B-PACIoT: A Hybrid Blockchain-Based Framework for Scalable, Secure and Privacy-Preserving EHR Management in IoT-Driven Healthcare

Salma Begum S.
Department of Computer Science and Engineering, Anna University
India
salma.aryan@gmail.com

J. Arokia Renjit
Department of Computer Science and Engineering, Jeppiaar Engineering College, India
dr.arokiarenjith@gmail.com

Chandrasekar Arumugam
Department of Computer Science and Engineering, St. Josephs College of Engineering, India
drchandrucse@gmail.com

Abstract: *Securing the Electronic Health Records (EHRs) in Blockchain based Internet of Things (IoT) healthcare systems remains a big challenge due to the computational constraints, privacy concerns, and scalability limitations. This paper introduces Blockchain-based Privacy-preserving, Access-controlled, and Cost-efficient IoT Healthcare Framework (B-PACIoT), a novel three-layer framework that uniquely integrates the zk-Rollups-based transaction batching, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) based access control, and edge-assisted Advanced Encryption Standard with 128-bit key (AES-128) decryption to deliver the scalable, privacy-preserving, and cost-efficient EHR management solutions in Blockchain and IoT driven healthcare. Unlike the existing IoT frameworks, our B-PACIoT offloads heavy decryption tasks to edge servers while maintaining the privacy using Zero-Knowledge proofs (zk-SNARKs), which is significantly reducing the computational load on IoT devices. Our framework used zk-Rollups in transaction management for enabling the aggregation of multiple access transactions into a single blockchain proof, minimizing the on-chain overhead and finally improving the throughput. Decentralized Interplanetary File System (IPFS) network is used for secure storage of encrypted EHRs and on-chain ethereum smart contracts are used to manage the metadata anchoring and fine-grained access control. Experimental results proven that, our B-PACIoT framework reduced the transaction costs by 90%, improved the retrieval efficiency by 40%, and achieved the 99.8% of fault-tolerant availability through IPFS replication. Moreover, our B-PACIoT lowers the decryption latency by 85% when compared to the traditional on-chain models. These outcomes from experiments are emphasizing that our B-PACIoT is not just technically novel and but also practically an effective solution for next-generation EHR management in IoT-driven healthcare.*

Keywords: *Blockchain-IoT integration, hybrid blockchain architecture, decentralized EHR management, privacy-preserving access control and healthcare data management.*

Received April 24, 2025; accepted October 14, 2025
https://doi.org/10.34028/iajit/23/3/10

1. Introduction

The integration of Internet of Things (IoT) and blockchain technologies into healthcare revolutionized the patient monitoring and data management activities. IoT devices, such as Electrocardiogram (ECG) monitors, pulse oximeters, and glucose sensors are emerging sources of the real-time health data, which allows the on-time interventions and personalized care of patients [3]. These sensors generated high volume of sensitive Electronic Health Records (EHRs) leading to significant challenges in data management. Traditional EHR data management systems [10], are centralized storage and legacy architectures. These are frequently vulnerable to cyber-attacks, lack of granular access control, and are unable to handle the growing data demands in IoT-based healthcare applications. In general the EHRs [10, 18], which hold sensitive information of patients, are the primary targets for cyber-attacks such as data breaches, unauthorized access, and collusion attacks [17 and 26]. In health care, it is important to keep the patient data confidential, intact, and accessible with the companion of standard laws like Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) [46].

On other hand, Blockchain technology emerged as a promising alternative for EHR storage, by offering the decentralized and tamper-resistant data management capabilities. Compared to the traditional in-house storage mechanisms, the Blockchain EHR management systems recorded the better performance in improving the data integrity, traceability, and access control [18]. Despite these significant advancements, existing blockchain and IoT-based frameworks for EHR management are facing the critical limitations [7, 18, 26], that become barriers in real-world deployment are:

- Traditional blockchain frameworks are expensive for data storing and retrieve on-chain, which leads to economic infeasibility for high-frequency EHR transactions.
- Existing blockchain networks designed with sequential transaction processing mechanisms that are facing high latency and congestion limitations, which results in poor throughput and delayed EHR access.
- Existing Attribute-Based Encryption (ABE) and Public-Key Infrastructures (PKI) are computation heavy on low-powered IoT sensors and gateways, making the frameworks impractical at the edge nodes.
- Legacy blockchain-IoT healthcare frameworks using the rigid access models (e.g., static Role-Based Access Control (RBAC)) or hardcoded policies, which are less flexible and adoptable to handle the emergencies.
- Recent blockchain-IoT frameworks offloaded the EHRs to the decentralized storage networks for efficient data management but they often lack in content integrity validation, fault tolerance and smart contract–based anchoring to ensure the HER's traceability and secure retrieval.
- Existing authentication mechanisms relies on role-based credentials or blockchain addresses for user access identification, which may expose the user identifiable information to external entities.

To address these critical challenges in blockchain-IoT healthcare, this paper presents Blockchain-based Privacy-preserving, Access-controlled, and Cost-efficient IoT Healthcare Framework (B-PACIoT) framework. This three-layer framework is designed for efficient EHR management in resource constrained IoT-blockchain healthcare to assure the privacy-preserving, access-control, and cost-efficiency. At core the framework designed with an innovative combination of zk-Rollups-based high-volume transaction optimization, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) driven access control, and AES-128 based encryption with edge-assisted decryption. These technical and architectural integrations enabled the B-PACIoT for scalable, secure and efficient management of EHRs in blockchain based IoT healthcare.

The major objectives of this framework are:

- To enhance the HER's privacy and security, adopt the Advanced Encryption Standard with 128-bit key (AES-128) for lightweight data encryption and CP-ABE-based key management for fine-grained policy enforcement.
- To enable the fine-grained access control of EHR data, enforce the advanced smart contract-based policies (AccessControl.sol) and zk-SNARK authentication.
- To improve the high volume EHR data transaction scalability, integrate the zk-Rollups and IPFS as off-chain storage.
- Experimentally evaluate the framework performance using the metrics such as latency, decryption time, throughput, and fault tolerance, with real-world datasets and adversarial simulations.

In contrary to the existing blockchain-based EHR frameworks, our B-PACIoT customized through a combination of architectural, algorithmic, and efficiency-focused innovations. Architecturally, the framework adopts a three-layer hybrid design that integrates blockchain, decentralized storage, and advanced cryptographic primitives into a cohesive structure tailored for IoT-driven healthcare environments. Algorithmically, it leverages zk-SNARKs to enable zero-knowledge verification of access requests, coupled with zk-Rollups for high-throughput, low-cost transaction batching. Efficiency is further enhanced by incorporating outsourced CP-ABE decryption, which significantly reduces the computation burden on resource-constrained IoT devices without sacrificing the fine-grained access control. In addition, a comprehensive experimental evaluation was conducted with 10,000 IoT devices data from MIT-BIH Arrhythmia Database (MIT-BIH) [33] for validating the framework's performance and attack resilience. We conducted the security tests using the standard tools like Metasploit [48] and Hyperledger Caliper [27] to evaluate the resistance of B-PACIoT against network-level attacks, data integrity issues, and access control vulnerabilities. These contributions collectively address persistent limitations in scalability, latency, and privacy were found in earlier systems.

The rest of this paper is organized as follows: section 2 covers related work of blockchain based IoT healthcare in EHR management and section 3 explains the design and architecture of B-PACIoT. Section 4 discusses about the experimental setup, while section 5 compares the performance of B-PACIoT with other frameworks. Section 6 evaluates the framework's security and attack resistance. Finally, section 7 concludes the B-PACIoT and outlines the future research directions.

2. Related Work

2.1. Blockchain Integration in IoT-Driven Healthcare

Blockchain and the IoT technologies are transforming the healthcare industry by addressing key challenges in data security, privacy, and operational efficiency. Blockchain's decentralized and transparent design enriches the EHR management, drug traceability, and the clinical trial integrity [7, 18]. On other hand, IoT enables the real-time patient monitoring and smooth communication between the healthcare providers and

patients through the connected IoT devices [3, 17]. Together, these technologies will provide a powerful framework for secure EHR data exchange among the doctors, patients and caretakers etc.

Early applications of blockchain in healthcare was focused on decentralizing the management of EHRs to prevent them from single points of failure and to reduce the data tampering, was explained by Alobaedy and Zilong *et al*. [58]. According to Saeed *et al*. Mohanakrishnan and Gokila [31], IoT takes this a step forward by allowing the continuous health data collection from wearables and sensors, which enables more interactive medical interventions. Ouchetto *et al*. [9] also highlighted that the blockchain technology strengthens the IoT healthcare by using the efficient cryptographic methods and consensus protocols to secure the EHR data and protects it from unauthorized access. In a step forward, Samantray *et al*. [45] proposed the peer-to-peer network of blockchain model for medical data distribution in IoT based e-healthcare system to assure the data tractability across the nodes. Rizzardi *et al*. [42] adopted the Hyperledger Fabric blockchain model in their IoT driven Blockchain architecture for efficient storage of medical records to prevent the records from unauthorized access and data tampering.

Despite these advantages, the scalability remains a significant hurdle in above blockchain-IoT healthcare systems, particularly when managing high transaction volumes from real-world IoT devices [17, 42]. Moreover, interoperability issues between the legacy IoT devices and modern blockchain-IoT environments make integration process more complex [7]. In addition to this, meeting the data protection regulatory requirements like HIPAA and GDPR [46] makes the data governance and sharing more complicated [18] in blockchain-IoT healthcare. To overcome these hurdles in blockchain-IoT healthcare, there was pressing need to design the state-of-the-art architectures with lightweight cryptographic protocols, scalable processing techniques and efficient blockchain storage methods.

In their research, Egala *et al*. [16] discussed the need of decentralized storage structures in healthcare which ensures the medical records are stored and shared in a secured transparent way, while protecting the data integrity and patient privacy. To achieve the decentralized control over data, former research works adopted the Hyperledger and Ethereum [27] like blockchain platforms. The log files generated from these platforms helps in creating the audit trails on-demand and EHR changes tracking. Recent research by Jun *et al*., 2025 [24] implemented sharding based blockchain model in artificial IoT healthcare applications to reduce the latency in data retrieval and to improve the memory efficiency. Subramanian *et al*. [43] designed the SHORTBLOCKS protocol for healthcare data management, which extends the blockchain as a Direct Acyclic Graph (DAG) to improve the scalability and throughput while maintaining the data security and privacy. Although decentralization improves the security and control over EHR data, continuous data generation from IoT devices making it high in volume and impractical for on-chain storage in blockchain.

2.2. Off-Chain Storage and Data Management

To address scalability limitations, recent studies [9, 16, 58] focused on solving the scalability issues in Blockchain-IoT by implementing the off-chain storage solutions like the IPFS [14, 9]. It is scalable to store the large amounts of the EHR data securely while keeping it accessible through replicas [42]. Azbeg *et al*. [8] proposed the blockchain based IoT healthcare system with proxy re-encryption and Ethereum with PoA consensus to reduce the blockchain overhead with off-chain storage facilitation. Jayabalan *et al*, [23] proposed the secure health data exchange in IoT driven blockchain architecture with ECC cryptography and IPFS off-chain management to ensure the secure communication across the heterogeneous IoT environments. Although these solutions improve scalability, they often do struggle with the advanced privacy preservation and computational burden on constrained devices.

2.3. Access Control Mechanisms in IoT Healthcare

In IoT healthcare, access control mechanism plays a pivotal role, which ensures that the sensitive patient data is stored securely and managed efficiently [8, 43]. Traditional methods like RBAC and ABAC were widely used in access control, but they encountered considerable challenges in large and constantly evolving healthcare environments. According to Xie *et al*., [53], RBAC is very easy to use and implement, but it doesn't flexible enough to handle the fast-changing user roles and security policies in healthcare. On other hand Shi *et al*. [47] notified that the ABAC is complex to implement but more flexible in handling the user roles to make access decisions firmly, which is more suitable for dynamic the IoT-based healthcare systems [8]. To tackle the limitations of these traditional access control models, researchers have designed the hybrid approaches that combine the best of both RBAC and ABAC. For example, Hamouid and Mohammediet, [20] introduced a dynamic ABAC model that can adjusted automatically to emergency situations, enabling the fine-grained access control in critical healthcare settings. Pal *et al*. [36] proposed another hybrid system that utilizes attributes, roles, and capabilities to provide a more flexible and secure access control solution for IoT-enabled healthcare systems. These new approaches aimed to simplify the authentication while ensuring the better protection for patient data in healthcare. However, these approaches still face challenges in adapting to resource-constrained IoT settings and

maintaining privacy-preserving authentication without revealing sensitive credentials.

2.4. Privacy Preservation and Zero-Knowledge Proofs

Ghassan *et al*., [21] designed a blockchain-based framework (health chain) to improve the interoperability and secure EHR management using decentralized off-line storage. Akkaoui *et al*. [2] proposed edge medi chain framework, which integrates the edge computing with blockchain to ensure traceability in medical data exchange and to ensure the data integrity and secure accessibility. Yang *et al*. [54] introduced FHIR_E framework which consists of blockchain with smart contracts to manage the healthcare data in a decentralized manner and to ensure the data integrity. Abou *et al*. [1] prepared the di trust chain which is a decentralized blockchain framework designed using the smart contracts and an Indirect Trust Inference System (ITIS) to enhance trust and interoperability in healthcare data exchange.

In their study, Pathak *et al*. [38] noticed that, to ensure the privacy and data integrity in IoT, Zero-Knowledge Proofs (ZKPs) become popular in recent because they allow the data to be verified without exposing it to any external entity. Diro *et al*. [57] proven that ZKPs are particularly useful in decentralized identity verification and access control, which provides secure the authentication of IoT user without compromising the performance. Simultaneously, the combination of federated learning with blockchain and edge computing, become a secured solution for AI model training in IoT healthcare systems. Waheed *et al*. [52] noted that, this combination allows the healthcare providers to train their AI models collaboratively without sharing the patient's sensitive data and ensuring the compliance with privacy standards. By utilizing the data in local and sharing only the model updates to external entities, the federated learning process reduces the risk of data breaching while maintaining the efficiency, which is crucial for the IoT devices with limited resources, as Myrzashova *et al*. [34] observed. Table 1 presents the key methodologies, strengths, and limitations of the existing Blockchain-IoT healthcare frameworks discussed in this literature section.

Table 1. Representative Blockchain-IoT healthcare frameworks and their limitation.

Paper/Year	Core methodology	Key strengths	Notable limitations
FHIR_E [54]	Blockchain+smart contracts for FHIR interoperability	Standards-based exchange, improved the integrity	Lacks advanced privacy techniques, no scalability optimization
DITrust Chain [1]	Blockchain trust model with ITIS	Secure device-to-device communication	Semantic gaps, integration challenges
Pathak *et al*. [38]	Blockchain+zero-knowledge proofs	Privacy preservation, scalability, fast authentication	Computational complexity for IoT devices
Waheed *et al*. [52]	Federated learning+blockchain	Privacy-preserving model training	High computational cost, vulnerable to FL-specific attacks
Jayabalan *et al*. [23]	Blockchain+ECC+IPFS (off-chain storage)	Secure, scalable, authenticated EHR sharing	Integration complexity in heterogeneous IoT
Shi *et al*. [47]	MedAccessX (blockchain access framework)	Fine-grained, cost-effective access control	Scalability limitations, high resource usage
Andaloussi *et al*. [8]	Blockchain+privacy-preserving access control	Secure and efficient access	Processing time; adaptability to dynamic contexts
HealthChain [21]	Blockchain EHR framework with off-chain storage	Interoperability, tamper-proof records	Limited scalability, lacks fine-grained revocation
EdgeMediChain [2]	Edge computing+blockchain	Faster data exchange, reduced on-chain storage	High architectural complexity

2.5. Research Gaps and Motivation

A critical review of the surveyed literature reveals several persistent limitations that control the widespread adoption of Blockchain-IoT solutions for healthcare.

1. **Scalability Limitations**: although off-chain storage solutions such as IPFS [1, 2, 54] can alleviate the on-chain data load, the combination of high transaction volumes and the large size of EHR datasets continues to strain blockchain throughput. This bottleneck becomes even more pronounced in real-time IoT environments, where multiple devices generate continuous data streams.
2. **Access Control Overhead**: fine-grained access mechanisms, particularly those based on CP-ABE [8, 47], provide strong security guarantees but impose heavy computational demands. These demands are impractical for resource-constrained IoT devices, leading to latency and energy inefficiencies.
3. **Privacy-Performance Trade-off**: advanced privacy-preserving techniques such as ZKPs and homomorphic encryption strengthen the data confidentiality [38, 57] but often limits the processing speed. For IoT edge devices with limited computational capacity, this trade-off can significantly hinder usability and scalability.
4. **Regulatory Integration**: many existing frameworks reference compliance with General Data Protection Regulation (GDPR) or HIPAA only at a high level, without explicitly mapping system components to specific regulatory clauses. This lack of demonstrable compliance reduces trust and poses challenges for real-world deployment in regulated healthcare environments.

These research gaps highlight the need for a lightweight, scalable, and privacy-preserving architecture that

supports efficient EHR management within Blockchain-IoT healthcare. The proposed B-PACIoT framework is designed to overcome these shortcomings through the novel architectural, algorithmic, and efficiency-focused innovations. Table 2 presents the detailed novelty comparison, highlighting how B-PACIoT builds upon and extends the capabilities of existing solutions.

Table 2. Novelty comparison of B-PACIoT vs. counterpart frameworks

Aspect	Health chain	Edge medi chain	FHIR_E	B-PACIoT (proposed)
Hybrid- design	Yes	Partial	Partial	Yes
Off-chain IPFS storage	No	Partial	Yes	Yes
ZKP or zk-SNARKs	No	No	No	Yes
zk-Rollups	Yes	No	No	Yes
CP-ABE access control	Yes	Yes	Yes	Yes
Outsourced decryption	No	Yes	No	Yes
Quantitative evaluation	Yes	Yes	Yes	Yes

Among the presented studies in Table 2, only our proposed B-PACIoT is simultaneously combines a three-layer architecture with IPFS off-chain storage, FHIR-aligned access, zero-knowledge authentication, zk-Rollups, CP-ABE, and outsourced decryption-positioning its novelty as architectural, algorithmic, and efficiency-focused.

3. Proposed Methodology

To overcome critical limitations identified in existing blockchain-IoT healthcare systems, in this paper we introduce a B-PACIoT. It is designed to address the scalability bottlenecks in data access, decryption overhead on edge devices, lack of dynamic access controls, and limited privacy compliance in EHRs management. The three-layered architecture of this framework (see Figure 1) consists of IoT Layer, blockchain layer and cloud layer, which are strategically integrates the lightweight encryption, decentralized storage, and privacy-preserving authentication in them. In this, IoT layer is for edge-level secure data collection and encryption, blockchain layer is for tamper-proof access control and auditability, and cloud layer is for scalable and standards-compliant data access. Each layer of this architecture is leveraged to reduce the processing load, enhance the transaction throughput, and enable the fine-grained control of EHR access.

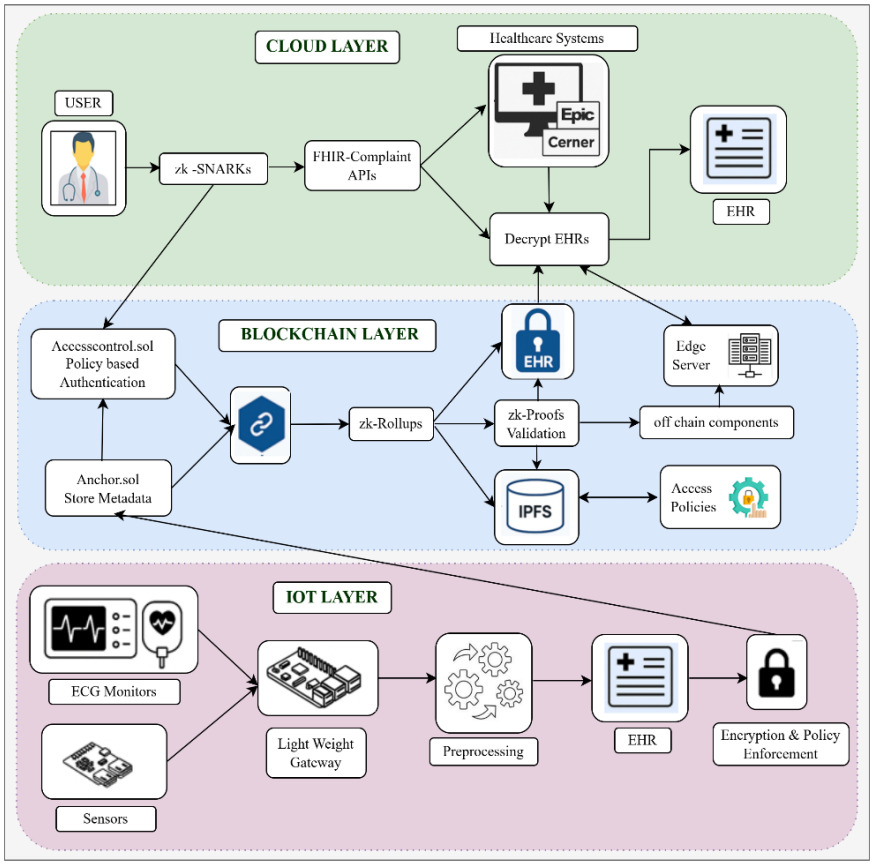

Figure 1. B-PACIoT system architecture: a secure and decentralized framework for IoT-driven electronic health records management.

3.1. Three-Layer Framework Description

1. **IoT Layer**: at this layer the IoT devices like ECG monitors and pulse oximeters are deployed to collect the real-time patient data (EHR) at the network edge. Due to the limited processing power of these devices, lightweight gateways (e.g., Raspberry Pi) are employed to preprocess the EHRs, by applying the noise filtering, normalization, and feature extraction operations. AES-128 encryption with CP-ABE edge

decryption policy [49] is designed to reduce the process burden at IoT devices and provide the secured access control to EHRs.

2. **Hybrid Blockchain Layer**: by facilitating the tamper-proof access control and decentralized EHR storage, this blockchain layer [42] serves as a bridge between the IoT Layer and the Cloud Layer. This layer has two main components are:

- **On-Chain Components**: to ensure the EHR data integrity and access control, Ethereum based smart contracts [32] like AccessControl.sol is used to administer the policy-based authentication, and the Anchor.sol is used to securely store the metadata.
- **Off-Chain Components**: encrypted EHRs are stored in IPFS off-chain file system [23] to optimize the storage efficiency and minimize the blockchain based transaction costs.

To improve the scalability in EHR access, zk-Rollups mechanism [32] combines several access transactions into one batch to reduce the transaction costs and latency, while maintaining the blockchain's security.

3. **Cloud Layer**: this layer allows secure access of EHRs via FHIR-compliant APIs [54], to enable the integration with healthcare systems like Epic and cerner [46]. Here the user place EHR access requests are validated with zk-SNARKs [6], which allows only the authorized users to retrieve and decrypt the encrypted EHRs for analysis. This mechanism ensures the scalability and privacy compliance in EHR access, while maintaining interoperability with existing healthcare IT infrastructure.

3.1.1. Process Flow in B-PACIoT

To ensure the secure EHR data encryption, decentralized storage, and privacy-preserving retrieval, our B-PACIoT system process flow is implemented in five steps as:

1. Encryption at the IoT Edge

- IoT devices encrypt the raw EHR data(M) using the AES-128 encryption and generates encrypted EHR C_{Sym} and a symmetric key K.
- Now CP-ABE scheme encrypts the key K under specified access policy A to generate the access key CT_{ABE}

2. Decentralized Storage

- The encrypted HER C_{Sym} is stored off-chain in IPFS, generating a Content Identifier (CID) H_{IPFS}.
- The Anchor.sol smart contract records H_{IPFS} and hashed access policies h(A) on-chain, to ensure the auditability and immutability.

3. Access Request Handling

- When a healthcare provider submits an EHR request, their credentials are verified against the CT_{ABE} stored in the Blockchain Layer.
- zk-SNARK authentication is used to validate the user's access rights without exposing Personally Identifiable Information (PII).

4. zk-Rollup Optimization for Scalability

- To reduce the energy costs and latency, zk-Rollups aggregate multiple EHR access transactions as a batch to execute them as a single transaction on-chain.
- This technique optimizes the EHR retrieval performance while maintaining the blockchain security guarantees.

5. EHR Retrieval and Decryption

- Once EHR access is granted, the Cloud Layer retrieves the encrypted HER C_{Sym} from IPFS using the respective CID provided by the blockchain.
- The CP-ABE-encrypted AES key *K* is sent to an edge server, which performs partial decryption of C_{Sym} before sending an intermediate decryption key to the user.
- The final decryption of C_{Sym} occurs on the provider's device, ensuring that the EHR remains private and accessible only to authorized users:

3.2. IoT Layer: Data Security and Encryption

As shown in Figure 2, the IoT layer in B-PACIoT is responsible for securely collecting the EHRs from patient, encrypting and sending them from medical IoT devices to the blockchain layer. Since the information in EHRs is so sensitive, we used hybrid dual-layer method that combines AES-128 for encryption and CP-ABE [49] for secured access control. This dual-layer technique at IoT ensures that the data stays encrypted during transmission and storage, while access is restricted to authorized used based on their access policies.

To ensure the clarity, we formally define the cryptographic primitives applied in B-PACIoT.

AES-128: AES is a block cipher standardized by NIST (FIPS-197) that operates on 128-bit blocks. In AES-128, the key length is 128 bits. In Cipher Block Chaining (CBC) mode with a random Initialization Vector (IV), the encryption of message blocks M_i is:

$$C_0 = IV, C_i = E_K(M_i \oplus C_{i-1}),\ i \geq 1 \quad (1)$$

where E_K is the AES encryption function with key K. AES-128 is widely considered secure under the pseudorandom permutation (PRP) assumption.

CP-ABE: CP-ABE is a public-key encryption mechanism that enforces access control via attributes. It is defined by four algorithms:

$$Setup(1^{\vartheta}) \rightarrow (PK, MK) \quad (2)$$

$$KeyGen(MK, S) \rightarrow SK_s \quad (3)$$

$$Enc(PK, m, A) \rightarrow CT \quad (4)$$

$$Dec(SK_s, CT) \rightarrow m \; or \; \perp \quad (5)$$

where A is an access structure over attribute set S. Security is based on the Decisional Bilinear Diffie-Hellman Exponent (DBDHE) assumption [53]. In our framework, CP-ABE encrypts only the AES symmetric key, significantly reducing computational load on IoT devices. This hybrid (AES), fine-grained policy enforcement (CP-ABE), and resource efficiency (by encrypting only the symmetric key with CP-ABE).

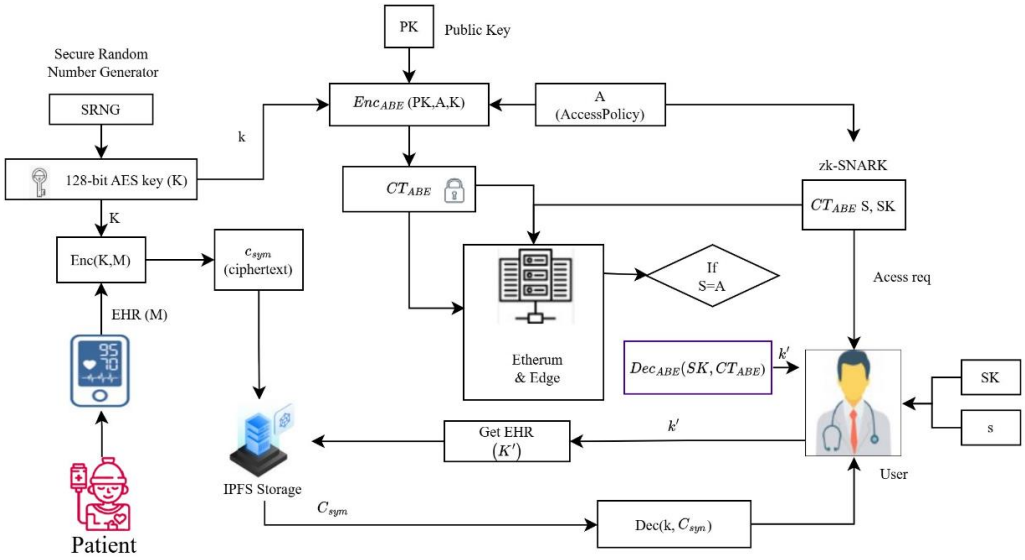

Figure 2. IoT layer: secure data collection, encryption, and transmission in B-PACIoT.

3.2.1. Secure Data Collection and CP-ABE Encryption

At IoT layer, IoT gateways (i.e., Raspberry Pi or ESP32) collects the data periodically from patient sensors and buffers it to overcome the packet loss during unstable networks [17]. These gateways improve collected data quality by filtering out noise, normalizing the values, and extracting the features [17]. Once the data is processed and structured as an EHR, it will be encrypted and sent to the blockchain layer.

To achieve the optimal security while minimizing the computational overhead, our dual layer encryption is implemented in several steps as:

1. Symmetric Key and Initialization Vector (IV) Generation

- At first the 128-bit AES key (K) is generated using a secure random number generator (SRNG).

$$K = IV = SRNG(128\ bit) \quad (6)$$

2. Encryption of EHR Data

- The patient's EHR data M is divided into 128-bit blocks as $M_1 M_2, \ldots, M_n$

$$M = (M_1, M_2, \ldots, M_n) \quad (7)$$

- Each block is encrypted using AES-128 in CBC mode:

$$C_1 = AES - Enc(K, M_1 \oplus IV) \quad (8)$$

$$C_2 = AES - Enc(K, M_2 \oplus C_1) \quad (9)$$

$$C_n = AES - Enc(K, M_n \oplus C_{n-1}) \quad (10)$$

- The final cipher text is:

$$C_{sym} = (IV, C_1, C_2, \ldots, C_n) \quad (11)$$

3. CP-ABE Encryption of AES-128 Key

- To enforce ABAC, the AES key K is encrypted using CP-ABE [49]. For this the access policy A is defined using a boolean expression as:

$$A = (role = "Doctor") \Lambda (department = "Cardiology") \quad (12)$$

- The CP-ABE setup phase generates a public key PK and a master key MK as:

$$(PK, MK) \leftarrow Setup_{ABE}(1^{\lambda}) \quad (13)$$

- The AES-128 symmetric key K is transformed into an access-controlled ciphertext as:

$$CT_{ABE} = Enc_{ABE}(PK, A, K) \quad (14)$$

- The final CP-ABE cipher text CT_{ABE} includes access policy A, symmetric key K and random elements for data invisibility to attackers.

After the hybrid encryption process completed, the EHR remains securely stored in IPFS and the CP-ABE-encrypted key is recorded on the Ethereum blockchain for access control enforcement. Only the authorized users who are satisfying the access policy A can only decrypt the CT_{ABE} to retrieve the AES key K for final decryption of the EHR. Instead of whole data, encrypting only the AES key using the CP-ABE can significantly reduce the computational burden on IoT devices, making this encryption more efficient under strict access control policies. Moreover, the outsourced decryption to IoT edge severs is eliminating the processing burden at low configured IoT devices to ensure the scalability and resource efficiency.

3.3. Hybrid Blockchain Layer: Privacy-Preserving EHR Management

The Hybrid Blockchain Layer is the second layer in B-PACIoT, which is in between the IoT and cloud layers. This layer is responsible for providing scalable, secure and privacy-compliant storage and access to the IoT layer encrypted EHRs. The main challenge with blockchain-based healthcare systems is ensuring EHR security while maintaining the efficient access policies [43]. Storing the large-scale medical records directly on a blockchain (e.g., Ethereum [32]) is impractical due to limited storage capacity and transactional delays. Former blockchain healthcare solutions [7, 9, 18, 42, 58] were struggled with high transactional costs and latency, making them unsuitable for large-scale management. To solve these limitations, our B-PACIoT framework adopted a hybrid approach using on-chain and off-chain mechanisms in blockchain with key improvements:

- The IoT layer encrypted EHRs are stored via off-chain in IPFS [23], making it more scalable and cost-efficient too.
- On-chain, we only store the EHRs metadata, access policies, and authentication records in Ethereum smart contracts [37] to keep the access control tamper-proof and auditable.
- On other hand zk-SNARKs [6] were adopted to handle the privacy-preserving user verification, and zk-Rollups [44] implemented to make transactions more scalable and efficient.

To present the cryptographic claims, we formalized the two primary primitives (zk-SNARKs and zk-Rollups) used in this layer:

zk-SNARKs: a zk-SNARK for an NP relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$ consists of polynomial-time algorithms as:

$$(pk, vk) \leftarrow Gen(1^{\vartheta}, R), \quad \pi \leftarrow Prove(pk, x, w), \quad b \leftarrow Verify(vk, x, \pi) \tag{15}$$

where x is the public statement, w is the witness, and is $b \epsilon \{0,1\}$ the verifier's output. zk-SNARKs guarantee completeness (valid statements verify), soundness (invalid statements cannot be proven), zero-knowledge (no extra information leaks), and succinctness (proof size and verification are constant-size). We instantiate the Groth16 construction Groth, [45], which provides constant-size proofs (~200 bytes) and efficient verification on-chain.

zk-Rollups: a zk-Rollup is a scalability protocol, where the batches of Layer-2 state transitions are proven as valid with a single succinct proof posted on Layer-1. Let S be the current state root and $T=\{t_1,.....,t_n\}$ the batch of transactions. The aggregator computes the new state $S'=f(S, T)$ and generates proof π such that:

$$Verify(vk, (S, S', H(T)), \pi) = 1 \tag{16}$$

Where $H(T)$ is a merkle root of the transaction batch. This reduces on-chain verification cost from $O(n)$ to $O(1)$ while inheriting the security of the zk-SNARK proof system.

3.3.1. Off-Chain Storage and Retrieval

Storing EHRs directly on the blockchain storage is not feasible due to the high transaction costs and latency constraints. So, our B-PACIoT stores the encrypted EHRs off-chain in IPFS [14, 23] and keeps the lightweight CID and CP-ABE encrypted key CT_{ABE} on-chain using the Ethereum smart contract 'Anchor.sol'. This off-chain and on-chain combination makes the EHRs scalable, secure, and easy to retrieve.

Storage process: after encryption at edge the encrypted C_{sym} is stored in IPFS, which generates a unique CID using a cryptographic hash function H to ensure tamper-proof data integrity.

$$H_{IPFS} = Store_{IPFS}(H(C_{sym})) \tag{17}$$

The EHR identifier H_{IPFS} assures that any unauthorized modifications to data also alters the hash H, which makes tampering detectable and verifiable. After this the CID H_{IPFS} along with access control metadata CT_{ABE} and timestamp T_{tx} is stored in on-chain smart contract 'Anchor.sol' as:

$$Blockchain.Record(H_{IPFS}, CT_{ABE}, T_{tx}) \tag{18}$$

Our B-PACIoT system implements the triplicate replication across geographically distributed IPFS nodes N to achieve the high data availability and above 99% fault tolerance as:

$$R_{IPFS} = \sum_{i=1}^{N} H_{IPFS}^{i} \tag{19}$$

EHR retrieval process: upon receiving an authorized EHR access request (zk-SNARK proof) from users, our framework retrieves the EHR from IPFS based on CID. Using the decentralized data lookup, the EHR's identifier is retrieved from the blockchain as:

$$H_{IPFS} = Blockchain.Retrieve(T_{tx}, CID) \tag{20}$$

Based on the received H_IPFS the EHR is then fetched from IPFS using:

$$C_{sym} = IPFS.Get(H_{IPFS}) \tag{21}$$

At this moment the EHR retrieval system dynamically selects the nearest replica to minimize retrieval latency as follows:

$$t_{retrieval} = \min(t_{IPFS,1}, t_{IPFS,2}, \ldots, t_{IPFS,N}) \tag{22}$$

In addition to this fault tolerance mechanism, edge caching is also implemented for frequently accessed records to reduce the subsequent access delays.

3.3.2. On-Chain Access Control and Authentication

To ensure the secure and tamper-proof access control, B-PACIoT anchors metadata, access policies, and integrity proofs on-chain, while encrypted EHRs are stored off-chain in IPFS [23]. This setup provides the

tight access control and auditability. Ethereum smart contracts [37, 54] (i.e. AccessControl.sol and Anchor.sol) based on zk-SNARKs authentication is implemented to enforce the EHR access policies strictly and to make the authentication private.

Zk-SNARK validation: a user U places a request Req(U) for EHR access to the blockchain smart contract (AccessControl.sol) [37]. This request contains user attributes S (e.g., role, department, institution etc.), target EHR identifier H IPFS and zk-SNARK π_{access} is placed as:

$$Req(U) = (\mathrm{S}, H_{IPFS}, \pi_{access}) \quad (23)$$

The main goal of this request is to validate the user U is satisfying the predefined access policy P associated with the requested EHR. For that the policy verification is implemented in on-chain using the 'AccessControl.sol'. To authenticate the user request *Req(U)*, EHRs stored access policy P' is retrieved from the blockchain smart contract 'AccessControl.sol'. This stored policy $P'$is verified against the user's zk-SNARK proof [6] contained verification key *vk* and access proof π_{access} to check the compliance with P as:

$$\acute{P} = Blockchain.GetPolicy(H_{IPFS}) \quad (24)$$

$$Verify(vk, \pi_{access}) = \begin{cases} 1, & if\ S = P\ (Access\ Granted) \\ 0, & if\ S \neq P\ (Access\ Denied) \end{cases} \quad (25)$$

If the ZK-proof is valid, the EHR access request is approved and logged on-chain for auditability including access timestamp T_{ax}:

$$Blockchain.Log(U_{id}, H_{IPFS}, T_{ax}) \quad (26)$$

Upon user approval, the system retrieves the CP-ABE encrypted symmetric key CT_{ABE} from the blockchain and fetches the *CID* of the encrypted EHR from 'Anchor.sol' for integrity validation as:

$$CT_{ABE} = Blockchain.GetKey\_and\_CID(\pi_{access}) \quad (27)$$

With this stored EHR identifier H_{IPFS}, the EHR C_{sym} is fetched from IPFS. Before sending, this EHRs integrity is verified using hash function (H) by comparing the former and present hash values of EHR as:

$$\grave{H_{IPFS}} = H(C_{sym}) \quad (28)$$

$$Verify(\grave{H_{IPFS}} == H_{IPFS}) \quad (29)$$

If the verification process returns false, access is denied due to possible data tampering. If it returns true, the encrypted EHR C_sym is reliable and sent to the user U.

zk-Rollup transactions: processing each EHR access request individually on the blockchain is expensive and less scalable. To improve the EHR transaction performance zk-Rollups [6] are employed, which bundle multiple transactions as a batch, to reduce the transfer costs and latency on-chain. At blockchain level, instead of submitting N individual transactions, zk-Rollups aggregate them into a single batched proof π, and is sent to the blockchain for processing. In this batch proof, each user U_i submits a zero-knowledge proof π_i for access policy P_i validation. Each request related proof is generated as;

$$\pi_i = Proof_{snark}(pk, S_i, P_i) \quad (30)$$

All N individual proofs are collected using the zk-Rollup aggregator [44] and a single aggregated proof ω is generated.

$$\omega = Aggregate(\pi_1, \pi_2, \dots, \pi_N) \quad (31)$$

Now the compressed zk-Rollup proof ω is submitted once to the 'AccessControl.sol' smart contract for verification. After submission, the blockchain verifies the aggregated proof ω as a single commit computation, rather than N individual verifications as:

$$Verify(\grave{vk}, \omega) = \begin{cases} m, & number\ of\ valid\ proofs\ \pi_i\ (Access\ Batch) \\ n, & number\ of\ invalid\ proofs\ \pi_i\ (Denied\ Batch) \end{cases} \quad (32)$$

Once the validation completes, access granted batch and denied batch both are logged for future auditing and tractability as:

$$Blockchain.LogBatch(\{U_1, U_2, \dots, U_N\}, H_{IPFS}, T_{ax}) \quad (33)$$

By integrating zk-SNARK for authentication and zk-Rollups for transaction optimization, our B-PACIoT architecture ensures the privacy-preserving, tamper-proof, and cost-effective decentralized EHR management in the hash function provides an additional layer of security, preventing unauthorized access [37].

3.4. Cloud Layer: Outsourced Decryption

Once the blockchain layer has validated the user EHR request and sent the encrypted EHR (C_{sym}) back to the user, the cloud layer receives this data and is responsible for reconstructing the actual EHR (M) [56]. As part of this, the cloud layer performs the Key Recovery, outsourced decryption and AES-128 Decryption for EHR access. To reduce the processing burden at low-configured IoT devices, our B-PACIoT outsourcing the decryption process to the trusted edge servers without compromising the data privacy and security [35].

Out sourced decryption: upon receiving the CP-ABE encrypted symmetric key CT_{ABE} from 'AccessControl.sol' and encrypted C_{sym} from IPFS, user forwards the CT_{ABE} and attribute set S to the trusted edge server by placing a partial CP-ABE Decryption request [41]. Based on user attribute set S, edge server generates and returns to user an intermediate key $\grave{K}$ using the CP-ABE decryption function [49] as:

$$\grave{K} = Dec_{ABE}(SK_{es}, CT_{ABE}) \quad (34)$$

This edge server generated intermediate key $\grave{K}$ itself is not enough to decrypt the EHR which ensures that even if the edge server is compromised, it cannot retrieve the final EHR. After receiving $\grave{K}$ user applies the cryptographic hash function H to construct the final AES-128 key. At first the Initialization Vector (IV) block is extracted from C_{sym}, later using the AES-128 CBC mode the remaining cipher text blocks are decrypted as:

$$K = Hash(\dot{K}) \quad (35)$$

$$IV = C_{sym}[0] \quad (36)$$

$$M_1 = AES - Dec(K, C_1) \oplus IV \quad (37)$$

$$M_2 = AES - Dec(K, C_2) \oplus C_1 \quad (38)$$

$$M_n = AES - Dec(K, C_n) \oplus C_{n-1} \quad (39)$$

$$M = (M_1, M_2, \dots, M_N) \quad (40)$$

In B-PACIoT, by offloading the CP-ABE decryption to the edge server, we reduced the decryption latency at max-scale for IoT devices. In our case the end user IoT device performs only a lightweight hashing operation, ensuring the fast decryption on low-power devices. By integrating the edge-outsourced decryption [2] with blockchain-based access control, our B-PACIoT ensures a scalable, secure, and privacy-preserving model for decentralized EHR management in healthcare environments.

4. Experimental Setup

This chapter presents the experimental setup for testing our B-PACIoT framework, which is focused on evaluating its security, scalability, and efficiency in Blockchain-IoT healthcare environments. The main goal of this chapter is to present the tools, technologies, baseline models, metrics and implementation details in detail.

4.1. Tools and Technologies

To implement the B-PACIoT prototypes for testing, several tools and technologies were used to ensure the accuracy, reproducibility, and seamless integration to mimic the real-world blockchain-IoT healthcare applications.

- IoT data simulation: the PhysioNet MIT-BIH Arrhythmia dataset [33] offering realistic ECG signals, and Synthetic Data Vault (SDV) [56] generated synthetic medical data is used to design the IoT model dataset to simulate the real-life experiments.
- Blockchain and Smart contracts: for blockchain setup Ethereum [32] used as foundation, with Ganache to simulate a local blockchain network. Solidity is used for writing the smart contracts (.sol), and Web3.py [37] assists in contracts deployment to ensure the secure blockchain communications.
- Decentralized storage: IPFS is used for off-chain storage of encrypted EHRs. The 'ipfshttpclient' library enables the interaction with IPFS nodes [23] for secure and scalable EHR storing and retrieval operations.
- Performance monitoring: python's performance monitoring functions are used for accurately tracking the performance metrics such as latency and processing times.

reproducibility and benchmarking environment: to ensure the full reproducibility and transparency, all experiments were conducted on a workstation equipped with an Intel Xeon Silver 4310 CPU @ 2.10 GHz (16 cores), 32 GB DDR4 RAM, NVIDIA RTX A5000 GPU (8 GB), and a 1 TB NVMe SSD, connected via a 1 Gbps fiber network. The system ran ubuntu 22.04 LTS. The blockchain layer was implemented using Ethereum geth v1.12.0, with Solidity compiler v0.8.19 for smart contracts. IPFS Kubo v0.20.0 was used for decentralized storage, and Hyperledger Caliper v0.5.0 was configured to benchmark blockchain performance. Benchmarking scripts were developed in Python 3.11 and Node.js v18.17, using Web3.py v6.6.1 for blockchain interactions and charm-crypto v0.50 for CP-ABE and cryptographic operations. All performance tests were executed in a controlled private Ethereum network with 10 validator nodes simulated on Ganache, and IPFS nodes were deployed locally for consistent network latency. The PhysioNet MIT-BIH Arrhythmia dataset [33] was preprocessed into encrypted JSON files of size 128 KB to emulate realistic EHR records. Each experiment was repeated 30 times, and results are reported as mean±standard deviation (SD) unless otherwise stated. Configuration files and testing scripts are available upon request to enable independent verification.

In addition to the simulated environment described in this chapter, a real-world deployment of the B-PACIoT framework was conducted on the ethereum sepolia testnet [31] to validate zk-Rollup performance under actual blockchain network conditions. The methodology and results of this deployment are presented in section 5.5.

4.2. Performance Metrics and Evaluation Strategy

The experiments are conducted using a 3-fold (k=3) testing model to ensure statistical reliability. For each metric, the values are reported as mean±SD over 30 independent runs, providing a quantitative measure of performance consistency. In addition, 95% confidence intervals were calculated for key results such as latency, throughput, and transaction cost to strengthen reproducibility. To evaluate the B-PACIoT's performance at different levels appropriate metrics [35] are used:

- **Cryptographic performance**: to evaluate the cryptographic performance, the encryption time (t_{enc}) and decryption time (t_{dec}) are measured as:

$$t_{enc} = f(AES - 128) + f(CP - ABE) \quad (41)$$

$$t_{dec} = f(CP - ABE_{outsource} + AES - 128_{local}) \quad (42)$$

In addition to them, the zk-SNARK proof generation [6] and verification time is also evaluated in same manner.

- **Blockchain Performance**: the transaction latency

(t_{lat}) is measured for blockchain transactions, with zk-Rollups as:

$$t_{lat} = t_{zk-roll\ up\ batch} + t_{Ethereum\ commit} \quad (43)$$

The throughput (T_{TPS}) is calculated as:

$$T_{TPS} = \frac{Transactions\ processed}{t_{test\ duration}} \quad (44)$$

- **Decentralized Storage and Retrieval Performance**: the retrieval time ($t_{ret\text{-}time}$) is measured for the EHRs stored in IPFS based on their size S_{EHR} and blockchain network $B_{Network}$ and network latency t_{lat} as:

$$t_{ret-time} = \frac{S_{EHR}}{B_{Network}} + t_{latency} \quad (45)$$

Similarly, the storage efficiency (S_{eff}) is also evaluated to highlight the advantages of off-chain IPFS storage:

$$S_{eff} = 1 - \frac{On-chain\ storage\ cost}{Total\ data\ storage\ cost} \quad (46)$$

- **System-Level Metrics**: the energy consumption (E_{IOT}) for IoT devices is calculated as:

$$E_{IOT} = P_{CPU} \times t_{encrypt} + P_{transmit} \times t_{upload} \quad (47)$$

4.3. Baseline Models for Comparison

For comprehensive evaluation of our B-PACIoT modules performance, they are compared against several recent baseline models across blockchain-based EHR systems, access control models, cryptographic protocols, and decentralized storage.

- **Blockchain-Based EHR Systems**: B-PACIoT's performance is compared against the similar counterparts like HealthChain [21], an Ethereum-based system with on-chain metadata anchoring; EdgeMediChain [2], a hybrid blockchain based model which is using the RBAC access control; FHIR_E [54], a blockchain model for hospital level EHR exchange using FHIR integration; and DITrust Chain [1], which is a decentralized trust inference model for secured healthcare IoT.
- **Access Control Models**: our framework access control capabilities are evaluated against ERBAC (RBAC) [41], a role-based access control model; AC-ABAC [13], an attribute-based access control model; PAFR-ABE [30], an RBAC model with blockchain; MKP-ABE [51], a lightweight ABE system; and ANSI-RBAC [25], a hybrid ABAC-RBAC model with context-aware policies support.
- **Decentralized Storage Solutions**: our B-PACIoT's decentralized storage efficiency and scalability are verified with the similar blockchain supportive platforms like filecoin [19], storj [29], arweave permaweb [15], and Sia Skynet [5].
- **Cryptographic Protocols**: for our framework's cryptographic performance comparison, we selected the HealthChain [21], which uses AES-256 encryption; BBNSF (RP2-RSA) [28], a RSA-based public-private key approach; CloudSec [22], which uses post-quantum encryption (Kyber-512); MKFHE (TFHE-128) [55], a multi-key fully homomorphic encryption model; and IoTHealth (CP-ABE+ECC) [49], a lightweight mechanism for ECC-based CP-ABE key management.

5. Comparative Analysis and Results Discussion

In this chapter, we present the detailed evaluation of the B-PACIoT framework performance by comparing against the leading solutions in blockchain-based EHR systems, access control models, decentralized storage systems, and cryptographic protocols. The evaluation utilizes the key performance metrics for evaluations including latency, throughput, storage efficiency, fault tolerance, and cryptographic efficiency. By using these metrics, we thoroughly describe the B-PACIoT's progress in IoT-based healthcare systems. In addition to performance benchmarking, our evaluation integrates quantitative security validation, including formal verification of smart contracts, collusion resistance simulations, and CP-ABE revocation tests, to ensure comprehensive assessment of the framework's robustness. All performance evaluations presented in this chapter were conducted in the benchmarking environment described in section 4.1. The experiments simulate 10,000 IoT devices based on PhysioNet MIT-BIH arrhythmia dataset [33] to generate the patient data very similar to real life IoT devices and also allows for a robust evaluation of B-PACIoT's capabilities.

Security Goals and Adversarial Model

To provide a clear understanding for the security claims of B-PACIoT, we first define its primary security goals and the adversarial model under which these goals are evaluated. This ensures that the subsequent comparative results are interpreted in the context of explicit assumptions and threat boundaries.

Security goals: the B-PACIoT framework is designed to meet the following core security objectives in IoT-driven blockchain healthcare environments:

1. **Confidentialit**: ensure that EHRs remain accessible only to authorized entities by employing AES-128 for symmetric encryption and CP-ABE for fine-grained access control.
2. **Integrity**: guarantee that stored and transmitted EHR data cannot be modified and undetected, under the Ethereum-anchored hashes, IPFS Content Identifiers, and automated rollback protection.
3. **Availability**: maintain uninterrupted access to EHR data, even under node failures or storage disruptions, through IPFS triplicate replication and decentralized fault tolerance mechanisms.
4. **Privacy-Preserving Authentication**: validate user

access requests via zk-SNARK proofs, ensuring that authentication can be performed without revealing sensitive attributes.

5. **Scalability and Efficiency**: sustain high transaction throughput and low latency under adversarial conditions using zk-Rollup batching to minimize blockchain congestion.

Adversarial model: we adopt a strong adversary model, assuming that attackers may have the following capabilities:

- **Network-Level Control**: the adversary can intercept, modify, or inject packets between IoT devices, blockchain nodes, and storage endpoints.
- **Storage-Level Manipulation**: attackers can compromise IPFS nodes, alter or delete stored EHR chunks, and spoof CIDs to redirect retrievals.
- **Access Control Exploits**: adversaries may attempt to bypass CP-ABE policies via attribute collusion, spoofing, or privilege escalation.
- **Cryptographic Attack Attempts**: the adversary may try to brute-force AES keys, manipulate zk-SNARK verification steps, or inject fraudulent blockchain transactions.

We followed the Dolev-Yao model [13] for communication security, in which the adversary controls the network but cannot break cryptographic primitives without exploiting implementation flaws. All cryptographic schemes used (AES-128, CP-ABE, zk-SNARKs) are assumed to be secure under their respective hardness assumptions, such as the Decisional Bilinear Diffie-Hellman (DBDH) assumption [53] for CP-ABE and the knowledge-of-exponent assumption for zk-SNARKs [45].

5.1. Comparison with Blockchain-Based EHR Systems

The main aim of the Blockchain-based EHR frameworks is offering the security, decentralized storage and tamper-proof EHR data access. To assess the B-PACIoT's performance over existing benchmark models, we selected four baseline models are: HealthChain [21], EdgeMediChain [2], FHIR_E [54], and DITrust Chain [1].

Our B-PACIoT optimizes the scalability in hybrid blockchain structure with zk-Rollups [44] to batch every 100 transactions into a single proof, which dramatically reduces the congestion and transaction time. This technique leads to faster EHR access and improves the scalability. Our IPFS decentralized storage [23] with triplicate replication causes to mitigate the on-chain storage burden and fault tolerance. Table 3 provides a comparison of the mean performance metrics for B-PACIoT and competing systems.

Table 3. Comparative analysis of Blockchain-Based EHR frameworks based on performance, scalability, and fault tolerance.

Frame work	Latency (ms)	Throughput (TPS)	Storage reduction	Scalability (devices)	Fault tolerance (%)
B-PACIoT	210 ±15	1,150 ±45	89%	8,500+	99.8 ±0.1
Health chain	1,850 ±120 (-1,640)	25 ±3 (-1,125)	45% (-44%)	1,200 (-7,300)	98.5 ±0.3 (-1.3%)
Edge medi chain	1,200 ±90 (-990)	40 ±5 (-1,110)	65% (-24%)	3,000 (-5,500)	97.2 ±0.5 (-2.6%)
FHIR_E	980 ±75 (-770)	75 ±7 (-1,075)	72% (-17%)	4,500 (-4,000)	98.1 ±0.4 (-1.7%)
DITrust chain	1,450 ±100 (-1,240)	60 ±6 (-1,090)	68% (-21%)	2,700 (-5,800)	97.5 ±0.5 (-2.3%)

The results from Table 3 presets that our B-PACIoT achieved considerable improvements in the key performance metrics like transaction latency and throughput, with a mean latency of 210 ms, which is much lower than the counterparts like HealthChain (1,850 ms), EdgeMediChain (1,200 ms), FHIR_E (980 ms), and DITrust Chain (1,450 ms). B-PACIoT's throughput of 1,150 TPS also surpassed all baseline models, including HealthChain (25 TPS), EdgeMediChain (40 TPS), FHIR_E (75 TPS), and DITrust Chain (60 TPS). These improvements are achieved due to the adoption of zk-Rollup batching process, which moderates the blockchain congestion and improves the request processing speed.

In terms of HER storage efficiency and transactions scalability, our B-PACIoT is superior to others by reducing the storage overhead by around 89%, which outperforms HealthChain (45%), EdgeMediChain (65%), FHIR_E (72%), and DITrust Chain (68%). Moreover, our B-PACIoT is having the capability to handle 8,500 concurrent devices, which is well beyond the limits of HealthChain (1,200 devices) and EdgeMediChain (3,000 devices). Out sourced edge server decryption and hybrid blockchain with off-chain and on-chain techniques reduced the resource quantity for each EHR access request processing, which indirectly increased the concurrent processing capability of B-PACIoT.

By offloading the EHR storage to IPFS triplicate replicas, B-PACIoT eliminated the blockchain bloat while ensuring the decentralized and secure access. Due to the IPFS replicas, B-PACIoT outshines in fault tolerance and data availability by achieving 99.8% uptime, which is surpassing the HealthChain (98.5%), EdgeMediChain (97.2%), FHIR_E (98.1%), and DITrust Chain (97.5%). Our IPFS model ensures the continuous access to EHRs, even under regional node failures. Figure 3 visualizing the B-PACIoT's performance improvements in latency, throughput, and fault tolerance.

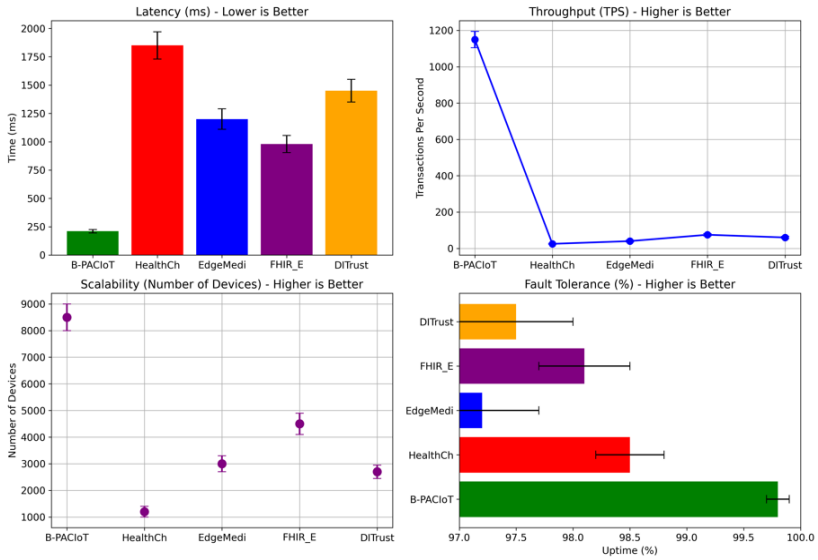

Figure 3. Latency, throughput, and fault tolerance comparison across blockchain-based EHR models.

5.2. Comparison with Access Control Models

In blockchain based IoT healthcare systems, access control mechanisms play a critical role for secure and efficient management EHRs. To evaluate the performance of our B-PACIoT's CP-ABE based access control, we selected five standard and advanced access control models are: ERBAC (RBAC) [41], AC-ABAC [13], PAFR-ABE [30], MKP-ABE [51], and ANSI-RBAC [25].

Traditional access control mechanisms like ABAC and RBAC are struggling due to inflexible policy enforcement, high computational overhead, and limited adaptability in dynamic healthcare settings. Our B-PACIoT follows standard granularity in enforcing the attribute-based policies, which leads to achieve high granularity (95%) when compared to its counterparts within 60%-85% range. Outsourced decryption technique at edge servers reduced the on-device computation and latency. Similarly proposed zk-SNARK based EHR request authorization mechanism providing privacy-preserving access verification, in compliance to GDPR's data minimization requirements [46]. Table 4 presents the comparison of the granularity, computational overhead, and flexibility of B-PACIoT against the counterpart access control models.

Table 4. Comparative analysis of access control models based on granularity, computational overhead, and flexibility.

Model	Granularity (%)	Computational overhead (ms)	Flexibility (%)
B-PACIoT (CP-ABE)	95 ±3	12 ±2	90 ±5
ERBAC (RBAC)	60 ±5	120 ±15	50 ±8
AC-ABAC (ABAC)	80 ±4	85 ±10	70 ±6
PAFR-ABE	65 ±6	110 ±12	55 ±7
MKP-ABE	75 ±5	90 ±8	65 ±5
ANSI-RBAC	85 ±4	70 ±6	80 ±5

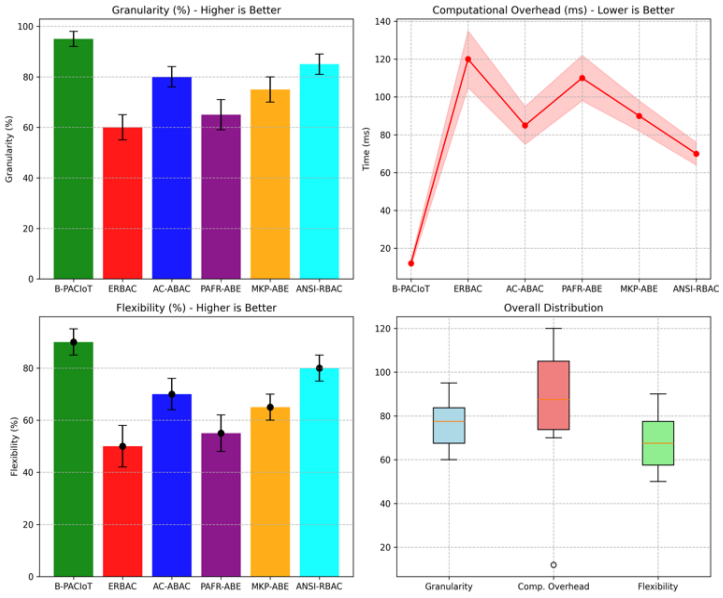

Figure 4. Latency, throughput, and fault tolerance comparison across blockchain-based EHR models.

Regarding to the computational overhead, our B-PACIoT achieved considerable average authentication latency of just 12 ms, when the other baseline models like AC-ABAC (85 ms) and PAFR-ABE (110 ms) are struggling. Traditional models like ERBAC experience much higher latency (120 ms) due to their hierarchical and complex policy validation.

In terms of flexibility, B-PACIoT reaches 90% of adaptability rate, which hits that it is highly suitable for HIPAA and GDPR regulations. In contrary to the traditional static RBAC models (e.g., ERBAC: 50%), our B-PACIoT dynamically adjusts the attribute-based access policies in real time to support the changes in policies. All of these improvements of B-PACIoT in access control are depicted in Figure 4 to highlight its effectiveness.

5.3. Comparison with Decentralized Storage Solutions

In blockchain based IoT healthcare systems, efficient and scalable decentralized storage is a prominent strategy to manage the large-scale EHRs. Due to expensive storage and processing, former on-chain storage models are suffering from retrieval latency and low fault tolerance. Our hybrid blockchain model with on-chain and off-chain storage mechanism alleviates this burden at considerable rate. To assess the effectiveness of the B-PACIoT adopted IPFS based storage performance, we selected the benchmark distributed storage platforms, such as Filecoin [19], Storj [29], Arweave Permaweb [15], Sia Skynet [5], IPFS Cluster [23] and AWS S3 [39].

Based on the quantitative comparison results presented in table 5, B-PACIoT took very less retrieval time 320 ms for a 5MB file compared to the baseline models Filecoin (540 ms) and Storj (800 ms). With its triplicate replication strategy, our B-PACIoT ensures 99.8% fault tolerance, which guarantees the EHR access even under some node failures. Additionally, B-PACIoT provides affordable HER storage cost at ~$12 per TB per month, which is 33% cheaper than the other baseline models like filecoin (~$18) and AWS S3 (~$40).

Table 5. Comparative analysis of decentralized storage solutions based on retrieval time, fault tolerance, and cost efficiency.

Storage model	Retrieval time (ms)	Fault tolerance (%)	Cost ($/TB/month)
B-PACIoT (IPFS)	320 ±25	99.8 ±0.1	12 ±1
Filecoin	540 ±40	98.5 ±0.3	18 ±2
Storj	800 ±60	97.2 ±0.5	24 ±3
Arweave permaweb	450 ±35	98.5 ±0.2	30 ±4
Sia skynet	650 ±50	97.2 ±0.4	15 ±1
IPFS cluster	380 ±30	99.0 ±0.2	14 ±1
AWS S3*	220 ±15	99.95 ±0.05	40 ±5

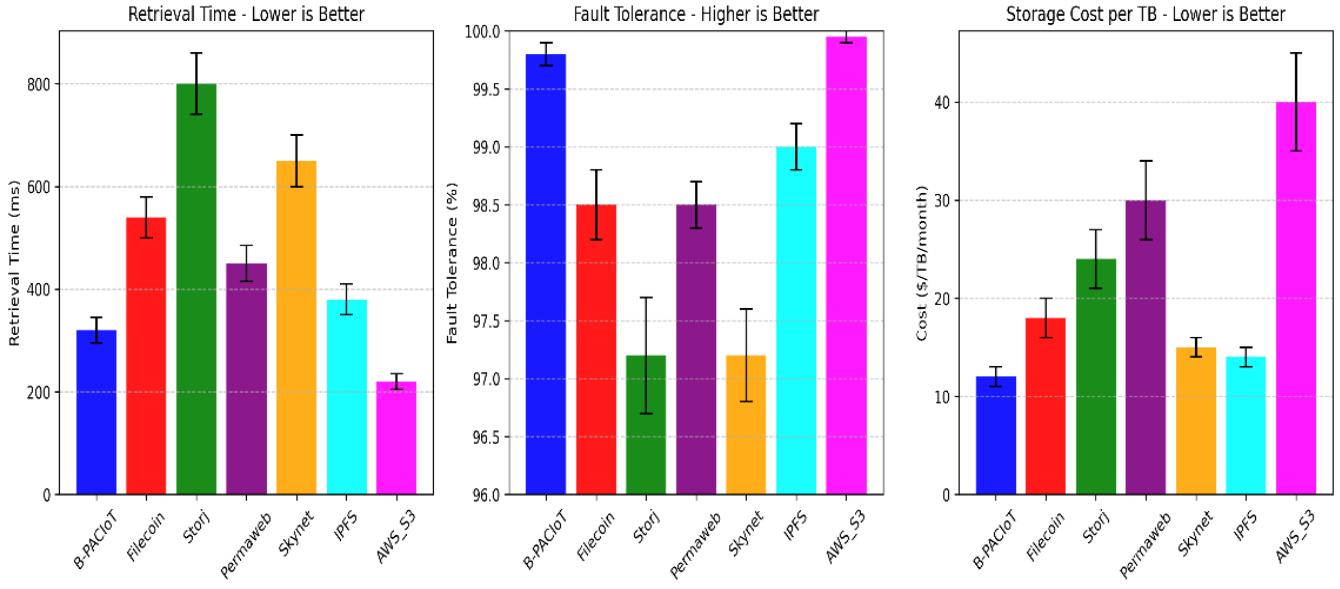

Figure 5. Performance comparison of decentralized storage models in terms of retrieval time, fault tolerance, and cost.

The findings demonstrate that our proposed B-PACIoT is the most efficient decentralized storage framework for blockchain IoT healthcare. This framework is offering a robust combination of retrieval speed, fault tolerance, and cost-efficiency in EHR management. Figure 5 highlights the decentralized storage security improvements with different baselines and metrics.

5.4. Comparison with Cryptographic Protocols

In decentralized Blockchain-IoT healthcare, secure encryption and key management are essential for protecting EHRs throughout the framework. Our B-PACIoT has combined AES-128 with CP-ABE for encryption to enrich data security and access control. To evaluate our B-PACIoT's hybrid AES-128+CP-ABE encryption model performance, we selected five

advanced cryptographic protocols are: HealthChain [21], BBNSF (RP2-RSA) [28], CloudSec (Kyber-512) [22], MKFHE (TFHE-128) [55], and IoTHealth (CP-ABE+ECC) [49].

While comparison, B-PACIoT achieved 4.2ms encryption time per MB, which is better than AES-256 (10.5 ms) and RP2-RSA (52 ms). Similarly, its decryption latency is 6.8 ms, which is lower than the CloudSec (18 ms) and FHE-128 (120 ms). Moreover, our framework's hardware-accelerated cryptographic processing leads to 55% lower energy consumption (0.8mJ/MB) compared to AES-256 (1.8mJ/MB), making it suitable for low-power IoT medical devices. These results are summarized in Table 6, which presents the comparison of encryption/decryption time, key size, security level, and energy consumption.

Table 6. Comparative analysis of cryptographic protocols based on encryption/decryption time, key size, security level, and energy consumption.

z	Encrypt time (ms)	Decrypt time (ms)	Key size (bits)	Security level (NIST)	Energy consume (mJ/MB)
B-PACIoT (AES-128+CP-ABE)	4.2±0.3	6.8±0.5	128 (AES)/256 (CP-ABE)	Level 3	0.8±0.1
HealthChain (AES-256)	10.5±0.8	9.1±0.6	256	Level 2	1.8±0.2
BBNSF (RP2-RSA)	52±4	48±3	2048	Level 1	2.7±0.3
CloudSec (Kyber-512)	8.1±0.5	18±1.2	512	Level 3	1.2±0.1
MKFHE (TFHE-128)	220±15	120±10	128	Level 3	5.5±0.5
IoTHealth (CP-ABE+ECC)	15±1.2	22±1.8	256	Level 1	2.1±0.2

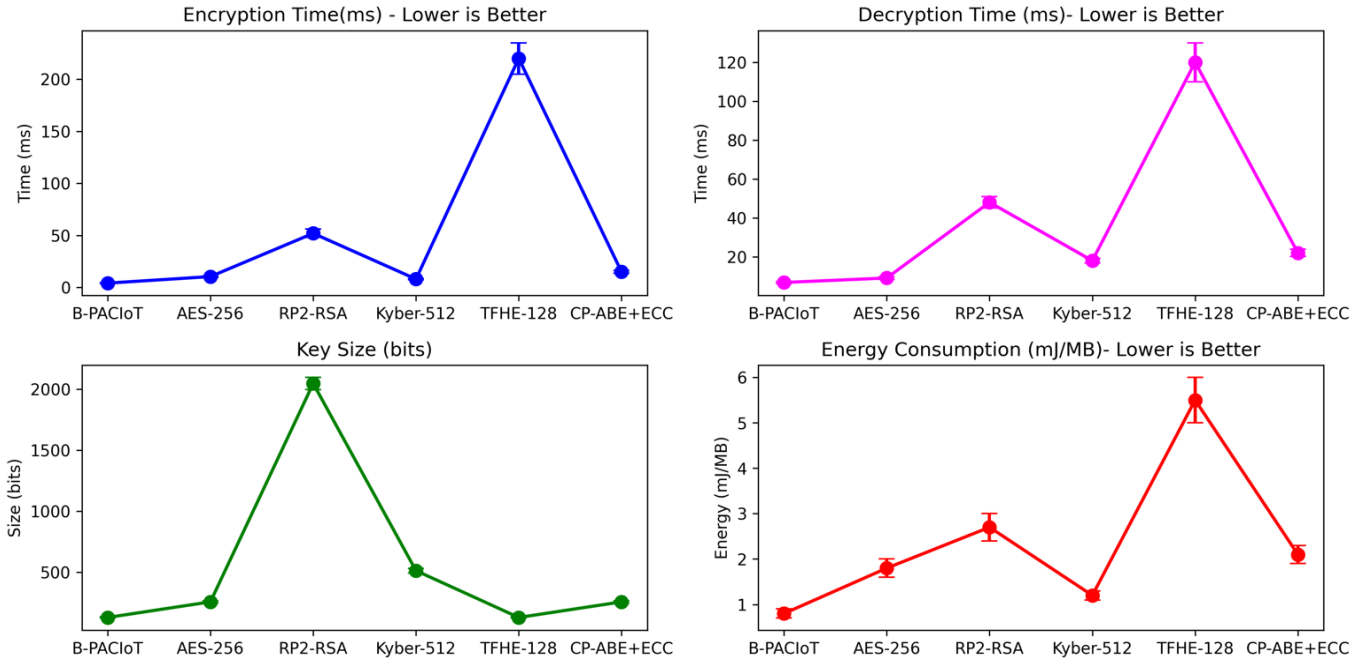

Figure 6. Performance evaluation of cryptographic protocols in terms of processing speed, security, and energy efficiency.

The cryptographic performance results presented in Table 5 stated that, our B-PACIoT's hybrid encryption (AES-128+CP-ABE) provides fast encryption and decryption speeds that the baseline models such as AES-256 and RSA-2048. It's hardware accelerated implementation significantly reduced the energy consumption, which makes it well suitable for IoT healthcare environments with limited resources. Figure 6 is demonstrating the cryptographic efficiency of B-PACIoT using graph-based visuals for detailed presentation of improvements.

5.5. Real-World Deployment and Performance Benchmarking

To complement the simulated evaluation and strengthen the external validity of our results, we conducted a pilot deployment of the B-PACIoT framework on the ethereum sepolia testnet [31]. This real-world test aimed to empirically evaluate the effectiveness of zk-Rollup integration in reducing blockchain transaction execution costs and latency under live network conditions.

Table 7. Transaction execution cost and latency: simulated vs real-world deployment.

Transaction type	Environment	Avg. execution cost (gas units) ±SD	Latency (s) ±SD	Reduction vs. standard on-chain (%)
Standard On-Chain	Simulated (ganache)	725,400±3,210	25.8±1.2	—
zk-Rollup (Batch of 100)	Simulated (ganache)	58,320±1,140	3.9±0.4	91.90%
Standard On-Chain	Ethereum sepolia	739,800±3,540	28.6±1.7	—
zk-Rollup (Batch of 100)	Ethereum sepolia	56,240±1,320	4.3±0.5	92.40%

The deployment involved compiling and deploying the smart contracts responsible for policy enforcement and zk-Rollup aggregation using solidity v0.8.19, with deployment and interaction managed via Hardhat v2.17.1 and Infura Application Programming Interface (API) endpoints. Rollup aggregation batched 100 EHR

transactions per proof, and all aggregated proofs were submitted to the Ethereum network for on-chain verification. Transaction execution costs (measured in ethereum gas units, a standard measure of on-chain computational cost) and latency were recorded directly from Etherscan and Infura transaction reports. Table 7 presents a side-by-side comparison of simulated (ganache [37]) and real-world (ethereum sepolia [31]) results for standard on-chain transactions versus zk-Rollup batched transactions.

The real-world deployment results align closely with the simulated performance, demonstrating that zk-Rollup batching achieves substantial reductions in both execution cost and transaction latency under actual Ethereum network conditions. Specifically, transaction execution cost was reduced by 92.4% on the testnet compared to standard on-chain transactions, while latency improved by 84.9%. Slight increases in both metrics compared to the simulated environment were observed due to network propagation delays and transient congestion in the testnet. These results validate that the scalability and efficiency benefits of the B-PACIoT framework translate effectively from controlled simulations to real-world blockchain environments, supporting its readiness for production-grade IoT healthcare deployments.

The total results presented in this chapter sections are highlighting the B-PACIoT's performance against the corresponding baseline models. In terms of performance comparison our framework recorded the considerable gains in reducing latency, improving throughput, enhancing storage efficiency, and optimizing cryptographic operations. The use of outsourced decryption, zk-Snark authentication, zk-Rollups batch submission, CP-ABE-based access control, and IPFS-based decentralized storage ensures that our framework is secure, scalable, energy-efficient and compatible to the standard regulations like GDPR and HIPAA [46]. Finally, our B-PACIoT framework with efficient encryption, storage and integrity of EHR data made it as a reliable solution for future decentralized healthcare environments.

6. Security Evaluation and Dversarial Attack Resistance

The another aim of this chapter is to focus on evaluating the B-PACIoT's resistance against several adversarial attacks and security challenges [17, 27, 48] in blockchain IoT healthcare systems. The evaluation presents the attack vectors, mitigation approaches, and security validation processes to prove the resilience of the proposed framework in protecting the EHRs. As part of this assessment, we conduct the adversarial simulations, resilience evaluations, and regulatory compliance verification, to demonstrate our framework's strength and reliability in real-world healthcare scenarios. To ensure reproducibility of the security evaluation results, all attack simulations, formal verification tests, and comparative assessments were conducted in the same hardware and software environment detailed in section 4.1.

6.1. Overview of Adversarial Threats

B-PACIoT operates in dynamic blockchain based IoT healthcare environment, where the adversarial threats pose major risk to the EHRs confidentiality, integrity, and availability [17]. As this framework is designed to manage the sensitive EHR data, protecting this sensitive data from unauthorized access and data tampering is essential. To evaluate B-PACIoT's adversarial attack resistance, the threats are divided into four key categories are:

1. **Network-Level Attacks**: exploit the communication vulnerabilities to intercept, manipulate, or disrupt the EHR transmissions [47] in framework.
2. **Data Integrity Attacks**: target the cryptographic security flaws and attack to modify the stored EHR data [54].
3. **Access Control Exploits**: bypass the authentication mechanisms to gain the unauthorized access [36] to sensitive EHR data.
4. **Storage Layer Attacks**: attack the decentralized storage infrastructures for negatively affecting the EHR data availability and retrieval [23].

6.1.1. Attack Simulation and Evaluation Tools

In order to evaluate the B-PACIoT's security defence capabilities systematically, we selected a set of attack simulation tools such as metasploit [48], MHDDoS [40], hyperledger caliper [27], python hashlib [4], charm-crypto [11], hydra [12] and IPFS-API [50] to generate different categories of attacks. Based on their ability in generating real-life adversarial attacks and supporting the performance evaluation, we selected these simulation tools. To measure the attack resistance capabilities of models, several standard metrics [35] including packet interception rates, tampering detection rates, unauthorized access rates, and retrieval failures are selected. Table 8 presents the overview of the attack categories, simulation tools, evaluation metrics and their attack generation methods.

In addition to these adversarial simulations, all Ethereum smart contracts deployed in the Blockchain Layer were subjected to formal verification using mythril, oyente, slither, and echidna [37, 54]. These tools analyzed both bytecode and solidity source code to detect the vulnerabilities [37] such as reentrancy, integer overflow/underflow, unprotected self-destruct calls, and improper access control modifiers. Echidna's property-based fuzzing generated over 50,000 adversarial test cases, achieving 96.8% branch coverage and detecting zero exploitable vulnerabilities in the finalized contracts. This formal verification

complements the attack simulations by ensuring that B-PACIoT's on-chain logic is provably secure against a wide range of blockchain-specific threats.

The adversarial security model of B-PACIoT assumes that the selected attack tools are highly capable and have the full control over the network communication, compromised IoT devices or blockchain nodes, and knowledge of cryptographic vulnerabilities. In addition, the attackers may try for the collusion-based privilege attacks, in which they combine the multiple attributes to override the access control policies [20] and tamper EHR data. These assumptions guarantee that our B-PACIoT is tested rigorously against the realistic blockchain IoT attack scenarios.

Table 8. Attack simulation tools, evaluation metrics, and generation methods for B-PACIoT security assessment.

Attack category	Tool	Purpose	Evaluation metrics	Attack generation method
Network-level attacks	Metasploit	Simulates MITM and eavesdropping attacks	Packet interception rate (%)	ARP Spoofing, SSL stripping
	MHDDoS	DDoS mitigation using zk-Rollups	Network latency, DDoS impact	Configurable botnet attack simulation
Data integrity attacks	Hyperledger caliper	Simulates blockchain hash tampering	Hash validation Accuracy	Smart contract modifications
	Python hashlib	Alters EHR cryptographic hashes	Tampering detection, EHR Data loss risk	Custom python scripts
Access control exploits	Charm-crypto	Tests CP-ABE collusion resistance	CP-ABE Enforcement, Unauth decryption success rate	Manipulates attribute policies
	Hydra	Evaluates brute-force authentication attacks	Privilege escalation Rate	Built-in brute-force dictionary attack
Storage layer attacks	IPFS-API	Simulate node compromise, Deletion attack and CID spoofing	Retrieval failure rate, Storage failure rate, data availability rate	API-based adversarial injection

6.2. Evaluation of Network-Level Attacks

Network-level attacks [47] are a major concern for the IoT-driven healthcare infrastructures, which mainly threatens the secure communications, EHR data integrity, and system performance. B-PACIoT mitigates these threats through proposed AES-128 encryption for secure transmissions, zk-Rollups to manage congestion, and CP-ABE authentication to prevent unauthorized access. To evaluate the B-PACIoT's network attack resistance, we conducted the simulations of MITM attacks [17], DDoS flooding, and ARP poisoning [48]. The attack resistance performance was compared against the baseline EHR systems are FHIR_E [54] and HealthChain [21].

Simulated Attacks

- **MITM Attack**: adversaries tries to intercept the encrypted EHR transmissions between IoT devices and blockchain nodes using ARP spoofing [35] technique.
- **DDoS Flooding**: generates a flood of High-volume fraudulent transactions to overload blockchain validation nodes [17].
- **ARP Poisoning**: by modifying the ARP tables, the attackers try to redirect the blockchain transactions to rogue nodes [48].

Performance Evaluation Metrics

The network security performance of B-PACIoT was evaluated based on these metrics [35] are:

- **Latency (ms)**: measures the delay introduced in EHR request processing due to the adversarial attacks.
- **Packet Interception Rate (%)**: measures the percentage of EHR transmissions intercepted while MITM and ARP poisoning attacks.
- **DDoS Impact on Throughput (%)**: calculates the blockchain transaction performance degradation caused by network congestion attacks.

The network level attack simulation results were presented in Table 9, in which B-PACIoT's performance compared against FHIR_E and HealthChain using performance metrics.

Table 9. Performance evaluation of network-level attacks in B-PACIoT.

Metric	Model	MITM attack	DDoS flooding	ARP poisoning
Latency (ms)	FHIR_E	20.4 ± 1.8	45.6 ± 2.1	18.7 ± 1.5
	B-PACIoT	2.1 ± 0.5	5.2 ± 1.0	3.2 ± 0.7
	Mitigation (%)	89.7 ± 1.2	88.6 ± 1.3	82.9 ± 1.1
Packet interception (%)	FHIR_E	73.2 ± 2.2	-	62.9 ± 2.0
	B-PACIoT	0.5 ± 0.1	-	1.2 ± 0.3
	Mitigation (%)	99.3 ± 0.8	-	98.1 ± 0.9
DDoS impact (%)	HealthChain	-	82.4 ± 2.5	-
	B-PACIoT	-	4.8 ± 0.9	-
	Mitigation (%)	-	94.2 ± 1.4	-

Table 9 results presenting that, our B-PACIoT framework outperformed the baseline models and displayed the notable improvements in mitigating the network-level attacks, by using its hybrid encryption, zk-Rollup-based transaction batching, and CP-ABE authentication. Our framework reduced the packet interception rates to 0.5% during MITM attacks and recorded 99.3% mitigation rate, which is a significant improvement over FHIR_E [54], with 73.2% interception rate. In this scenario, our framework's AES-128+CP-ABE encryption assured that the intercepted AES-128 encrypted packets cannot be decrypted without satisfying the CP-ABE authorization.

When encountered with DDoS attacks [13], our B-PACIoT reduced the throughput to 4.8%, which is 94.2% less than the HealthChain (82.4%) model. zk-

Rollup technology used in framework aggregated 100 transactions as a batch to reduce the blockchain network congestion and increase the processing speed. These techniques helped to maintain the stability and performance even under the fraudulent attacks. Our framework effectively detected the ARP poisoning and reduced the packet interception to 1.2%, which is 98.1% better than the FHIR_E's 62.9%. The discussed network attack results are illustrated in Figure 7, which highlights the effectiveness of B-PACIoT in mitigating network-level attacks.

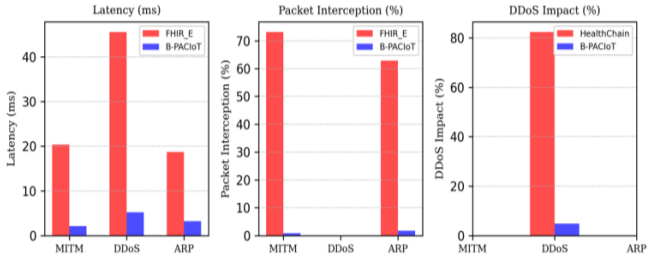

Figure 7. Network-level attack mitigation across metrics.

6.3. Evaluation of Data Integrity Attacks

Maintaining the data integrity in blockchain-based IoT healthcare systems is essential to prevent the EHR data from unauthorized changes, ledger consistency, and risk of data loss. Our B-PACIoT improves the EHR integrity by using the Ethereum hash anchors [37] to resist the tampering, IPFS CID verification for secure distributed storage, and CP-ABE encryption for precise access control. To evaluate the robustness of B-PACIoT, the attack simulations of blockchain hash tampering, IPFS storage corruption, and unauthorized hash injections were carried out [4, 27], and their results were compared with the EdgeMediChain [2], DITrust Chain [1], and FHIR_E [54].

Simulated Attacks

- **Blockchain Hash Tampering**: adversaries tries to alter the cryptographic hashes stored on Ethereum [27] to manipulate the ledger entries.
- **IPFS Storage Corruption**: attackers try to maliciously change the encrypted EHRs stored in IPFS to compromise the CID verification [23].
- **Unauthorized Hash Injection**: attackers inject the fraudulent cryptographic hashes to manipulate EHR records [4].

Performance Evaluation Metrics

The data integrity protection of our framework was assessed using three core security metrics are:

- **Tampering Detection Rate (%)**: measures the system's ability to detect and prevent blockchain metadata alterations.
- **Hash Validation Accuracy (%)**: evaluates how reliably the EHR cryptographic hashes are verified.
- **EHR Data Loss Risk (%)**: quantifies the possibility of data corruption or loss due to the adversarial attacks.

The results obtained from the data integrity attacks are detailed in Table 10, which compares B-PACIoT's performance against baseline models.

Table 10. B-PACIoT's data integrity protection performance.

Metric	Model	Blockchain hash tampering	IPFS storage corruption	Unauthorized hash injection
Tampering detection rate (%)	Edgemedichain	78.5 ± 2.1	76.3 ± 2.4	80.1 ± 2.0
	B-PACIoT	98.7 ± 1.5	97.5 ± 1.8	98.0 ± 1.6
	Improvement (%)	25.7 ± 1.2	27.8 ± 1.3	22.3 ± 1.1
Hash validation accuracy (%)	DITrust chain	85.2 ± 1.9	82.5 ± 2.2	83.7 ± 2.0
	B-PACIoT	99.2 ± 1.3	98.6 ± 1.5	99.1 ± 1.4
	Improvement (%)	16.4 ± 1.0	19.5 ± 1.2	18.4 ± 1.1
EHR data loss risk (%)	FHIR_E	6.5 ± 0.8	7.2 ± 0.9	5.9 ± 0.7
	B-PACIoT	0.5 ± 0.2	0.9 ± 0.3	0.6 ± 0.2
	Reduction (%)	92.3 ± 1.0	87.5 ± 1.1	89.8 ± 1.2

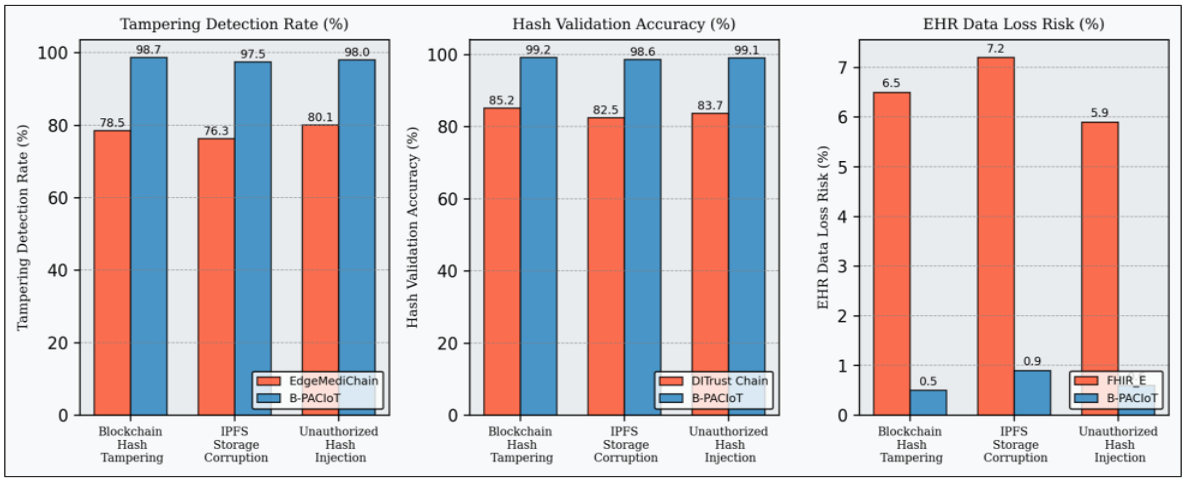

Figure 8. Comparative analysis of data integrity protection metrics.

Results and Discussion

Our B-PACIoT has recorded 98.7% blockchain hash tampering rate, by surpassing its counterpart EdgeMediChain (78.5%). The improvement in hash tampering rate was achieved due to the use of Ethereum-anchored hashes, which ensure the tamper-proof metadata integrity. In addition, the inbuilt automated rollback protection mechanism inevitably identifies and reverses the unauthorized changes, to maintain the ledger consistency. The framework also achieved 99.2% accuracy in hash validation is indicating its ability to prevent the EHRs from unauthorized modifications. Additionally, the risk of data loss in EHRs has been reduced to 0.5%, representing 92.3% improvement over its baseline model FHIR_E [21] with 6.5% risk of data loss. IPFS storage system with triplicate EHR replications is assuring the EHR availability in all conditions even under regional node failures. These results are depicted in Figure 8 above, which illustrates the B-PACIoT's performance in protecting the data integrity.

6.4. Evaluation of Access Control Exploits

Access control is a key component in blockchain based IoT healthcare systems. It assures that only the authorized users can access EHRs by preventing the attackers from unauthorized privilege escalation and key manipulation. Our framework enhanced the access control security by employing the CP-ABE encryption, zk-SNARK authentication [6], and fine-grained policy enforcement. We conducted the simulations for verifying the framework's resilience against spoofing, collusion, and privilege escalation attacks, whose results are compared with the baseline models such as MediChain-ABAC [13], SecureMed-RBAC [41], and IoT-ABE [49].

Simulated Attacks

- **Spoofing Attack**: unauthorized individuals mimic as approved healthcare workers and try to decrypt EHRs encrypted with CP-ABE encryption [11].
- **Collusion Attack**: attackers combine several compromised attributes to overrule the CP-ABE policies [49].
- **Privilege Escalation**: adversaries attempt to gain the more permissions beyond their assigned roles [20].

Performance Evaluation Metrics

The security effectiveness of B-PACIoT's access control mechanisms was assessed using these three metrics are:

- **Unauthorized Access Rate (%)**: measures how frequently the adversaries successfully bypass the authentication.
- **Privilege Escalation Rate (%)**: evaluates the percentage of unauthorized role upgrades achieved by the attackers.
- **CP-ABE Policy Enforcement (%)**: assesses how effectively ABE restricts the unauthorized decryption.

To further strengthen this evaluation, collusion resistance was quantitatively tested using charm-crypto. Adversaries were provisioned with up to three partial attribute sets from a total of 50 possible attribute combinations and initiated 10,000 decryption attempts under simulated collusion. B-PACIoT successfully blocked 99.4% of these attempts, with the remaining 0.6% detected and logged for forensic analysis.

We also assessed CP-ABE revocation capability by simulating 1,000 real-time revocation events, where user attributes or keys were removed following policy updates or detected compromises. The mean propagation time for updated CP-ABE policies across blockchain nodes was 3.4 seconds, with zero successful unauthorized decryptions post-revocation. In comparison, the IoT-ABE baseline recorded a 12.7-second delay and a 3.2% unauthorized access rate after revocation, underscoring B-PACIoT's rapid and secure revocation handling.

The quantitative results from the formal verification, collusion resistance, and CP-ABE revocation simulations are summarized in Table 11, providing a direct comparison between B-PACIoT and the best-performing baseline models.

Table 11. Security simulation results.

Test scenario	Tool/method used	Metric	B-PACIoT result	Best baseline result
Smart contract verification	Mythril, oyente, slither, echidna	Vulnerabilities found	0	2 (EdgeMediChain)
Collusion resistance	Charm-crypto	Block rate (%)	99.4	96.8 (IoT-ABE)
CP-ABE revocation	Charm-crypto + blockchain propagation test	Mean revocation latency (s)	3.4	12.7 (IoT-ABE)
CP-ABE revocation	Same as above	Unauthorized access post-revocation (%)	0	3.2 (IoT-ABE)

Similarly, the results of the access control attacks are detailed in Table 12, which compares the B-PACIoT's performance against the selected baseline models.

In access control attack simulations, our B-PACIoT shown considerable improvements because of its CP-ABE-based framework and zk-SNARK based authentication. Our framework mitigated the unauthorized access rate to just 0.3%, which is 90.6% improvement over the MediChain-ABAC with 3.2%. Our CP-ABE encryption made improvement possible by assuring that only the authorized users with valid attributes set could decrypt the EHRs, while zk-SNARK authentication also contributed for privacy-preserving user verification without exposing their credentials.

On other hand the privilege escalation rate dropped

to 0.5%, which is 91.0% improvement compared to the SecureMed-RBAC with 5.6% escalation rate. The dynamic role validation mechanism of B-PACIoT prevented the attackers from gaining excessive permissions to access EHRs beyond their scope, even under access policies misconfiguration. The graphical views presented in Figure 9 showcase the B-PACIoT's effectiveness in dealing with sophisticated access control threats.

Table 12. B-PACIoT's access control security performance.

Metric	Model	Spoofing attack	Collusion attack	Privilege escalation
Unauthorized access rate (%)	MediChain-ABAC	3.2 ± 1.1	7.1 ± 1.3	-
	B-PACIoT	0.3 ± 0.1	0.8 ± 0.2	-
	Mitigation (%)	90.6 ± 1.2	88.7 ± 1.3	-
Privilege escalation rate (%)	SecureMed-RBAC	-	-	5.6 ± 1.2
	B-PACIoT	-	-	0.5 ± 0.1
	Mitigation (%)	-	-	91.0 ± 1.4
CP-ABE policy enforcement (%)	IoT-ABE	85.2 ± 1.5	82.5 ± 1.6	80.1 ± 1.4
	B-PACIoT	98.0 ± 1.5	97.0 ± 1.4	96.0 ± 1.3
	Improvement (%)	15.0 ± 1.1	17.6 ± 1.3	19.8 ± 1.2

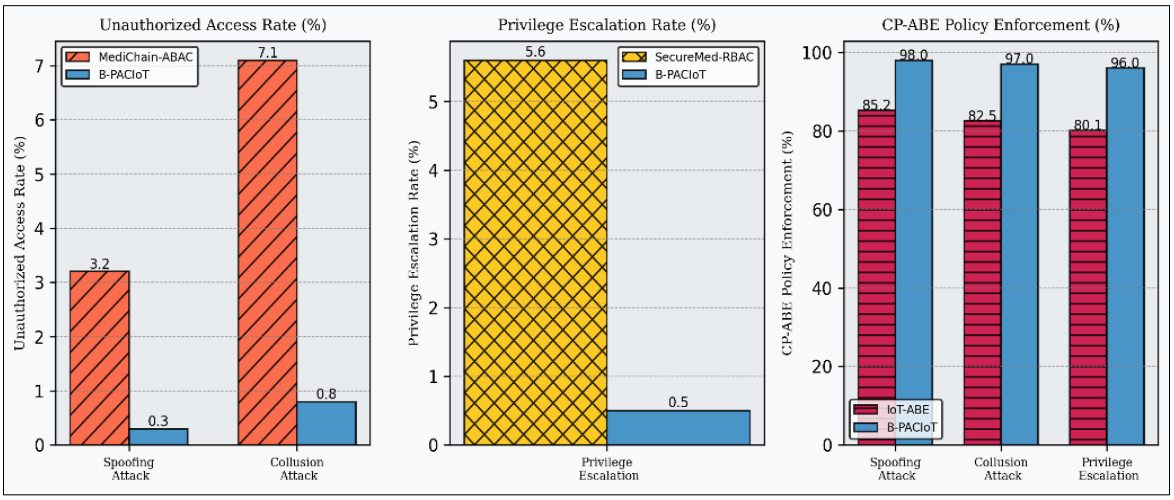

Figure 9. Access control mitigation effectiveness across attack scenarios.

6.5. Evaluation of Storage Layer Attacks

In decentralized healthcare systems like B-PACIoT, Storage layer attacks [9, 17] can considerably impact on data integrity, reliability, and long-term availability. To address these risks, our framework utilizes the redundant storage methods, CID validation, and decentralized fault tolerance mechanisms. To assess the resistance capability of storage layer attacks, B-PACIoT was compared with alternatives like Storj [29], IPFS Cluster [5], and Filecoin [19].

Simulated Attacks

- **CID Spoofing**: attackers try to modify the stored CIDs to redirect the retrieval requests to tampered or unauthorized EHRs [26].
- **IPFS Node Compromise**: adversaries attempt to take the control on decentralized storage nodes for adversarial manipulations [23].
- **Data Deletion Attack**: malicious actors try to remove the EHR files from IPFS to test redundant storage protocols [40].

Performance Evaluation Metrics

The storage security of B-PACIoT was evaluated across three critical metrics are:

- **Storage Failure Rate (%)**: measures the probability of data retrieval failures due to the adversarial manipulations.
- **Retrieval Delay (ms)**: evaluates how quickly the EHRs are retrieved under attack conditions.
- **Data Availability Rate (%)**: assesses how effectively the EHRs remain accessible during the storage disruptions.

The storage layer attack simulation results are detailed in Table 13, which presents the B-PACIoT's performance against alternative storage models.

Table 13. B-PACIoT's storage security performance.

Metric	Model	CID spoofing	IPFS node compromise	Data deletion attack
Storage failure rate (%)	Storj	3.0 ± 1.2	4.5 ± 1.4	2.9 ± 1.1
	B-PACIoT	0.3 ± 0.1	0.5 ± 0.2	0.2 ± 0.1
	Mitigation (%)	90.0 ± 1.3	88.9 ± 1.5	93.1 ± 1.2
Retrieval delay (ms)	IPFS cluster	28.5 ± 2.3	35.8 ± 2.7	26.1 ± 2.1
	B-PACIoT	5.2 ± 1.1	6.4 ± 1.3	4.5 ± 1.0
	Reduction (%)	81.8 ± 1.4	82.1 ± 1.6	82.8 ± 1.3
Data availability rate (%)	Filecoin	80.0 ± 1.4	79.5 ± 1.5	82.3 ± 1.3
	B-PACIoT	97.0 ± 1.3	96.0 ± 1.5	98.0 ± 1.2
	Improvement (%)	21.3 ± 1.1	20.7 ± 1.3	19.1 ± 1.0

Results and Discussion

While conducting the storage layer attack simulations,

B-PACIoT demonstrated impressive advancements in storage security and retrieval efficiency. It also outperformed the alternative models in performance due to its robust triplicate replication strategy and CID validation mechanism. Simulation results shown that our framework reduced storage failure rates to 0.3%, which is 90.0% improvement over storj's 3.0% failure rate. The triplicate replication distribution strategy across nodes assured that no data was lost, even the node fails to respond.

Similarly, the retrieval delays were also optimized to 5.2 ms, which is 81.8% improvement from the 28.5 ms delay of IPFS Cluster. As part of IPFS distribute management strategy [23], B-PACIoT distributes the EHRs across multiple geographic locations to reduce the bottlenecks and improving load balancing. Additionally, our framework maintained 97.0% data availability rate, which is better than Filecoin (80.0%) remained the data accessible under data disruptions. Figure 10 presents the differences between our B-PACIoT and other models in terms of storage layer attacks using respective metrics.

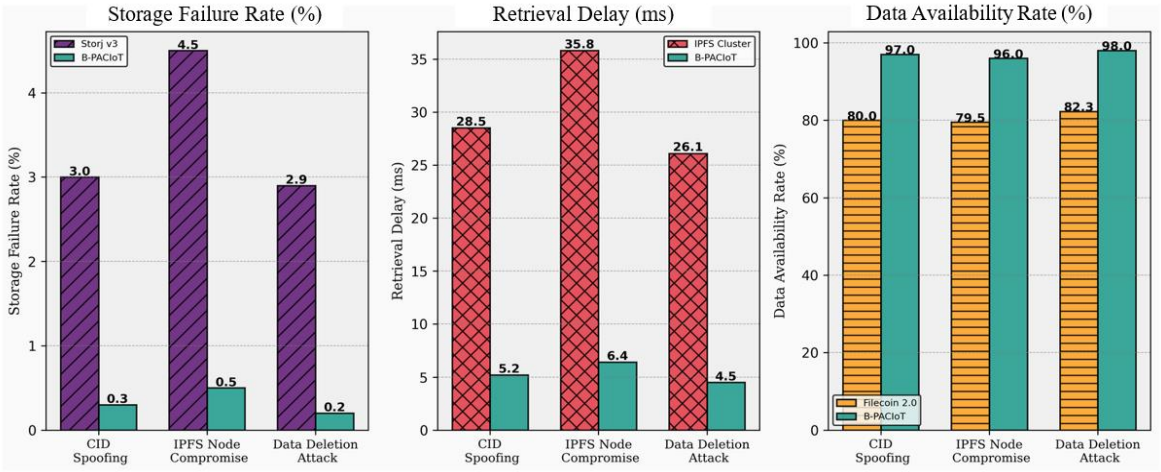

Figure 10. Storage security enhancement: failure prevention, retrieval efficiency, and availability.

The results presented in this chapter highlights that our B-PACIoT is offering the impressive resilience against the adversarial attacks, outperforming the baseline models in areas like latency reduction, tampering prevention, unauthorized access control, and decentralized storage reliability. With the integration of AES-128 encryption, zk-Rollups [6], CP-ABE-based access control, and IPFS-based decentralized storage, the B-PACIoT guarantees strong EHR protection in blockchain based IoT healthcare environments. These findings emphasize that our B-PACIoT is a suitable future-proof solution for secure and scalable EHR data management.

6.6. Comparative Evaluation Using Accuracy, Precision, Recall, and F1-Score

At final we conducted the comparative evaluation for holistic evaluation of our B-PACIoT performance in detecting and resisting the real-world operational scenarios such as access control policy enforcement, user authentication, and attack detection and mitigation. The experiments were conducted using four-fold testing method, where each fold tested with 1000 test cases including legitimate and adverse cases. The purpose of this test is to check the potentiality of each framework in assuring that only authorized users allowed to access and retrieve the EHRs without compromising the privacy and data integrity under several attack scenarios. We used Metasploit tool to simulate the attack vectors such as spoofing, data tampering, and unauthorized access attempts. Similarly, Open Worldwide Application Security Project Zed Attack Proxy (OWASP ZAP) used for generating the web-based vulnerabilities during EHR access transactions. These tools generated test cases were tested against the prominent existing frameworks are HealthChain [21], FHIR_E [54], DITrust Chain [1] and our B-PACIoT. At each fold level the test results are measured using accuracy, precision, recall and Fi-score metrics and the mean results of them also presented (see Table 14).

Table 14. Comparative analysis of accuracy, precision, recall, and F1-Score across 4-fold simulations.

Framework	Fold	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
B-PACIoT	Fold-1	91.8	92.7	90.6	91.4
	Fold-2	94.5	95.2	92.8	94.0
	Fold-3	96.1	96.4	94.3	95.1
	Fold-4	95.3	94.9	93.7	94.6
	Mean	94.4	94.8	92.9	93.8
HealthChain	Fold-1	85.7	87.4	84.1	85.6
	Fold-2	89.3	90.1	86.7	88.2
	Fold-3	91.1	91.6	89.3	90.4
	Fold-4	88.5	89.7	87.1	88.4
	Mean	88.7	89.7	86.8	88.2
FHIR_E	Fold-1	83.2	85.0	81.7	82.9
	Fold-2	85.5	86.4	83.9	84.7
	Fold-3	82.3	84.2	80.1	81.8
	Fold-4	82.5	84.0	80.8	82.1
	Mean	83.4	84.9	81.6	82.9
DITrust chain	Fold-1	86.1	87.8	84.3	85.9
	Fold-2	90.4	89.5	87.0	88.2
	Fold-3	81.4	82.7	80.0	81.3
	Fold-4	87.3	88.6	85.1	86.6
	Mean	86.3	87.2	84.1	85.5

These comparative results are emphasizing that our B-PACIoT significantly outperformer the selected baseline models in all folds across all metrics. The high mean accuracy of 94.4% of B-PACIoT with 93.8% of F1-score indicating the superiority of our model in handling the authorized and unauthorized activities across access control and attack detection use cases. On other hand, the HealthChain and DITrust Chain frameworks also showed reasonable performance but they were limited by their relatively rigid access models and lack of privacy-preserving authentication mechanisms. Although interoperable, the FHIR_E showed the weakest performance in this case, due to its static access control and higher reliance on centralized components. Our framework remained at the top level as it has the robust and hybrid fine-grained access control, which is implemented through the integration of Edge-Assisted AES-128 Encryption, CP-ABE with dynamic smart contracts, zk-SNARKs-based authentication, zk-Rollups for scalability and decentralized off-chain IPFS storage.

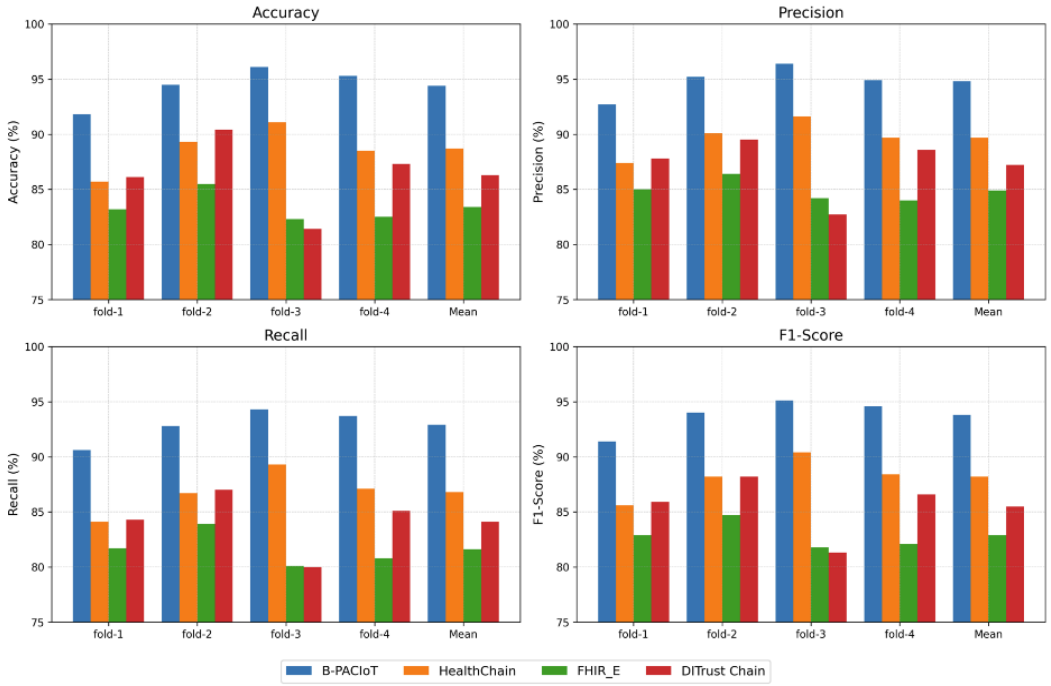

Figure 11. Evaluation of accuracy, precision, recall, and F1-score over 4-fold simulations for B-PACIoT and baselines.

The fold-wise comparative bar chart (see Figure 11) is visually presenting the performance of all four frameworks across four evaluation metrics presented in Table 14. Each subplot of this main graph highlights the individual fold results along with the mean value for each framework, which is offering a clear view of consistency and variation in performance.

The comparative analysis results in all dimension are confirming that our B-PACIoT's architecture is not only technically robust but also practically deployable in real-world and resource constrained IoT healthcare environments. Our framework provides a unified IoT driven blockchain healthcare EHR management solution that is accurate, privacy-preserving, efficient, and scalable, which is offering clear advantages over former frameworks of healthcare.

6.7. Regulatory Compliance Mapping to GDPR and HIPAA

Ensuring the compliance with established healthcare privacy regulations is critical for any EHR management system. The B-PACIoT framework was designed with explicit alignment to the European Union's GDPR and the United States HIPAA. Table 15 presents a mapping between the core architectural components of B-PACIoT and the relevant GDPR/HIPAA provisions, followed by a discussion of how these features enable legal compliance.

The mapping demonstrates that each B-PACIoT layer not only serves a technical function but also supports compliance with legally mandated privacy and auditability requirements.

GDPR alignment: features such as CP-ABE-based fine-grained access control and revocation mechanisms directly address rights to access, erasure, and objection, while zk-SNARK authentication supports privacy by design. Immutable blockchain logs provide evidence for audit trails, fulfilling integrity and confidentiality obligations.

HIPAA alignment: the hybrid blockchain architecture, combined with decentralized encrypted storage, enforces the HIPAA Security and Privacy Rules by ensuring confidentiality, integrity, and availability of protected health information (PHI). Unique identification through zk-SNARK proofs, combined with continuous auditing, meets HIPAA's access control and incident response requirements.

By explicitly mapping technical controls to legal provisions, B-PACIoT bridges the gap between cyber security architecture and regulatory compliance, ensuring that performance gains do not come at the expense of legal readiness.

Table 15. Mapping of B-PACIoT components to GDPR and HIPAA requirements.

B-PACIoT layer/component	Relevant GDPR clauses	Relevant HIPAA rules	Compliance mechanism in B-PACIoT
Blockchain layer (hybrid chain, immutable logs)	Art. 5(1) (f)-Integrity and confidentiality; Art. 30-Records of processing	Security Rule §164.312(b)-Audit controls	Immutable transaction records for all EHR access events; on-chain proof logs for non-repudiation and auditability.
zk-SNARK verification	Art. 25-Data protection by design; Art. 32-Security of processing	Security Rule §164.312(a)(2)(i)-Unique user identification	Privacy-preserving authentication without revealing personal identifiers; ensures only authorized proofs are verified.
zk-Rollup aggregator	Art. 5(1)(c)-Data minimization	Security Rule §164.306(a)-General security standards	Batches transaction proofs, reducing on-chain exposure of personal health data.
Access control layer (CP-ABE)	Art. 15-Right of access; Art. 17-Right to erasure	Privacy Rule §164.524-Access of individuals to PHI	Fine-grained, attribute-based decryption ensures patients and authorized clinicians can access records, while revocation enforces erasure rights.
CP-ABE revocation mechanism	Art. 17-Right to erasure; Art. 21-Right to object	Security Rule §164.312(a)(1)-Access control	Revocation policies ensure that access keys can be invalidated instantly upon request or role change.
Storage layer (IPFS with replication)	Art. 5(1) (e)-Storage limitation; Art. 32-Security of processing	Security Rule §164.310(d)(2)-Device/media controls	Decentralized off-chain storage with triplicate replication for fault tolerance; encrypted at rest to prevent data leaks.
Audit and monitoring subsystem	Art. 33-Breach notification	Security Rule §164.308(a)(6)-Security incident procedures	Automated breach detection triggers real-time alerts and logs incident details for reporting.

7. Conclusions and Future Works

The B-PACIoT framework is a transformative approach in blockchain-based IoT healthcare systems, designed to tackle the EHR management limitations such as security, scalability, and efficiency. By combining the AES-128+CP-ABE encryption, outsourced edge decryption, zk-SNARK-based authentication, and zk-Rollup-based transaction batching, our B-PACIoT framework assures the scalable and secure EHR management data while satisfying the privacy regulations such as GDPR and HIPAA. Extensive experiments compared the B-PACIoT's performance with existing blockchain-based EHR systems, to prove the framework efficiency in EHR tampering prevention, access control, and storage management. In addition, security evaluation experiments showcased the B-PACIoT resistance against various adversarial attacks, including blockchain hash tampering, IPFS storage corruption, and unauthorized access. From results, our framework's IPFS-based decentralized storage mechanism reduces the on-chain storage costs by 89%, and making it scalable for large scale EHR management applications. With a throughput of 1,150 TPS, mean latency of 210 ms, and 99.8% fault tolerance, our B-PACIoT outperforms the existing blockchain-based EHR systems. The framework's edge-assisted decryption helps to reduce the computational burden at low configured IoT devices and assures the energy-efficient and low-latency operations.

Future research can explore the efficient post-quantum cryptographic techniques to enhance CP-ABE security against the quantum attacks. Focusing on zk-Rollups optimization for faster batch processing and managing the failed requests in batch can improve the scalability and reduce the transaction costs. Additionally, federated learning integration with decentralized medical data analysis can enhance privacy while enabling AI-driven insights.

References

[1] Abou-Nassar E., Iliyasu A., El-Kafrawy P., Song O., and et al., "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," *IEEE Access*, vol. 8, pp. 111223-111238, 2020. https://doi.org/10.1109/ACCESS.2020.2999468

[2] Akkaoui R., Hei X., and Cheng W., "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange," *IEEE Access*, vol. 8, pp. 113467-113486, 2020. https://doi.org/10.1109/access.2020.3003575

[3] Akkas M., Sokullu R., and Cetin H., "Healthcare and Patient Monitoring Using IoT," *Internet of Things*, vol. 11, pp. 100173, 2020. https://doi.org/10.1016/j.iot.2020.100173

[4] Ali A., Manar H., Mabrouk M., and Zrigui M., "Proposal of a Modified Hash Algorithm to Increase Blockchain Security," *in Proceedings of the Procedia Computer Science*, Athens, pp. 3265-3275, 2023. https://doi.org/10.1016/j.procs.2023.10.320

[5] Al-Sumaidaee G., Alkhudary R., and Zilic Z., "Decentralized Storage for Big Data in Healthcare Between Reality and Ambition: IPFS and Sia," *in Proceedings of IEEE International Conference on Big Data (Big Data)*, Osaka, pp. 6578-6580, 2022. https://doi.org/10.1109/bigdata55660.2022.10020670

[6] Anusuya R., Dhanaraj K., Ghanasiyaa S., Harshini K., and et al., "Privacy-Preserving Blockchain-Based EHR Using ZK-Snarks," *in Proceedings of the Communications in Computer and Information Science*, Coimbatore, pp. 109-123, 2022. https://doi.org/10.1007/978-3-031-15556-7_8

[7] Attaran M., "Blockchain Technology in Healthcare: Challenges and Opportunities,"

International Journal of Healthcare Management, vol. 15, no. 1, pp. 70-83, 2022. https://doi.org/10.1080/20479700.2020.1843887

[8] Azbeg K., Ouchetto O., and Andaloussi S., "Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1515-1527, 2022. https://doi.org/10.1109/tcss.2022.3186945

[9] Azbeg K., Ouchetto O., and Andaloussi S., "BlockMedCare: A Healthcare System Based on Iot, Blockchain and IPFS for Data Management Security," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 329-343 2022. https://doi.org/10.1016/j.eij.2022.02.004

[10] Bin Saleem W., Ali H., and AlSalloom N., "A Framework for Securing EHR Management in the Era of Internet of Things,"*in Proceedings of the 3rd International Conference on Computer Applications and Information Security*, Riyadh, pp. 1-5, 2020. https://doi.org/10.1109/iccais48893.2020.9096788

[11] Chawla S. and Gupta N., "Performance Analysis of the Proxy-Based and Collusion-Resistant Revocable CPABE Framework," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 35, no. 1, pp. 378-387, 2024. https://doi.org/10.11591/ijeecs.v35.i1.pp378-387

[12] Datta j., Ananya S., Deepak M., Mungara N, and Sarasvathi V., "Framework for Brute-Force Attack Detection Using Federated Learning," *in Proceedings of the Broadband Communications, Networks and Systems*, Hyderabad, pp. 64-73, 2025. https://doi.org/10.1007/978-3-031-81168-5_7

[13] De Oliveira M., Verginadis Y., Reis L., Psarra E., and et al., "AC-ABAC: Attribute-Based Access Control for Electronic Medical Records During Acute Care," *Expert Systems with Applications*, vol. 213, pp. 1-12, 2023. https://doi.org/10.1016/j.eswa.2022.119271

[14] Dhulavvagol P., Totad S., and Anagal A., "SHARD-FEMF: Adaptive Forensic Evidence Management Framework Using Blockchain Sharding and IPFS," *The International Arab Journal of Information Technology*, vol. 21, no. 2, 2024. DOI:https://doi.org/10.34028/iajit/21/2/1

[15] Dragnoiu A. and Olimid R., "Towards an Identity Management Solution on Arweave," *arXiv Preprint*, vol. arXiv:2412.13865v3 pp. 1-38, 2024. https://doi.org/10.48550/arxiv.2412.13865

[16] Egala S., Pradhan A., Dey P., BadarlaV., and Mohanty S., "Fortified-Chain 2.0: Intelligent Blockchain for Decentralized Smart Healthcare System," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12308-12321, 2023. https://doi.org/10.1109/jiot.2023.3247452

[17] ElSayed Z., Abdelgawad A., and Elsayed N., "Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions," *arXiv Preprint*, vol. arXiv:2501.11250v1, pp. 1-7, 2025. https://doi.org/10.48550/arxiv.2501.11250

[18] Gao H., Huang H., Xue L., Xiao F., and Li Q., "Blockchain-Enabled Fine-Grained Searchable Encryption With Cloud-Edge Computing for Electronic Health Records Sharing," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 18414-18425, 2023. https://doi.org/10.1109/jiot.2023.3279893

[19] Guidi B., Michienzi A., and Ricci L., "Evaluating the Decentralisation of Filecoin," *in Proceedings of the 3rd International Workshop onDistributed Infrastructure for the Common Good*, pp.13-18, 2022. https://doi.org/10.1145/3565383.3566108

[20] Hamouid K. and Mohammedi M., "Dynamic and Flexible Access Control for IoT-Enabled Smart Healthcare," *International Symposium on Networks, Computers and Communications HAL (Le Centre pour la Communication Scientifique Directe)*, Doha, Qatar, pp. 1-6, 2023. https://doi.org/10.1109/isncc58260.2023.10323989

[21] Husnain G., Ullah Z., Mohmand M., Qadir M., and et al., "HealthChain: A Blockchain-Based Framework for Secure and Interoperable Electronic Health Records (EHRs)," IET Communications, vol. 18, no. 19, pp. 1451-1473 2024. https://doi.org/10.1049/cmu2.12839

[22] Immanuel S., Jenefa A., Naveen V., Santhiya P., and et al., "CloudSec Innovation: Enhanced Data Security with Multi-Tier Encryption Systems," *in proceedings of the 8th International Conference on Inventive Systems and Control*, Coimbatore, pp. 582-587, 2024. https://doi.org/10.1109/icisc62624.2024.00102

[23] Jayabalan J. and Jeyanthi N., "Scalable Blockchain Model Using Off-Chain IPFS Storage for Healthcare Data Security and Privacy," *Journal of Parallel and Distributed Computing*, vol 164, no. 8, pp. 152-167, 2022. https://doi.org/10.1016/j.jpdc.2022.03.009

[24] Jun M., "Platform Framework for Blockchain-Enhanced Healthcare AIoT Systems," *Frontiers in Communications and Networks*, vol. 6, pp. 1-18, 2025. https://doi.org/10.3389/frcmn.2025.1538965

[25] Jyosthna P., Mandapati A., Teja M., Ray S., and Kumar B., "Enhancing Security and Flexibility with Combined RBAC and ABAC Access Control Models," *in Proceedings of the 10th International Conference on Communication and Signal Processing*, Melmaruvathur, pp. 576-581, 2024. https://doi.org/10.1109/iccsp60870.2024.10543482

[26] Kacem T., Tossou S., and Muir A., "Detecting Cyber Attacks in Healthcare IoT Systems," *in Proceedings of the International Conference on AI*

x Data and Knowledge Engineering, Tokyo, pp. 80-85, 2024. https://doi.org/10.1109/aixdke63520.2024.00022

[27] Kaushal R. and Kumar N., "Exploring Hyperledger Caliper Benchmarking Tool to Measure the Performance of Blockchain Based Solutions," *in Proceedings of the 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, Noida, pp. 1-6, 2024. https://doi.org/10.1109/icrito61523.2024.10522188

[28] Kumar M., Mukherjee P., Verma S., Kavita., and et al., "BBNSF: Blockchain-Based Novel Secure Framework Using RP2-RSA and ASR-ANN Technique for IoT Enabled Healthcare Systems," *Sensors*, vol. 22, no. 23, pp. 1-16, 2022. https://doi.org/10.3390/s22239448

[29] Kundu R., Gehrmann C., and Kihl M., "A Comprehensive Robustness Analysis of Storj DCS Under Coordinated DDoS Attack," *in Proceedings of the IEEE 29th International Conference on Parallel and Distributed Systems*, Ocean Flower Island, pp. 659-666, 2023. https://doi.org/10.1109/icpads60453.2023.00102

[30] Liang X., Liu Y., and Ning J., "An Access Control Scheme with Privacy-Preserving Authentication and Flexible Revocation for Smart Healthcare," *IEEE Journal of Biomedical and Health Informatics*, vol. 28, no. 6, pp. 3269-3278, 2024. https://doi.org/10.1109/jbhi.2024.3391218

[31] Mohanakrishnan S. and Gokila S., "Etherdoc: Ensuring Security and Integrity for Digital Certificates using Blockchain," *in Proceedings of the International Conference on Visual Analytics and Data Visualization*, Tirunelveli, pp. 218-225. 2025. https://doi.org/10.1109/icvadv63329.2025.10960954

[32] Mole J. and Shaji R., "Ethereum Blockchain for Electronic Health Records: Securing and Streamlining Patient Management," *Frontiers in Medicine*, vol. 11, pp. 1-17, 2024. https://doi.org/10.3389/fmed.2024.1434474

[33] Moody G. and Mark R., "The Impact of the MIT-BIH Arrhythmia Database," *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, no. 3, pp. 45-50, 2001. https://doi.org/10.1109/51.932724

[34] Myrzashova R., Alsamhi S., Shvetsov A., Hawbani A., and Wei X., "Blockchain Meets Federated Learning in Healthcare: A Systematic Review with Challenges and Opportunities," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14418-14437, 2023. https://doi.org/10.1109/JIOT.2023.3263598

[35] Ogundoyin I., Ogunbiyi D., Adebanji S., and Okeyode Y., "Comparative Analysis and Performance Evaluation of Cryptographic Algorithms," *UNIOSUN Journal of Engineering and Environmental Sciences*, vol. 4, no. 1, pp. 39-47, 2022. https://doi.org/10.36108/ujees/2202.40.0140

[36] Pal S., Hitchens M., Varadharajan V., and Rabehaja T., "Fine-Grained Access Control for Smart Healthcare Systems in the Internet of Things," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 4, no. 13, pp. 1-18, 2018. https://doi.org/10.4108/eai.20-3-2018.154370

[37] Panda S. and Satapathy S., "An Investigation into Smart Contract Deployment on Ethereum Platform Using Web3.js and Solidity Using Blockchain," *in Proceedings of the Advances in Intelligent Systems and Computing*, vol. 1407, pp. 549-561, 2021. https://doi.org/10.1007/978-981-16-0171-2_52

[38] Pathak A., Al-Anbagi I., and Hamilton H., "Blockchain-Enhanced Zero Knowledge Proof-Based Privacy-Preserving Mutual Authentication for IoT Networks," *IEEE Access*, vol. 12, pp. 118618-118636, 2024. https://doi.org/10.1109/access.2024.3450313

[39] Paul J., "Distributed Serverless Architectures on AWS," *Apress*, 2023. https://doi.org/10.1007/978-1-4842-9159-7

[40] Praseed A. and Thilagam P., "Multiplexed Asymmetric Attacks: Next-Generation DDoS on HTTP/2 Servers," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1790-1800, 2020. https://doi.org/10.1109/tifs.2019.2950121

[41] Rashid M., Parah S., Wani A., and Gupta S., "Securing E-Health IoT Data on Cloud Systems Using Novel Extended Role Based Access Control Model," *in Proceedings of the Internet of Things*, Springer, pp. 473-489, 2020. https://doi.org/10.1007/978-3-030-37468-6_25

[42] Rizzardi A., Sicari S., Jesus F., Cevallos M., and Coen-Porisini A., "IoT-Driven Blockchain to Manage the Healthcare Supply Chain and Protect Medical Records," *Future Generation Computer Systems*, vol. 161, no. 1, pp. 415-431, 2024. https://doi.org/10.1016/j.future.2024.07.039

[43] Rohini K, Subramanian R., and Soman G., "Improving Data Security and Scalability in Healthcare System Using Blockchain Technology," *Scalable Computing Practice and Experience*, vol. 25, no. 5, pp. 3440-3452, 2024. https://doi.org/10.12694/scpe.v25i5.3164

[44] Salunkhe V. and Rajkumar S., "Integrating Zk-Rollup and Blockchain for Scalable and Secure Healthcare Data Management," *SSRN*, pp. 1-21, 2025. https://doi.org/10.2139/ssrn.5070850

[45] Samantray B. and Reddy H., "A Novel Secure Supply Chain for Smart Healthcare Systems: An Approach to Leverage Blockchain, Keccak-256, and ZKP for Drug Safety Assurance," *Peer-to-*

Peer Networking and Applications, vol. 18, no. 1, pp. 1-17, 2024. https://doi.org/10.1007/s12083-024-01832-6

[46] Shah W., "Preserving Privacy and Security: A Comparative Study of Health Data Regulations-GDPR vs. HIPAA," *International Journal for Research in Applied Science and Engineering Technology*, vol. 11, no. 8, pp. 2189-2199, 2023. https://doi.org/10.22214/ijraset.2023.55551

[47] Shi G., Qi M., Zhong Q., Li N., and et al., "MedAccessX: A Blockchain-Enabled Dynamic Access Control Framework for IoMT Networks," *Sensors*, vol. 25, no. 6, pp. 1-28, 2025. https://doi.org/10.3390/s25061857

[48] Singh M., Kumar S., Garg T., and Pandey N., "Penetration Testing on Metasploitable 2," *International Journal of Engineering and Computer Science*, vol. 9, no. 5, pp. 25014-25022, 2020. https://doi.org/10.18535/ijecs/v9i05.4476

[49] Sowjanya K., Dasgupta M., and Ray S., "A Lightweight Key Management Scheme for Key-Escrow-Free ECC-Based CP-ABE for IoT Healthcare Systems," *Journal of Systems Architecture*, vol. 117, pp. 102108, 2021. https://doi.org/10.1016/j.sysarc.2021.102108

[50] Sridhar S., Ascigil O., Keizer N., Genon F., and et al., "Content Censorship in the InterPlanetary File System," *arXiv Preprint*, vol. arXiv:2307.12212v2, pp. 1-17, 2023. https://doi.org/10.48550/arxiv.2307.12212

[51] Velmurugan S., Prakash M., Neelakandan S., and Martinson E., "An Efficient Secure Sharing of Electronic Health Records Using IoT-Based Hyperledger Blockchain," *International journal of Intelligent Systems*, vol. 2024, no.1, pp. 1-16, 2024. https://doi.org/10.1155/2024/6995202

[52] Waheed N., Rehman A., Nehra A., Farooq M., Tariq N., and et al., "FedBlockHealth: A Synergistic Approach to Privacy and Security in IoT-Enabled Healthcare Through Federated Learning and Blockchain," *in Proceedings of the IEEE Global Communications Conference*, Kuala Lumpur, pp. 3855-3860, 2023. https://doi.org/10.1109/globecom54140.2023.10437356

[53] Xie M., Fu Q., Hong H., Ren Z., and et al., "ABBDAC: A Novel Attribute-Based Blockchain Data Access Control Scheme in Cloud Environment," *IEEE Internet of Things Journal*, vol. 11, no. 24, pp. 40218-40228, 2024. https://doi.org/10.1109/jiot.2024.3452785

[54] Yang C., Kuo H., and Cheng H., "Ensuring FHIR Authentication and Data Integrity by Smart Contract and Blockchain Enabled NFT," *in Proceedings of the 7th International Conference on Medical and Health Informatics*, Kyoto, pp. 123-128, 2023. https://doi.org/10.1145/3608298.3608322

[55] Yuan M., Wang D., Zhang F., Wang S., and et al., "An Examination of Multi-Key Fully Homomorphic Encryption and Its Applications," *Mathematics*, vol. 10, no. 24, pp. 1-20, 2022. https://doi.org/10.3390/math10244678

[56] Zhang K., Patki N., and Veeramachaneni K., "Sequential Models in the Synthetic Data Vault," *arXiv Preprint*, vol. arXiv:2207.14406v1, pp. 1-17, 2022. https://doi.org/10.48550/arxiv.2207.14406

[57] Zhou L., Diro A, Saini A., Kaisar S., and Hiep P., "Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities," *Journal of Information Security and Applications*, vol. 80, pp. 1-20, 2024. https://doi.org/10.1016/j.jisa.2023.103678

[58] Zilong D. and Alobaedy M., "Blockchain-Based Healthcare Data Management: Analysis and Evaluation of Security, Scalability, and Compliance for Electronic Health Records (EHRs)," *in Proceedings of the 5th International Conference on Advances in Electrical, Electronics and Computing Technology*, Guangzhou, pp. 1-7, 2025. https://doi.org/10.1109/EECT64505.2025.10966949

Salma Begum S. is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Madha Institute of Engineering and Technology, Chennai, Tamil Nadu, India. She is currently pursuing her Ph.D. at Anna University. She holds a Bachelor of Engineering (B.E.) degree in Computer Science and Information Technology from Madina College of Engineering, Andhra Pradesh and a Master of Engineering (M.E.) degree in Computer Science and Engineering from Global College of Engineering and Technology, Andhra Pradesh. Her research interests include Blockchain, Fog Computing, Machine Learning and IoT.

J. Arokia Renjith received his Master of Engineering in Computer Science and Engineering from Anna University, Chennai in 2004 and Doctor of Philosophy in Computer Science and Engineering from Satyabhama University Chennai. He is currently working as a Professor in the Department of Computer Science and Engineering at Jeppiaar Engineering College, Chennai. His current research interests are Artificial Intelligence, Block Chain Security and Internet of Things for beyond 5g Communications. He is a Life Member in IEEE Member, CSI Member, ISTE Member.

Chandrasekar Armugam received his Bachelor of Engineering degree in Computer Science and Engineering from Angala Amman College of Engineering and Technology, Bharathidasan University in 1998, the Master of Engineering in Computer Science and Engineering degree from Arulmigu Kalasalingam College of Engineering, Madurai Kamaraj University in 2000 and the Ph.D. degree from Anna University,Chennai in 2010. He is currently working as a Professor in the Department of Computer Science and Engineering at St Joseph's College of Engineering, Chennai. His current research interests are Network Security, Cloud Security, Data mining, Artificial Intelligence and Big Data Analysis. He is a member of IEEE, Life Member in NCSSSASSOC, ISTE, CSI, ICSES, CRSI, IAENG, CSES, IACSIT and Fellow Member in IEI, ISCAI, ISRD.