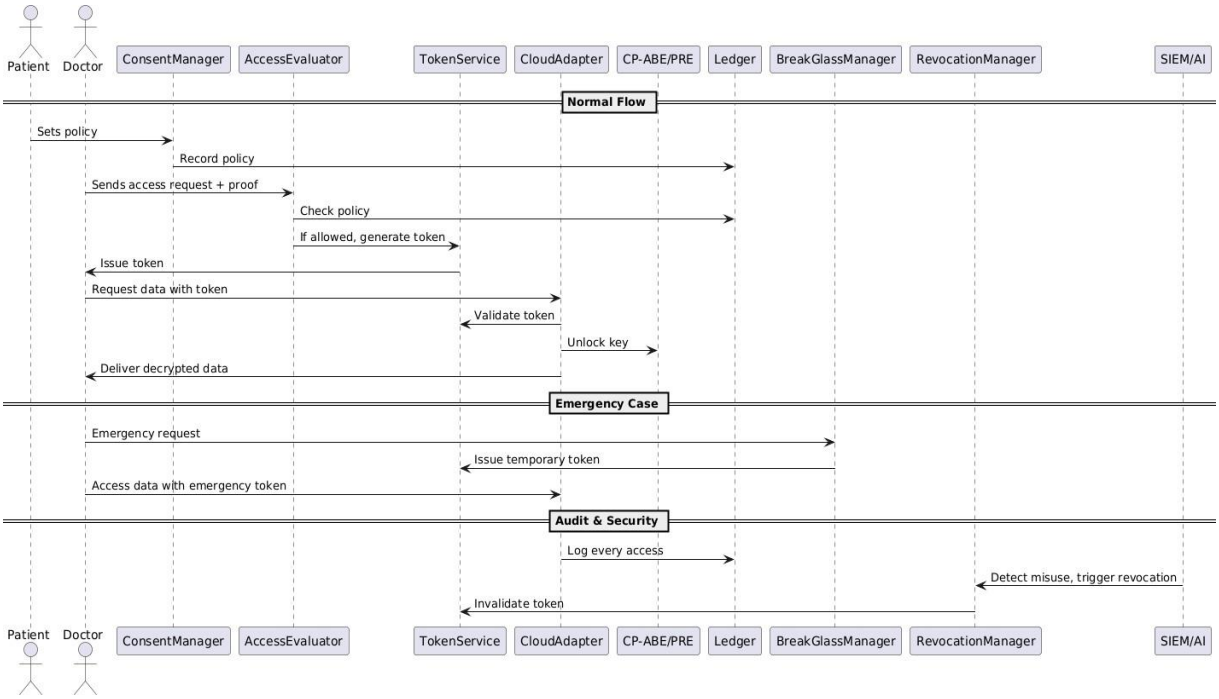


Figure 4: Sequence Diagram

4.9 Algorithm

In this section, the proposed algorithm for the proposed methodology for securing cloud infrastructure through Hyperledger fabric-based access management is presented.

Input:

- u_i: requesting doctor
- pat: patient identity
- r_j: requested record (EHR)
- a: requested action (read/write/analytics)

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Output:

- Access decision, transaction receipt, or denial

Function AccessRequest(u_i, pat, r_j, a):

Step 1: The Doctor provides Zero-Knowledge Proof (π)

If VerifyZKP(u_i, π) == False OR PolicyMatch(u_i, pat, a) == False then Log("Access Denied", u_i, pat, a)

Return "Denied" End If

Step 2: Mint short-lived Capability Token T

T ← CreateToken(u_i, pat, r_j, a, AccumulatorWitness(u_i))

$Receipt_0$ ← SignIssuer(T) Log("Token Issued", u_i, pat, a)

Step 3: Validate Token

If ValidateToken(T) == False then Log("Invalid Token", u_i, pat, a) Return "Denied"

End If

Step 4: Key Unwrapping using CP-ABE/PRE AESKey ← CP_ABE_PRE_Decrypt(T, C_ABE) If AESKey == NULL then

Log("Key Decryption Failed", u_i, pat, r_j) Return "Denied"

End If

M ← AES_Decrypt(AESKey, C_AES) Deliver(M, u_i)

Log("Record Delivered", u_i, pat, r_j) Step 5: If a == "Analytics" then

VerifyReceipts(u_i, pat, r_j) y ← RunQuery(M)

$\tilde{y}$ ← ApplyDifferentialPrivacy(y, ε, Δf) Receipt_DP ← SignIssuer($\tilde{y}$, ε, Δf) Log("DP Analytics Released", u_i, pat) Return $\tilde{y}$

End If

Step 6: Audit and Anomaly Detection LogEvent(u_i, pat, r_j, a)

score ← AnomalyDetection(u_i, context) If score ≥ θ then

RevokeUser(u_i) UpdateAccumulator(u_i) Log("Revocation Triggered", u_i)

End If

Step 7: Expiry & Cleanup

If CurrentTime ≥ TokenExpiry(T) then InvalidateToken(T)

Log("Token Expired", u_i)

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

```
    Return "Access Granted with Receipt"
End Function
```

5. Results and Discussion

This section highlights and discusses the results of the research and assessment metrices that are employed. It also offers a comparative study assessing the system's performance against previous approaches.

5.1 Evaluation Matrices

Evaluation matrices are numerical parameters used in analyzing a system or model's performance. Such matrices facilitate the assessment of experimental findings and act as a sound methodology to evaluate differing methods or techniques. Metrices used in research work to analyze levels of proposed model performance are throughput, latency, response time, and accuracy.

$$Throughput = \frac{Number\ of\ transactions\ completed\ successfully}{Time\ taken} \tag{11}$$

$$Latency = End\ Time - Start\ Time \tag{12}$$

$$Response\ Time\ (RT) = Time\ of\ Output - Time\ of\ Input \tag{13}$$

$$Accuracy: TP + TN/TP + TN + FP + FN \tag{14}$$

5.2 Experimental setup

The experimental setup configuration is shown in Table 1, comprising 5 ordered nodes and 4 peer nodes distributed across 2 organizations. Each node is equipped with a 32-core CPU, 128 GB RAM, and 1 TB NVMe SSDs, connected through a 10 Gbps LAN. The system runs on Ubuntu 22.04 LTS with Raft consensus, a batch size of 500 transactions per block, and a batch timeout of 2 seconds.

Table 1: Experimental setup configuration

Component	Specification
Hardware	5 Orderer Nodes, 4 Peer Nodes (2 Orgs), 32-core CPU, 128 GB RAM
Storage	NVMe SSDs (1 TB)
Network	10 Gbps LAN
Operating System	Ubuntu 22.04 LTS
Batch Size	500 Transactions per block
Batch Timeout	2 seconds
Consensus Mechanism	Raft
Channel Configuration	Single Channel, Two Organizations, Anchor Peers Enabled

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

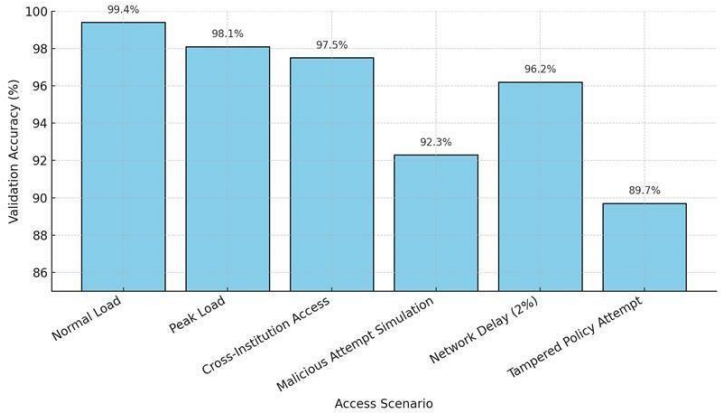


Figure 5: ZKP Validation Accuracy

5.3 Result Analysis

Result analysis is an essential phase in research, data-centric projects, or any experimental investigation. It encompasses the data analysis, interpretation, and explanation as well as reasoning for the findings from the study or experiment. Result analysis aims to explain data in a meaningful way, determine key insights, and assess whether the objectives or the working hypotheses of the study have been accomplished. Below is an analysis of the results and the accompanying systematic outcome assessment for the proposed methodology.

5.3.1 Performance Analysis

Assessing the use of Hyperledger Fabric for access management in a cloud-computing setting illustrates its capability to secure the AWS infrastructure. The analysis of performance presents critical factors, including throughput, latency, and response time of the system's transaction processing capabilities.

- **ZKP Validation**

The ZKP validation results demonstrate strong accuracy across varied scenarios as depicted in Figure 5. Under normal load, accuracy reached 99.4 percent and remained high at 98.1 percent during peak load and 97.5 percent in cross-institutional access. In more challenging conditions, accuracy was 92.3 percent under malicious attempt simulation,

96.2 percent with a 2 percent network delay, and 89.7 percent for tampered policy attempts. Overall, the results confirm that the framework maintains reliable validation performance even under stress, ensuring secure and trustworthy access control.

This validates Hypothesis 1 by demonstrating the robustness of ZKP in providing secure and trustworthy identity validation while maintaining high performance, even under stress conditions.

- **Token Revocation Time**

Experimental testing of token management in the designed system for cloud-based access control shows consistent performance in fluctuating conditions, as shown in Figure 6. With regular operations, token revocation took around

0.8 seconds, ensuring quick response and minimal risk. With a burst load scenario, it attained up to 1.2 seconds, while

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

in a cross-organization setup, the overhead raised this to 1.5 seconds. Network stress further impacted performance such that packet loss of 1% caused a 1.7-second lag and 3% maximum peak at 1.9 seconds. Though environmental setups caused small delays, the system showed consistent revocation all the time, ensuring extensibility, resilience, and operational viability, hence validating the soundness of the Hyperledger Fabric-based cloud healthcare environment access control system.

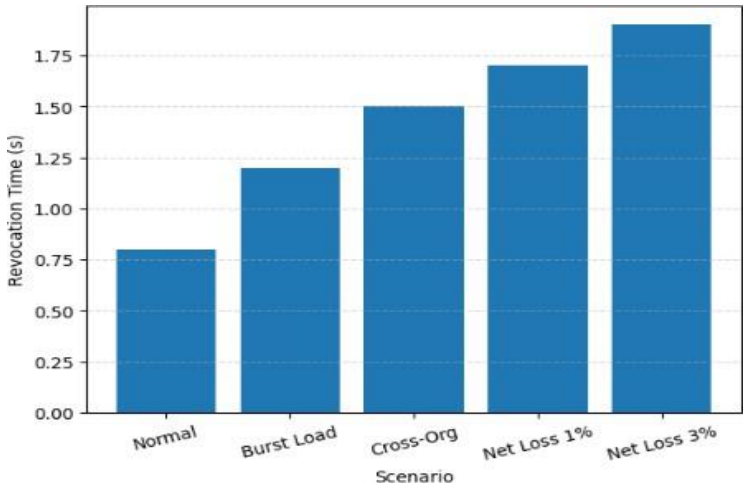


Figure 6: Token Revocation Time

This confirms that the framework maintains efficient token revocation, even under network stress, validating Hypothesis 2 by showing that the system can handle access control operations efficiently under varying conditions.

- **Cloud Access Time**

Measurements of cloud access time against concurrent users have been tabulated in Table 2 below, wherein the latency measurements both at the p50 and p95 levels are considered. This validates Hypothesis 2 by confirming the system's scalability and predictable performance as the number of concurrent users increases, ensuring that access times remain manageable. With 100 users, the system reached a p50 latency of 320 ms and a p95 latency of 540 ms. With 200 users, these increased to 410 ms (p50) and 640 ms (p95). With 400 users, latency increased again to 520 ms (p50) and 780 ms (p95). Later on, at maximum utilization of 800 users, the system was measured at 690 ms for p50 and 980 ms for p95.

Table 2: Cloud Access Time vs Concurrent Users

Concurrent Users	**Cloud Access Time**	
	p50 latency (ms)	**p95 latency (ms)**
100	320	540
200	410	640

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

400	520	780
800	690	980

This evaluation of latency confirms that latency increases proportionally with user load. Yet, the system maintains predictable scalability and efficient performance, making it well-suited for real-time cloud-based access control scenarios.

- **Privacy Preservation Analysis**

The privacy preservation analysis highlights how different access control techniques contribute to safeguarding sensitive data (see Figure 7). Using CP ABE alone provided 91.3 percent privacy, which improved to 94.2 percent when combined with PRE. Adding ZKP further enhanced privacy to 97.8 percent, and the highest preservation of 99.1 percent was achieved when ZKP, CP-ABE, PRE, and DP receipts were integrated. With break-glass control, which is designed for emergencies, privacy slightly decreased to 95.6 percent but still remained high.

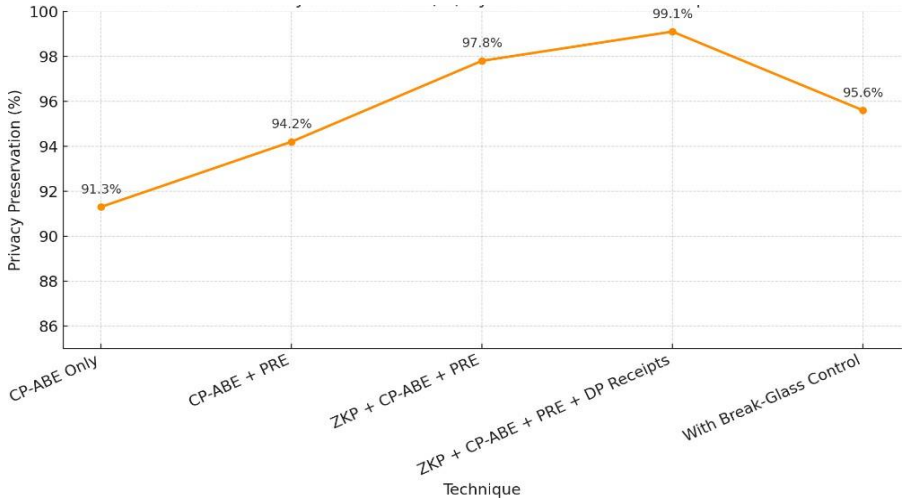


Figure 7: Privacy Preservation Analysis

These results confirm that layered approaches combining cryptographic controls, privacy receipts, and ZKP deliver the strongest guarantees, while emergency mechanisms maintain a balance between accessibility and privacy. This validates that integrating cryptographic techniques significantly enhances privacy, supporting Hypothesis 1 about blockchain-based frameworks offering superior privacy protection compared to traditional models.

- **Encryption and Decryption Time**

The encryption and decryption analysis shows that processing time increases steadily with larger EHR sizes. At 0.5 MB, encryption took 19 ms and decryption 13 ms, while at 20 MB, encryption rose to 49 ms and decryption to 36 ms, as shown in Figure 8. Although encryption consistently required slightly more time, both operations remained efficient and within acceptable limits, confirming the framework's scalability and suitability for secure real-time healthcare applications.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

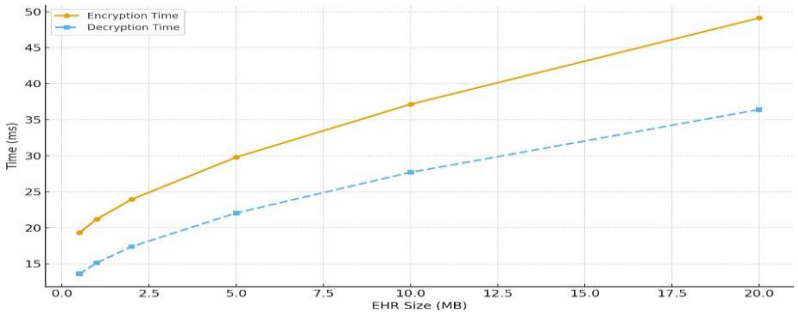


Figure 8: Encryption and Decryption analysis shows

- **Storage Cost Analysis**

The storage cost analysis demonstrates a clear linear relationship between EHR size and the total storage required within the proposed model (see Figure 9). For smaller records of around 0.5 MB, the storage requirement was approximately 1 MB, while at 5 MB the storage grew to nearly 6 MB, and for 10 MB records it reached around 12 MB. At the largest tested size of 20 MB, the storage requirement peaked at about 22 MB. This steady and predictable increase indicates that the system manages encryption metadata, logs, and policy receipts efficiently without adding disproportionate overhead and validates Hypothesis 2 by demonstrating that the framework's storage utilization remains efficient and predictable, even as data sizes grow.

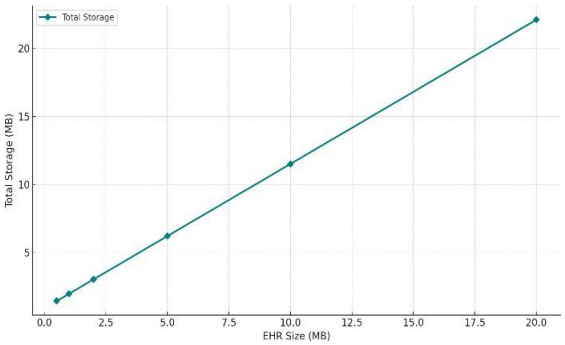


Figure 9: Storage Cost

The results highlight that as the size of healthcare records grows, the framework scales proportionally, making it suitable for managing large volumes of EHR data while keeping storage utilization practical and cost-effective.

- **Throughput vs Transaction**

Figure 10 illustrates the throughput performance of Hyperledger Fabric over AWS infrastructure as a function of increasing transaction batch sizes. It is observed that, in the early phase, the throughput increases very fast with an increase in batch size from 0 to approximately 2000 transactions, reflecting good utilization of resources and

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

processing. After this, throughput saturates at around 15,000 transactions per second and increases in batch size thereafter, offering decreasing returns. The figure also shows that for the range of 4000-6000 transactions, Hyperledger Fabric has obtained its optimal performance. To ensure access management for secured AWS infrastructure, consistent throughput under heavy loads is obtained, which signifies the robustness as well as scalability of Hyperledger Fabric for cloud-based blockchain systems.

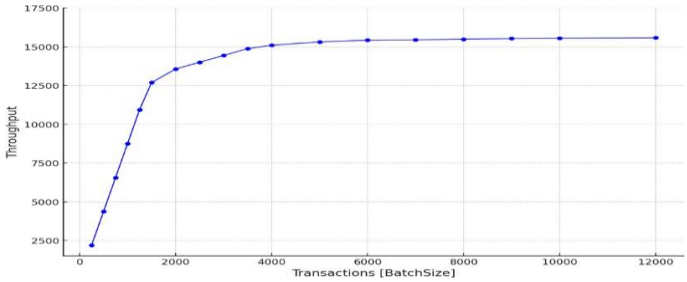


Figure 10: Throughput Concerning Transactions

- **Latency vs Transaction**

The visual representation in Figure 11, securing AWS infrastructure for access management, demonstrates the latency performance of Hyperledger Fabric with rising transaction loads. As the figure shows, at 50 transactions, the latency is low, which stands at approximately 150 ms. It gradually increases with rises to 100 and 150, and still stands below 200 ms. This goes on to indicate that moderate loads can be handled efficaciously. However, the latency increases dramatically from 200 transactions to about 350 ms. This emphasizes the importance of optimized transaction management in reducing latency and protecting AWS infrastructure in cloud-based blockchain settings by suggesting that the time taken to process certain transactions increases with load. The total task latency recorded is 2.1 seconds, with the IAM process contributing approximately 350 ms. Considering the security enhancements provided by blockchain-based IAM mechanisms, this level of latency is regarded as a reasonable trade-off for secure enterprise cloud environments.

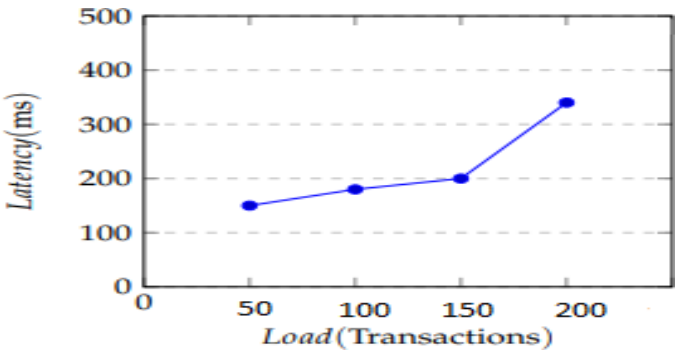


Figure 11: Latency Concerning Transaction

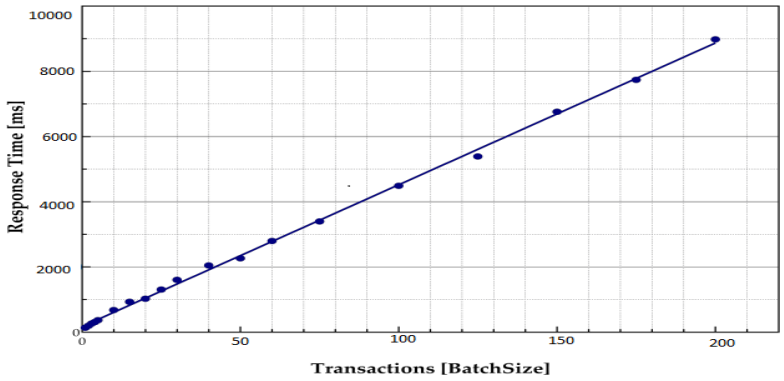
This supports Hypothesis 2 by showing that the system can process high volumes of transactions with low latency, confirming its scalability and efficiency in real-world environments.

- **Response Time vs Transaction**

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The performance of Hyperledger Fabric on AWS infrastructures with the rise of transaction batch size has been depicted in Figure 12. Response time can be seen to follow an upward linear trend, with proportional increase with increasing batch sizes, and at lower batch sizes, it remains at minimum values, thus indicating the efficiency of processing. However, with growing transactions above 100, the response time significantly goes up and reaches approximately 9000 ms at a batch size of 200. It shows that increasing the batch size also means a trade-off in the delay caused by the system processing. Ensuring that the AWS infrastructure is secured keeps the system stable in heavy loads, while batch sizes should be adjusted to reach a balance between throughput and response time for the cloud-based access management systems.

Figure 12: Response Time Concerning Transaction



- **Results based on access control**

Figure 13 illustrates a simulated analysis of access control events focusing on immutability and auditability using Hyperledger Fabric. It records 18,000 authentication logs, 15,000 permission grants, 12,000 revocations, and 4,500 audit queries within 24 hours. Notably, there were zero tamper attempts, showcasing the strong integrity and security of the system's audit logs. The data highlights the blockchain-based system's capability to ensure comprehensive access tracking and resistance to unauthorized modifications, thereby reinforcing the effectiveness of the proposed approach in secure identity and access management.

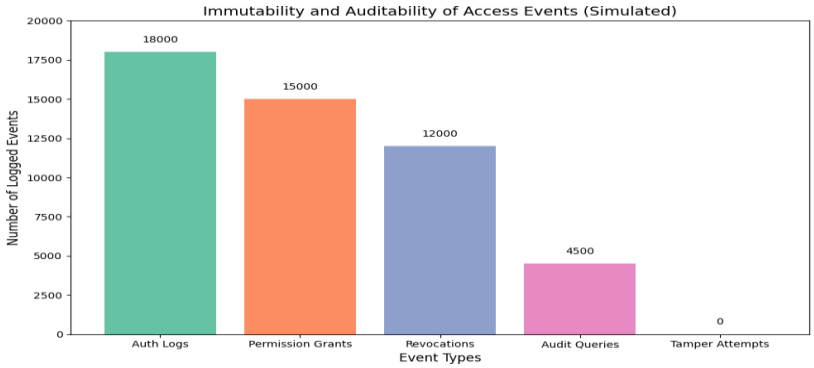


Figure 13: Immutability and auditability of access events

The tamper-proof audit logs validate Hypothesis 1 by confirming that the blockchain framework enhances the auditability and integrity of access control data, a key advantage over centralized IAM models.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- **ROC**

The anomaly detection capability of the proposed framework was further validated through the ROC analysis, which demonstrated its strong effectiveness in distinguishing between normal and malicious access events. As shown in Figure 14, the model consistently maintained a high True Positive Rate (TPR) while keeping the False Positive Rate (FPR) extremely low, resulting in an AUC score of 0.991. The anomaly detection accuracy rate is 99.63%, which is much higher. This near-perfect classification performance highlights that the integration of SIEM with Random Forest ensured highly reliable anomaly detection within the Hyperledger Fabric-based access control system.

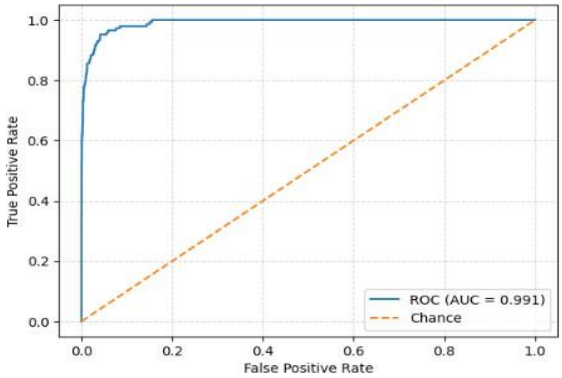


Figure 14: ROC analysis

These results flow directly with the overall objectives of the work, establishing that the framework not only manages secure access through blockchain and cryptographic controls but also strengthens resilience by detecting and mitigating anomalous behavior in real time, which is crucial for cloud-based healthcare environments.

5.3.2 Comparative Analysis

This section discusses how well the proposed approach performs compared to previous studies in terms of the throughput and latency that are obtained.

- **Comparison based on throughput**

The throughput of 15,000 TPS for the proposed system when implemented under the Hyperledger Fabric surpasses earlier studies, which reported 508 TPS, 3,500 TPS, and 14,200 TPS in Honar et al. (2021) [24], Ghosh et al. (2023) [54], and Thantharate and Thantharate (2023) [55], as shown in Table 3. This exceptionally high throughput is primarily attributed to the optimized experimental setup, particularly the use of a large batch size of 500 transactions per block combined with a batch timeout of 2 seconds. The throughput comparison of the proposed model of Blockchain technology based on Hyperledger Fabric with the model performance of early studies for Access, Security, and Data Management Applications is depicted in Table 3.

Table 3: Throughput Comparison

Study	Throughput (TPS)
Hyperledger Fabric with IoT Edge Security [24]	3,500

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Hyperledger Fabric [56]	508
ZeroTrustBlock [57]	14,200
Blockchain technology based on Hyperledger Fabric [Proposed]	15,000

- **Comparison based on latency**

A latency comparison of a proposed model of Blockchain technology based on Hyperledger Fabric with model performance of early studies for Access, Security, and Data Management Applications is shown in Table 4. The latency of the proposed Hyperledger fabric system is 350 ms, which is significantly smaller than the 2,109 ms in Honar et al. (2021) [24] and the 3,710 ms in Ghosh et al. (2023) [54], indicating faster reaction times. In Thantharate and Thantharate (2023) [55], the latency was found to be 480 ms; however, the proposed approach here provides even better performance when it comes to dealing with transaction delays.

Table 4: Latency Comparison

Study	Latency (ms)
Hyperledger Fabric with IoT Edge Security [24]	2,109
Hyperledger Fabric [54]	3,710
ZeroTrustBlock [55]	480
Blockchain technology based on Hyperledger Fabric [Proposed]	350

6. Conclusion and Future Scope

Cloud infrastructure refers to the on-demand delivery of computing resources, including storage, networking, and processing power, hosted virtually to support scalable and flexible digital operations. Due to rising security concerns in such distributed environments, this study was initiated to establish a reliable access control mechanism. The research demonstrates that integrating Hyperledger Fabric with AWS provides a highly secure, decentralized, and auditable framework for access management in healthcare-focused cloud infrastructures. Using ZKP validation, CP-ABE, PRE, and anomaly detection using ML, the system achieved exceptional performance with throughput reaching 15000 transactions per second, a latency of 350 milliseconds, and privacy preservation up to 99.1 percent. Anomaly detection attained an accuracy of 99.63 percent, while token revocation maintained efficiency even under high load and adverse network conditions. The framework ensures tamper-resistant access logs, fine-grained access control, and robust compliance, outperforming conventional IAM systems in scalability and security.

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Future research can focus on extending the framework to multi-cloud and hybrid environments, improving the energy efficiency of blockchain transactions, and incorporating advanced cryptographic methods such as homomorphic encryption and post-quantum security. Real-time performance optimization for large-scale deployments and integration with federated learning for adaptive access policies may further enhance the system. Additionally, conducting longitudinal studies in live healthcare ecosystems could validate long-term reliability, cost-effectiveness, and regulatory compliance across diverse operational contexts.

References

1. Kewate N, Raut A, Dubekar M, Raut Y, Patil A (2022) A review on AWS cloud computing technology. Int J Res Appl Sci Eng Technol 10(1):258–263. https://doi.org/10.22214/ijraset.2022.39802
2. Tihfon GM, Park S, Kim J, Kim Y-M (2016) An efficient multi-task PaaS cloud infrastructure based on docker and AWS ECS for application deployment. Cluster Comput 19:1585–1597. https://doi.org/10.1007/s10586-016-0599-0
3. Ahmad T, Morelli U, Ranise S, Zannone N (2018) A lazy approach to access control as a service (ACaaS) for IoT: an AWS case study. In: Proc 23rd ACM Symp Access Control Models Technol, pp 235–246. https://doi.org/10.1145/3205977.3205989
4. Ziegler W (2017) A framework for managing quality of service in cloud computing through service level agreements. PhD thesis, Niedersächsische Staats- und Universitätsbibliothek Göttingen. https://ediss.uni-goettingen.de/handle/11858/00-1735- 0000-002B-7D14-F
5. Google Cloud (n.d.) Compute Engine Service Level Agreement (SLA). Retrieved October 26, 2024, from https://cloud.google.com/compute/sla/
6. Google (2023) Cloud Storage Service Level Agreement. Last modified March 16, 2023. Retrieved October 26, 2024, from https://cloud.google.com/storage/sla/
7. Amazon Web Services (AWS) (n.d.) Compute Service Level Agreement (SLA). Retrieved October 26, 2024, from https://aws.amazon.com/compute/sla/
8. Amazon Web Services, Inc. (n.d.) Amazon S3 Service Level Agreement. Retrieved October 26, 2024, from https://aws.amazon.com/s3/sla/
9. Oracle (n.d.) Cloud Service Level Agreements (SLA). Retrieved October 26, 2024, from https://www.oracle.com/cloud/sla/
10. Sarmah SS (2018) Understanding blockchain technology. Comput Sci Eng 8(2):23–29. https://doi.org/10.5923/j.computer.20180802.02
11. Singh C, Thakkar R, Warraich J (2023) IAM identity access management—importance in maintaining security systems within organizations. Eur J Eng Technol Res 8(4):30–38. https://doi.org/10.24018/ejeng.2023.8.4.3074
12. Wang Y, He J, Zhu N, Yi Y, Zhang Q, Song H, Xue R (2021) Security enhancement technologies for smart contracts in the blockchain: a survey. Trans Emerg Telecommun

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Technol 32(12):e4341. https://doi.org/10.1002/ett.4341

13. Iftekhar A, Cui X, Tao Q, Zheng C (2021) Hyperledger fabric access control system for internet of things layer in blockchain- based applications. Entropy 23(8):1054. https://doi.org/10.3390/e23081054
14. Pešić S, Radovanović M, Ivanović M, Tošić M, Iković O, Bošković D (2019) Hyperledger fabric blockchain as a service for the IoT: proof of concept. In: Model and Data Engineering: 9th Int Conf, MEDI 2019, Toulouse, France, Oct 28–31, 2019, Proc 9, pp 172–183. Springer Int Publ. https://doi.org/10.1007/978-3-030-32065-2_12
15. Banoun N, Diarra N (2021) IoT-BDMS: securing IoT devices with hyperledger fabric blockchain. In: CS & IT Conf Proc 11(6). https://doi.org/10.5121/csit.2021.110604
16. Sato T, Himura Y (2018) Smart-contract based system operations for permissioned blockchain. In: 2018 9th IFIP Int Conf New Technol, Mobility Secur (NTMS), pp 1–6. IEEE. https://doi.org/10.1109/NTMS.2018.8328745
17. Dreyer J, Fischer M, Tönjes R (2021) Towards configuring Hyperledger Fabric 2.0 blockchain platform for Industry 4.0 applications. In: 2021 IEEE Int Conf Ind 4.0, Artif Intell Commun Technol (IAICT), pp 241–247. IEEE. https://doi.org/10.1109/IAICT52856.2021.9532547
18. Sujihelen L (2023) An efficient chain code for access control in hyper ledger fabric healthcare system. e-Prime Adv Electr Eng Electron Energy 5:100204. https://doi.org/10.1016/j.prime.2023.100204
19. Kadaskar HR, Kamthe VR (2024) An overview of AWS. Int J Sci Res Mod Sci Technol 3(7):22–30. https://doi.org/10.59828/ijsrmst.v3i7.223
20. Centobelli P, Cerchione R, Del Vecchio P, Oropallo E, Secundo G (2022) Blockchain technology for bridging trust, traceability, and transparency in the circular supply chain. Inf Manag 59(7):103508. https://doi.org/10.1016/j.im.2021.103508
21. Song J, Zhang P, Alkubati M, Bao Y, Yu G (2022) Research advances on blockchain-as-a-service: architectures, applications, and challenges. Digital Communications and Networks 8(4):466–475. https://doi.org/10.1016/j.dcan.2021.02.001
22. Khan S, Gani A, Wahab AWA, Bagiwa MA, Shiraz M, Khan SU, Buyya R, Zomaya AY (2016) Cloud log forensics: foundations, state of the art, and future directions. ACM Comput Surv 49(1):1–42. https://doi.org/10.1145/2906149
23. Amar M, Lemoudden M, El Ouahidi B (2016) Log file's centralization to improve cloud security. In: 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), pp 178–183. https://doi.org/10.1109/CloudTech.2016.7847696
24. Honar Pajooh H, Rashid M, Alam F, Demidenko S (2021) Hyperledger Fabric blockchain for securing the edge Internet of Things. Sensors 21(2):359. https://doi.org/10.3390/s21020359

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

25. Sabir A, Shahid A (2023) Effective management of hybrid workloads in public and private cloud platforms. Master's thesis, University of Stavanger.
26. Alshammari ST, Alsubhi K, Aljahdali HMA, Alghamdi AM (2021) Trust management systems in cloud services environment: taxonomy of reputation attacks and defense mechanisms. IEEE Access 9:161488–161506. https://doi.org/10.1109/ACCESS.2021.3132580
27. Ali A, Bhatti BM (2024) Spies in the Bits and Bytes: The Art of Cyber Threat Intelligence. CRC Press.
28. Elghoul MK, Bahgat SF, Hussein AS, Hamad SH (2024) Performance analysis of a Hyperledger-based medical record data management using Amazon Web Services. Int J Adv Comput Sci Appl 15(8). https://doi.org/10.14569/IJACSA.2024.015082
29. Kakarlapudi PV, Mahmoud QH (2021) Design and development of a blockchain-based system for private data management. Electronics 10(24):3131. https://doi.org/10.3390/electronics10243131
30. Sotenga PZ, Djouani K, Kurien AM (2020) Media access control in large-scale Internet of Things: a review. IEEE Access 8:55834–55859. https://doi.org/10.1109/ACCESS.2020.2982357
31. Khanna A, Sah A, Bolshev V, Burgio A, Panchenko V, Jasiński M (2022) Blockchain–cloud integration: a survey. Sensors 22(14):5238. https://doi.org/10.3390/s22145238
32. Sutradhar S, Karforma S, Bose R, Roy S, Djebali S, Bhattacharyya D (2024) Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: a blockchain-based approach for security and scalability for the healthcare industry. Internet of Things and Cyber-Physical Systems 4:49–67. https://doi.org/10.1016/j.iotcps.2023.07.004
33. Elghoul MK, Bahgat SF, Hussein AS, Hamad SH (2023) Management of medical record data with multi-level security on Amazon Web Services. SN Appl Sci 5(11):282. https://doi.org/10.1007/s42452-023-05502-9
34. Saah AEN, Yee JJ, Choi JH (2023) Securing construction workers' data security and privacy with blockchain technology. Appl Sci 13(24):13339. https://doi.org/10.3390/app132413339
35. Shammar EA, Zahary AT, Al-Shargabi AA (2022) An attribute-based access control model for the Internet of Things using Hyperledger Fabric blockchain. Wirel Commun Mob Comput 2022:6926408. https://doi.org/10.1155/2022/6926408
36. Shih D-H, Wu T-W, Shih M-H, Chen G-W, Yen DC (2022) Hyperledger Fabric access control for industrial Internet of Things. Appl Sci 12(6):3125. https://doi.org/10.3390/app12063125
37. Gohar AN, Abdelmawgoud SA, Farhan MS (2022) A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. IEEE Access 10:92137–92157. https://doi.org/10.1109/ACCESS.2022.3202902

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

38. Elghoul MK, Bahgat SF, Hussein AS, Hamad SH (2022) Secured cloud-based framework for electronic medical records using Hyperledger blockchain network. Egyptian Comput Sci J 46(2).

39. Gaur N, O'Dowd A, Novotny P, Desrosiers L, Ramakrishna V, Baset SA (2020) Blockchain with hyperledger fabric: Build decentralized applications using hyperledger fabric 2. Packt Publishing Ltd

40. Qureshi KN, Shahzad L, Abdelmaboud A, Elfadil Eisa TA, Alamri B, Javed IT, Al-Dhaqm A, Crespi N (2022) A blockchain- based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the internet of vehicles. Applied Sciences 12(1):476. https://doi.org/10.3390/app12010476

41. Paloviita O (2022) Infrastructure as Code for Managed Service Providers: A Case Study

42. Cai L, Li Q, Liang X (2022) Advanced Blockchain Technology: Frameworks and Enterprise-Level Practices. Springer Nature. https://doi.org/10.1007/978-981-19-3596-1

43. Müller C, Brandenburger M, Cachin C, Felber P, Göttel C, Schiavoni V (2020) TZ4Fabric: Executing smart contracts with ARM TrustZone: (Practical experience report). In: 2020 International Symposium on reliable distributed systems (SRDS), pp 31-40. IEEE. https://doi.org/10.1109/SRDS51746.2020.00011

44. Gochhayat SP, Shetty S, Mukkamala R, Foytik P, Kamhoua GA, Njilla L (2020) Measuring decentralism in blockchain-based systems. IEEE Access 8:178372-178390

45. Foschini L, Gavagna A, Martuscelli G, Montanari R (2020) Hyperledger fabric blockchain: Chaincode performance analysis. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), pp 1-6. IEEE. https://doi.org/10.1109/ICC40277.2020.9149080

46. Andrade-Salinas G, Salazar-Chacon G, Vintimilla L-M (2020) Integration of IoT equipment as transactional endorsing peers over a Hyperledger-Fabric blockchain network: a feasibility study. In: Applied Technologies: First International Conference, ICAT 2019, Quito, Ecuador, December 3–5, 2019, Proceedings, Part I, pp 95–109. Springer International Publishing. https://doi.org/10.1007/978-3-030-42517-3_8

47. Ahmad T, Morelli U, Ranise S, Zannone N (2022) Extending access control in AWS IoT through event-driven functions: an experimental evaluation using a smart lock system. Int J Inf Secur 21(2):379–408. https://doi.org/10.1007/s10207-021-00558- 3

48. Awaysheh FM, Aladwan MN, Alazab M, Alawadi S, Cabaleiro JC, Pena TF (2021) Security by design for big data frameworks over cloud computing. IEEE Transactions on Engineering Management 69(6):3676-3693. https://doi.org/10.1109/TEM.2020.3045661

49. Galiveeti S, Tawalbeh L, Tawalbeh M, Abd El-Latif AA (2021) Cybersecurity analysis: Investigating the data integrity and privacy in AWS and Azure cloud platforms. In: Artificial intelligence and blockchain for future cybersecurity applications, pp 329-360. Cham: Springer

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

International Publishing. https://doi.org/10.1007/978-3-030-74575-2_17

50. Mwikya J, Karani J, Obura J (2022) Secure Management of Encryption Keys for Small and Medium Enterprises in Africa: A Comparative Study. 5th KyU International Conference

51. Khoma V, Abibulaiev A, Piskozub A, Kret T (2024) Comprehensive Approach for Developing an Enterprise Cloud Infrastructure. In: CPITS, pp 201-215

52. Bazzaza MW, Salah K (2015) Using the cloud to teach computer networks. In: 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), pp 310-314. IEEE. https://doi.org/10.1109/UCC.2015.49

53. Botez R, Costa-Requena J, Ivanciu I-A, Strautiu V, Dobrota V (2021) SDN-based network slicing mechanism for a scalable 4G/5G core network: A Kubernetes approach. Sensors 21(11):3773. https://doi.org/10.3390/s21113773

54. Miloslavskaya, Natalia. "Analysis of siem systems and their usage in security operations and security intelligence centers." In *First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures*, pp. 282-

288. Cham: Springer International Publishing, 2017.

55. Aslam, Nida, Irfan Ullah Khan, Aisha Alansari, Marah Alrammah, Atheer Alghwairy, Rahaf Alqahtani, Razan Alqahtani, Maryam Almushikes, and Mohammed AL Hashim. "Anomaly detection using explainable random forest for the prediction of undesirable events in oil wells." *Applied Computational Intelligence and Soft Computing* 2022, no. 1 (2022): 1558381.

56. Ghosh S, Dutta M (2023) Indriya: Building a Secure and Transparent Organ Donation System with Hyperledger Fabric. arXiv preprint arXiv:2307.02416. https://doi.org/10.48550/arXiv.2307.02416

57. Thantharate P, Thantharate A (2023) ZeroTrustBlock: Enhancing security, privacy, and interoperability of sensitive data through ZeroTrust permissioned blockchain. Big Data and Cognitive Computing 7(4):165. https://doi.org/10.3390/bdcc7040165.

Received: August 08, 2025