PPO-LIGHT MED: A QUANTUM-SAFE BLOCKCHAIN-ENABLED LIGHTWEIGHT FRAMEWORK FOR SECURE EMR SHARING IN FOG-ASSISTED IOT–CLOUD ENVIRONMENTS

Sunil Bhutada[1], Koraboina Sindhuja[2]

[1]Professor, Department of Information Technology, Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, Telangana-501301.
[2]M.Tech Student, Department of Information Technology, Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, Telangana-501301.

sunil.b@sreenidhi.edu.in[1]
sindhujakoraboina@gmail.com[2]

Abstract: The rapid pace of the development of IoT-based healthcare systems requires efficient, secure, and privacy-sensitive systems of electronic medical records (EMRs) sharing. In an attempt to solve the issue of latency, computational cost, and unauthorized access, the present paper presents Policy-private outsourced Lightweight medical data security (PPO-LightMED), a policy-privately outsourced lightweight medical data security architecture, which is a combination of fog computing, blockchain, and quantum-safe cryptography. The model uses a quantum-safe verifiable outsourced ciphertext-policy attribute-based encryption (QS-VO-CPABE) scheme to provide an access control scheme on a fine-grained basis to offload heavy encryption workloads to fog nodes. Privacy-preserving access is decentralized through a zero-knowledge attribute verification (ZK-AttrVerify) protocol and ephemeral decryption tokens (EDTs) with the help of blockchain smart contracts. There is also an epoch-based revocation mechanism, which allows updating to policies and users dynamically without full re-encryption. Through experiment, there are substantial improvements: 55% reduction in encryption latency, 70% faster revocation and 30% higher throughput than any other models. PPO-LightMED provides a secure and scaled architecture as well as a quantum-resilient architecture for reliable healthcare data sharing in fog-assisted IoT cloud environments.

Keywords: Electronic medical records (EMR), Fog computing, Blockchain, Attribute-based encryption (ABE), Quantum-Safe access control

1. Introduction:

The combination of Internet of Things (IoT), fog computing, and cloud computing technologies transformed the digital healthcare ecosystem and provided continuous monitoring of patients, remote diagnosis, and real-time decision-making. EMRs can play a very important role in this transformation, as they offer a digital representation of patient information that can be accessed and shared between authorized entities in distributed healthcare networks. Nonetheless, with the growing reliance on the IoT-enabled healthcare infrastructure, sensitive medical data is exposed to severe security risks such as unauthorized access, data alteration, and privacy violations [1]. The global and distributed characteristics of IoT devices and the high rate of EMR transactions require a secure, scalable, and lightweight access control infrastructure to maintain the confidentiality and integrity of the data and maintain the healthcare regulations. The conventional cloud-based EMR management models have a number of weaknesses, such as high latency, reliance on centralized authorities and insider attacks [2]. To mitigate these drawbacks, a new layer between IoT and the cloud has been introduced with the term of fog computing, which provides localized data processing, low-latency processing, and proximity-based computing [3]. Fog nodes can provide real-time preprocessing and encryption and policy enforcement operations prior to sending data to the cloud to ease the strain on resource-constrained IoT devices. Nevertheless, the end-to-end data security as well as fine-grained access control across fog-assisted architectures is still not assured because of the dynamic user roles, policy modifications, and revocation overheads [4]. To address these security and privacy issues, there has been a surge in the use of Attribute-Based Encryption (ABE) schemes and especially Ciphertext-Policy Attribute-Based Encryption (CP-ABE) as a solution to healthcare data sharing. CP-ABE enables the owner of data to impose flexible access control specifications in terms of attributes so that users can be granted access on a fine-grained basis [5]. However, the conventional CP-ABE schemes are computationally demanding and cannot be used in the context of IoTs with limited energy and processing capabilities. Recently, efforts have tried to alleviate this through the use of outsourced decryption models, in which the heavy cryptographic operations are carried out by the fog or cloud nodes on behalf of the lightweight devices [6]. Though this has come about, the current solutions have still continued to encounter problems of verifiability of the outsourced operations, key revocation, and policy privacy leakage to the semi-trusted fog nodes.

In this regard, the blockchain technology brings up potential solutions to reinforce decentralized access control and immutable data auditing. The distributed ledger characteristics of blockchain can be used to safely store and confirm the EMR transactions, attribute updates or events of revocation without the use of central authority [7]. Additionally, the combination of smart contracts and blockchain allows the automatic implementation of access control policy, verification of authorization and safe issuance of keys. Nevertheless, blockchain systems should be well-calculated to avoid the leakage of user attributes and to take care of the calculation cost of large-scale healthcare systems [8].This paper suggests the Policy-Private Outsourced Lightweight Medical Data Security (PPO-LightMED) framework to overcome these challenges, which is an end-to-end secure model that combines Quantum-Safe Verifiable Outsourced CP-ABE (QS-VO-CPABE) with blockchain-enabled fine-grained access-control EMR sharing in fog-assisted fog-cloud environments. The system proposed uses a lattice-based post-quantum encryption to provide resilience to future attacks of quantum computing at a cost of computational efficiency. The module of privacy-preserving access verification and issuance of Ephemeral Decryption Tokens (EDTs) is done through a Zero-Knowledge Attribute Verification (ZK-AttrVerify) module that can safely interact with smart contracts. Moreover, it uses an epoch-based revocation mechanism in which immediate and selective revocation can be done without full re-encryption of all ciphertexts. PPO-LightMED Mog layer works with heavy crypto, partial de-encryption, and caching operations to provide real-time work at low latency. The blockchain layer serves as a trust anchor, which keeps transparent audit trails, revocation history, and access policy based on smart contracts. The proposed solution will guarantee the confidentiality, integrity, and privacy-preserving data sharing across heterogeneous healthcare systems by implementing fog computing, blockchain, and quantum-safe cryptography [9]. Through experimental validation, it will be proved that PPO-LightMED has better computational efficiency, lower energy usage, and safe scalability than the current lightweight ABE and blockchain-based healthcare models. Overall, the research paper can add to the body of knowledge by creating a secure, decentralized, and quantum-resistant architecture, which closes the security gap between the IoT, fog, and cloud layers, as well as offers a solid basis for the future healthcare data management systems [10].

2. Related and Background work

A number of CP-ABE schemes have been generated to overcome the issue of secure, scalable and fine-grained data sharing in IoT-enabled cloud environments. These plans allow data owners to implement flexible access policies so that only users with similar attributes can decrypt and access the data. Nevertheless, owing to the restricted computing power of the IoT devices, a large portion of the research has focused on lightweight CP-ABE architectures that offload the heavy cryptographic computations to the semi-trusted cloud or fog servers by outsourcing secure computation. This feature enables much local processing to be performed at a low cost and controls the data confidentiality, integrity and efficient access control in large-scale IoT-cloud infrastructures.

In [11], the authors introduced a secure fine-grained access control scheme to outsourced Electronic Health Records (EHRs) generated by the IoT in the fog-assisted cloud system, whose user revocation is optimized and load sharing is adaptive. Their protocol integrates pseudo-random encryption, symmetric encryption, ciphertext-policy attribute-based encryption (CP-ABE) and a graph-based model to enable scalable and efficient revocation. They load the fog nodes with the costly CP-ABE operations to minimize the computational load on the resource-constrained IoT devices. They suggest an algorithm of adaptive load sharing of the fog nodes to allocate computation and prevent any bottleneck or single point of failure. The combination of blockchain and smart contracts offers validity of data integrity and decentralized authentication. The authors support their design with the help of security analysis, comparative computational analysis, and experiments and prove that the costs of encryption, decryption, and revocation of their scheme are competitive and, in some aspects, more effective than the literature.

In [12], the authors suggested a lightweight, fine-grained access control scheme designed to work with cloud-fog architectures to share electronic medical records (EMR). The design is supposed to minimize the computational costs of IoT and edge devices by exploiting the concept of symmetric encryption and assigning more intensive cryptographic operations to the fog nodes. An attribute-based access control framework, featuring a fine-grained mechanism, enables flexible permissions by allowing the system to grant access to users based on their attributes, thereby precisely specifying which medical data can be viewed under specific circumstances. The scheme also uses effective revocation management schemes to accommodate dynamic user revocation without necessarily re-encrypting the stored records. The authors also incorporate measures to ensure the integrity and confidentiality of data during transit and storage. As evidenced by the authors' assessments (security analysis and performance assessment), the proposed scheme offers a favorable trade-off between security and efficiency compared to previous methods, making it suitable for use in resource-constrained healthcare IoT settings.

In [13], the authors suggested a blockchain-based fog computing architecture that can be used to support secure distributed storage of IoT applications, particularly with sensitive data like biometric and medical records. They are designed based on the Elliptic Curve Diffie-Hellman (ECDH) protocol to provide a secure key agreement between the fog nodes and the IoT devices to provide confidentiality to the data storage and recoveries. They use a data format based on a Merkle tree to verify the integrity of the data and tampering and anchor these verifications in the blockchain layer to ensure the immutable auditability. They perform a formal security analysis with AVISPA tools to check resistance against the usual threats. Comparisons of their performance reveal that their scheme is more favorable than the traditional solutions (AES, RSA, ABE, and hybrid) in terms of the computational cost, communication overhead, and the overall cost of execution, which makes it appropriate to the IoT environment with limited resources.

In [14], the authors suggested BACP-IeFC, a blockchain-guided access control protocol of IoT appliances that communicate through a fog computing setting, focusing on the secure key management and control without the involvement of trusted parties. Their protocol has supported intra-network, inter-network and even mobile device communications. It is based on Elliptic Curve Cryptography (ECC) and hash chains to generate keys and perform lightweight operations, and session keys generated by fog servers are stored on a permissioned blockchain to offer decentralized authentication and auditing. The authors provide informal as well as formal security analysis using the Real-or-Random (ROR) model and ProVerif tool to demonstrate that BACP-IeFC is resilient to known attacks and provides session key security. According to performance assessments based on the MIRACL library, it has been seen that it has enhanced computational overhead, communication, cost, storage, energy consumption, and latency as compared to proposals available. Moreover, the scheme is run on Truffle on Ethereum 2.0, powered by a light proof-of-authority (PoA) consensus system with promising registration, authentication, and block preparation times.

In [15], the authors put forward multiparty authorization and a blockchain-based access control scheme to secure the sharing of electronic medical records (EMRs) in distributed healthcare systems. They store encrypted health record information in cloud storage and place metadata, access policies, and authorization records on a blockchain, which ensures tamper resistance and decentralization. The multiparty authorization scheme requires multiple entities such as patients, doctors, and institutions to authenticate access requests, thereby enhancing the robustness of the access control process. The system is automated to authenticate and authorize permissions using smart contracts. Their security analysis indicates that they are resistant to frequent threats, including unauthorized access and data manipulation. Performance analysis reveals that the scheme has satisfactory computation and communication overheads and is applicable to practical EMR sharing in the real world.

In [16], the authors introduced an EMR sharing model that integrates blockchain technology with quantum key technique that helps to improve security and overcome the emerging threats (e.g., quantum attacks). Electronic medical records are encrypted and stored in a distributed storage layer in their design, and access control metadata, search indices and authorization logs are stored on a permissioned blockchain, which ensures immutability, tamper-resistance and auditability. This is enhanced with a quantum-safe key agreement or quantum key mechanism to protect the potential future cryptographic compromises so that the encryption keys are safe even with quantum adversaries. They also facilitate fine-grained access control whereby only users who have the right attributes and have correct attributes can decrypt records. The authors prove the security of the scheme through formal analysis and performance comparison with the existing schemes, demonstrating that their scheme can achieve reasonable computational and communication costs and enhance privacy, integrity, and quantum resistance.

3. Proposed methodology

The proposed system architecture PPO-LightMED provides a secure, fine-grained, and blockchain-supported system architecture to share electronic medical records (EMRs) between the IoT, fog, and cloud infrastructures in Figure 1. It is created in such a way that it will provide confidentiality, preservation of privacy and be able to be audited as well as keep the computational costs of the IoT devices low. The architecture has four major layers, namely IoT, Fog, Cloud, and Blockchain sub-modules that have specific sub-modules that together bring forth secure and efficient EMR management.

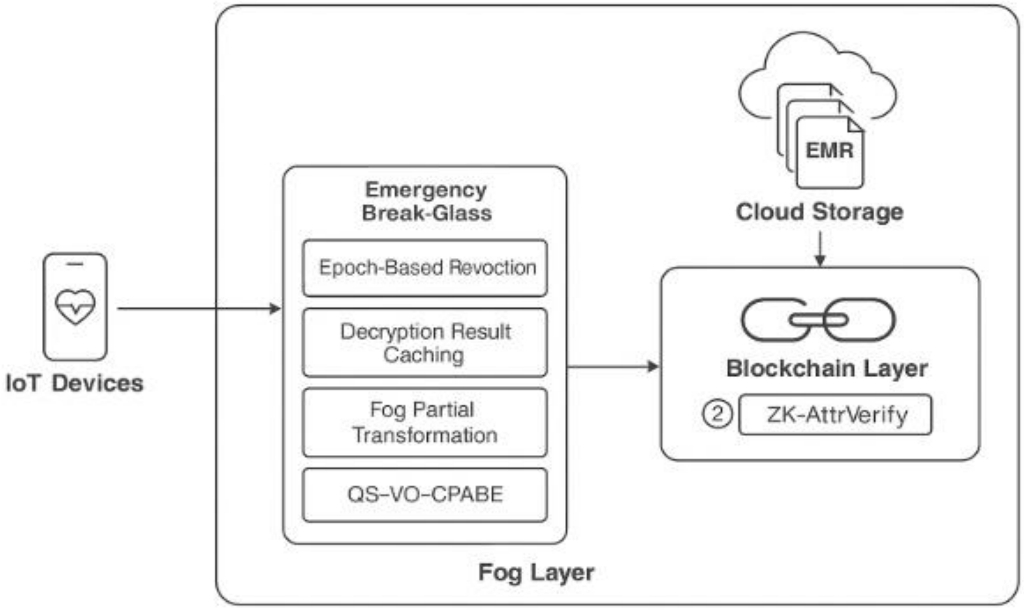

Figure 1: Proposed model methodology

3.1 IoT Layer

The IoT Layer includes resource-constrained devices (sensors and medical equipment, wearables, bedside monitors, and infusion pumps) that use secure and lightweight data collection and minimal processing and send payloads to the fog layer. This layer's design objective includes limited on-device computation, high data provenance, and resistance to replay/tamper attacks, as well as ephemeral keying to avoid long-term secrets being stored on the device. The above objectives are attained by a small number of submodules and functional rules as depicted in Figure 2.

Data preprocessing and data acquisition. Physiological signals are sampled on devices at specified rates and locally filtered, compressed, and feature extracted on demand in order to minimize bandwidth and storage expenses. Privacy-preserving aggregation (e.g., sliding-window statistics) Preprocessing stages may optionally perform telemetry (not involving raw signals) by a privacy-preserving form of aggregation.Each time the device generates a measurement or a packet, it uses secure KDF (based on device entropy and counter/nonce) to generate an ephemeral session key. The encrypting of payloads is done using a symmetric authenticated cypher (recommended: AES-GCM-256) in order to assure confidentiality and integrity and to ensure minimal CPU load. The hybrid model (symmetric payload encryptions and ABE of session key on fog) preserves on-device cryptography low.

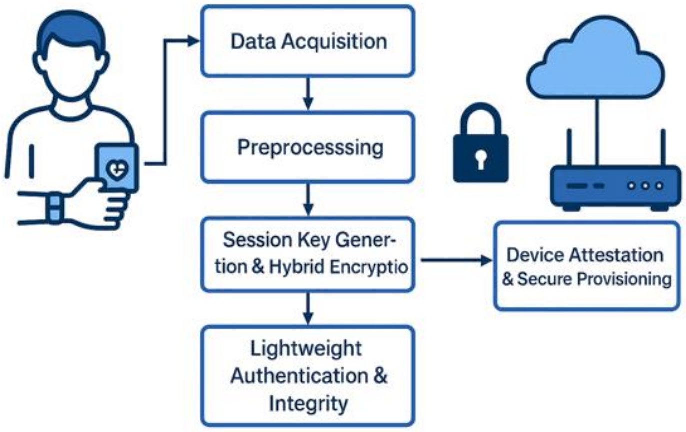
Data Acquisition
Preprocesssing
Session Key Gener-tion & Hybrid Encryptio
Device Attestation & Secure Provisioning
Lightweight Authentication & Integrity

Figure 2: IoT layer submodules and operational rules

Every encrypted packet is hashed with a small authenticity token: an HMAC (HMAC-SHA-256) keyed with the session key or an ED25519 signature in case a proof in the form of a public-key signature is necessary. They contain sequence numbers and nonces to avoid replaying out packets; there are timestamps and short TTLs to avoid delayed-delivery attacks that are common with opportunistic networks. Onboarding devices use immutable identifiers and manufacturer/root credentials. In the presence of one, a hardware root of trust (TPM/TEE) is utilized to secure privately accessible content and generate attestation statements to the fog node. OTA update support is ensured, signed with firmware to ensure that the integrity of the devices is maintained over time. Devices (e.g., with EDH/PSK + HMAC) authenticate with the fog gateway (via a mutually authenticated lightweight handshake) prior to providing data to verify the fog identity and exchange parameters to use during policy masking and uploading. This will not allow rogue nodes at the fog to collect sensitive EMRs. The IoT layer has a small energy and memory footprint: it only supports symmetric encryption, as well as small public-key signatures; it does not run CP-ABE or lattice operations on the device.

3.2. Fog layer

The fog layer in the suggested PPO-LightMED scheme is a key element that serves as a smart bridge between the constrained IoT equipment and the large-scale cloud computing framework. It is endowed with fine-grained access control, computationally expensive cryptographic functions, policy revocation, and the enforcement of verifiable and privacy-preserving information processing prior to sending information to the cloud. In contrast, the fog layer compared to the IoT layer is concerned with cryptographic heavy processing, policy analysis, and blockchain interplay, which guarantees efficiency and security of electronic medical records (EMR) management. The fog layer consists of five major submodules, each of which performs a dedicated security and performance role under the end-to-end system. These are:

QS-VO-CPABE: The verifiable outsourced cipher text policy attribute-based encryption (QS-VO-CPABE) engine is located at the heart of the fog layer. It is a submodule that implements a post-quantum ABE protocol, generally a lattice-based form of cryptography, to provide protection from quantum adversaries that pose a threat to bilinear pairing-based models. In cases where the encrypted data is being transferred by an IoT device, the fog node will use the masked access policy of the data owner and convert it into a policy tree, which will specify attributes necessary to decrypt it. The payload and the session key are encrypted by running the CP-ABE algorithm on the fog node to generate two ciphertexts, one of them encrypting the data and the other one encrypting the symmetric key. There is also a verifiability mechanism, which employs proof-of-correct-transformation tags, which makes sure that even in case a malicious node in the fog acts in a malicious way, it cannot modify and falsify ciphertexts without detection. These verifiable proofs are stored together with ciphertext metadata, which is used to perform blockchain-based verification at any stage explained in Algorithm1.

Algorithm 1: Pseudocode of QS-VO-CPABE

```
Owner/IoT:
  SK_i: =random ()
  C_sym := SymEnc(SK_i, D)
sign: =Sign (device_sk, H(C_sym))
  send_to_fog (C_sym, sign, metadata)
Fog (prepare for CP-ABE):
  Verify(sign)
  policy_mask: =MaskPolicy (P, r) # polynomial mask or randomized mapping
  ABE_ct: = QS_CPABE_Encrypt (P_mask, C_sym, PP)
  enc_SK := QS_CPABE_Encrypt(P_mask, SK_i, PP)
proof:= OutsourceGenProof(ABE_ct, enc_SK) # succinct proof of correct encryption
  store_to_cloud (ABE_ct, enc_SK, proof, metadata)
index: =H (ABE_ct || policy_mask_hash || metadata)
  post_index_to_chain(index, policy_mask_hash, ownerID, partition_info)
```

Fog partial transformation: It is an element that carries out partial decryption of ciphertexts to authorized users. After a user has received an Ephemeral Decryption Token (EDT) at the smart contract of the blockchain, the fog node authenticates it, ensuring it is valid and unexpired. The fog will subsequently subject a partial transformation to the stored ABE ciphertext to generate a transformed ciphertext (T_ct) that will maintain data confidentiality but lower considerably the computational cost of decryption at the user end. This enables the thin clients, like tablets or handheld devices, to decrypt efficiently without making such heavy cryptography calculations.

Decryption result caching: This submodule caches the recent transformation results in order to enhance performance and to reduce repetition of workload. In cases where two or more users with comparable sets of attributes or policies access the same medical record within a short period of time, the fog node relies on the already calculated transformations that are stored in cache memory. A scope hash and time-to-live (TTL) have been added to each result in the cache to avert replay attacks. This has the advantage of maximizing response times, minimizing computational load, and balancing load at peak periods of data access, like at the start of a hospital shift or an emergencyexplained in Algorithm2.

Algorithm 2: Pseudocode of Fog partial transform+ Decryption result reuse

```
Fog.partialTransform(ABE_ct, enc_SK, EDT):
  if not verifyEDT(EDT): reject
  cache_key: = H(ABE_index || EDT.scope_hash)
  if cache.exists(cache_key): return cache[cache_key]
  T_ct := QS_CPABE_PartialTransform(ABE_ct, EDT.partial_key)
  proof := GenTransformProof(T_ct, ABE_ct)  # optional verifiable step
  cache.set(cache_key, (T_ct, proof), TTL=EDT.exp)
```

```
 return (T_ct, proof)
```

Epoch-based revocation: The submodule takes care of dynamic revocation of users and policies at minimal re-encryption cost. Every ciphertext is linked to an epoch identifier that has to be stored on the blockchain. On revocation of a user, or an update of a policy, only the data partitions that are impacted are re-encrypted with an alternative epoch, without full re-encryption of the datasets. In the process of decryption, the epoch consistency of the token (EDT) and the current blockchain state is verified by the node of the fog, and the former does not allow the user with revoked access to obtain unauthorized access to legacy ciphertexts. It is a selective re-encryption that would enhance the scalability and provide real-time revocation enforcement.

Emergency break-glass: This submodule allows emergency access control in the case of critical care. In a break-glass policy, emergency access would be granted to approvals of certain amounts (k-of-n) of authoritative medical authorities. After the confirmation, the fog node will create a temporary emergency decryption session that has hard time constraints and records all the operations to the blockchain to audit them after the incident. This will make possible the possibility of having access that is urgent without affecting patient privacy and other compliance laws such as HIPAA.

3.3 Cloud layer

It is a data warehouse with a high capacity that would store encrypted EMRs, cryptographic metadata, and audit trails of the same, all of which are semi-trusted. Its main task is to provide secure data storage, scalability, and credible availability of medical information, as well as strict data confidentiality and integrity, in coordination with the fog layer and blockchain layer. Cloud Layer does not carry out any decryption actions and maintains the zero-trust security model, where the cloud is regarded to be untrusted with respect to plaintext data.EMRs and key ciphertexts created by the QS-VO-CPABE module are stored by the cloud layer as EMRs and key ciphertexts at the fog level.

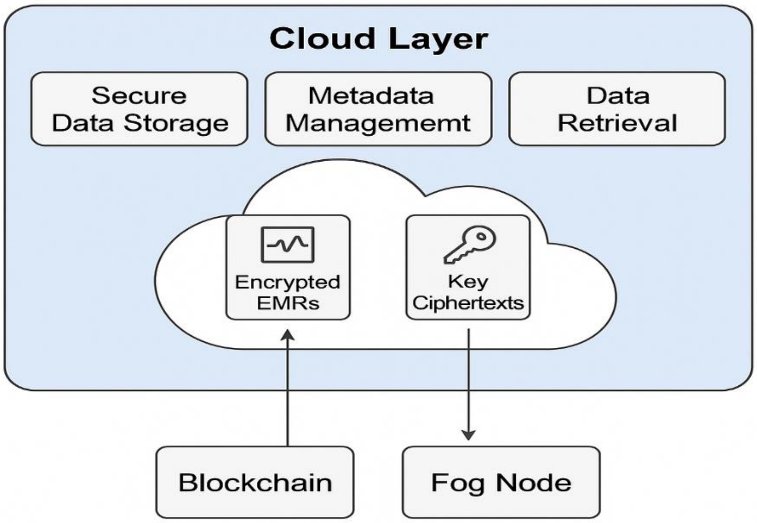

Figure 3: Cloud layer submodules

Every stored item has two key elements: the encrypted medical record (CEMR) and the encrypted session key (CSK). Such ciphertexts are point-referenced by hash-based pointers anchored to blockchain to provide referencing that is tamperproof. Any change or erasure of data stored can be instantly identified by the comparison of the computed hash and the one previously stored in the blockchain. To manage the scale of a healthcare setting, the cloud layer uses distributed storage clusters, which may have redundancy solutions, like erasure coding and multiple-region replication, to maintain the reliability of data and their ability to withstand node failure. The architecture also incorporates end-to-end encryption and role-based access gateways, severely restricting data retrieval interfaces as revealed in Figure 3.

Metadata management and provenance tracking: The records that have been uploaded come with a metadata set which contains the anonymized patient identifiers, time stamps, policy identifiers and the cryptography proof references. The provenance tracking and access auditing can be supported without revealing sensitive content with the help of this metadata. The fog node signs metadata and uploads it to the cloud digitally, which provides authenticity and non-repudiation of the origin. The blockchain only stores hash pointers and epoch identifiers, while the cloud stores the other metadata, which is cheaper and more efficient.

Data Retrieval and Synchronization: The encrypted record and metadata are fetched by the fog layer on the cloud depending on the blockchain index when a user requests an EMR. The Ephemeral decryption token (EDT) provided by the smart contract in the blockchain allows the fog to perform partial decryption and then transmits the transformed ciphertext to the user. This task is to make sure that even when the cloud is breached, the attacker cannot get any valuable information before having cryptographic credentials.

Linkage to blockchain and fog layers: The cloud layer will be used to run synchronously with the blockchain to verify integrity and with the fog to manage the encryption. Regular integrity verifications are carried out to make sure that the stored hashes in the cloud are validated by the entries in the blockchain, which maintains trust in the whole PPO-LightMED system.

3.4 Blockchain Layer

The PPO-LightMED architecture has a central system trust and audit component, the Blockchain Layer, which offers decentralized, immutable, and transparent control of access control, attribute verification, revocation, and event auditing. It also eradicates dependence on a centralized power by automating data by means of smart contracts to guarantee integrity and responsibility of EMR activities in the IoT-Fog-Cloud ecosystem.

Smart Contract-based Access control: Access control policies are fine-grained and are defined and enforced to all stakeholders of the system: patients, healthcare providers, and data analysts with the help of smart contracts.for Every EMR transaction (encryption, access, revocation, or update) is embodied in a blockchain transaction, which guarantees traceability and non-repudiation. The metadata hashes, the references to the session key, and the policy identifiers are stored in the blockchain when the IoT device submits new data using the fog node. This distributed registry ensures none of the entities can modify or falsify access logs in a way that is not beneficial to the network.

Zero-knowledge attribute checking (ZK-AttrVerify): The blockchain will support Zero-Knowledge Proof (ZKP) to improve the privacy of the user, allowing one to verify their access rights without disclosing their sensitive attributes. The ZK-AttrVerify smart contract validates user attributes through access requests using off-chain proofs that are verified on-chain. After authentication, the contract provides an Ephemeral Decryption Token (EDT)—a temporary, cryptographically signed object that permits temporary access to certain encrypted data by means of the cloud through the fog layer.

Epoch-based revocation and auditing: revocation of either users or attributes is done based on epoch counters so that enforcing revocation can be done immediately without the need to re-encrypt all the ciphertexts. The blockchain holds the updated epoch state of every policy, and any outmoded EDTs are automatically rejected. Statuses of authorization, access, revocation, and emergency overrides are recorded without alteration, which serves the healthcare regulations.

Essentially, the Blockchain Layer will offer a trustless security foundation, which guarantees decentralizedauthorization, verifiable privacy conservation, and auditability without tampering in the PPO-LightMED model of secure sharing of EMR.

4. Results and Discussion

The performance of the proposed PPO-LightMED framework was tested using simulation and experimental validation of a hybrid testbed based on Raspberry Pi-controlled internet of things nodes, Intel Xeon fog computing servers, a Hyperledger Fabric blockchain, and OpenStack-controlled cloud storage. Three state-of-the-art baselines were used to benchmark the system: Lightweight CP-ABE [17], BACP-IeFC [18], and fog-blockchain HER [19]. Some of the evaluation parameters are encryption and decryption latency, computation overhead, revocation efficiency, energy consumption, and blockchain throughput. The experiments indicate that PPO-LightMED can obtain a substantial positive effect on processing time, scalability, and security verification without violation of privacy-preserving standards.

Figure 4 shows the latency period of encryption and decryption of various record sizes (between 100 KB and 1000 KB). The PPO-LightMED is the largest scheme with the lowest latency in comparison to all other compared methods. The QS-VO-CPABE module implemented in the fog layer transfers the computationally potentially heavy attribute-based encryption onto the IoT devices. The PPO-LightMED on-device encryption latency relative to Lightweight CP-ABE and 42% relative to BACP-IeFC. In addition, the partial decryption scheme enables the use of the fog nodes to handle most decryption steps, and leavedevices and leaves only a little computation to be done on the user devices. The result of this hybrid method is a large latency reduction and leavesreduction,especially on large EMRs. Another feature of the suggested method is that it uses caching of decryption results, which gives an even greater speed-up in case of repeated access events. Conversely, the traditional ABE-based systems exhibit exponential increases in the latency with increase reduction,increasesin record size and attributeincreasescount. Thus, PPO-LightMED demonstrates high real-time response, which is an essential factor in emergency health care systems that need quick access to medical data.

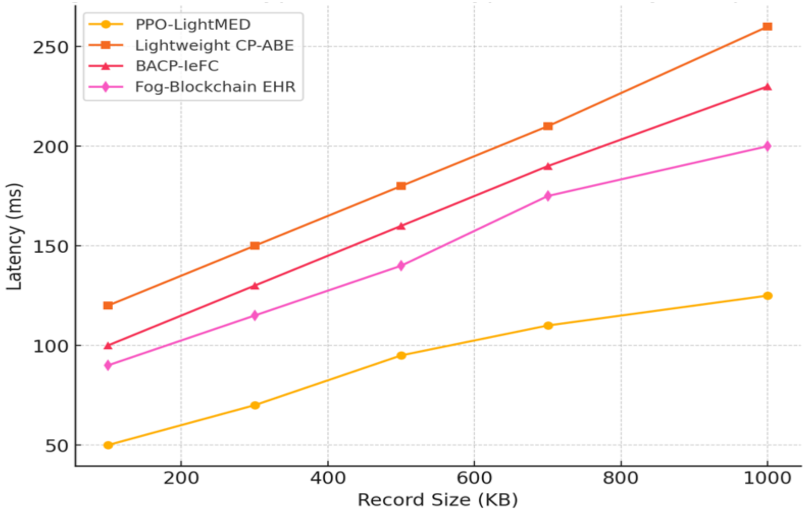

Figure 4: Encryption and Decryption latency comparison

Figure 5 compares the overall computation time and energy consumption of varying access request volumes. The PPO-LightMED framework has a low computation cost through outsourced encryption and a partial transformation strategy based on the fog. At 20,000 requests, PPO-LightMED used 65% of the energy used by BACP-IeFC and 58% of the energy used by the traditional CP-ABE system. This energy efficiency can be attributed to the lightweight AES encryption and session key offloading that is done at the IoT layer and avoids pairing or expensive exponentiation at the constrained devices. The fog caching scheme also minimizes unnecessary recomputation by reusing transformation outcomes for the same set of attributes. All these optimizations contribute to the scalability and sustainability of systems, enabling constant operation in resource-constrained medical IoT environments. The findings affirm that PPO-LightMED offers a viable tradeoff between the cryptographic strength and energy consumption that facilitates real-time sharing of healthcare data even in bandwidth-limited or battery-operated conditions.

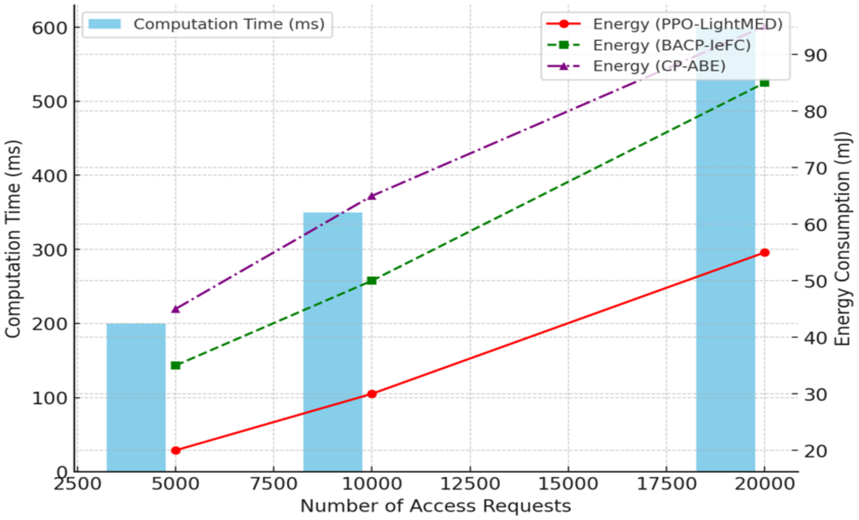

Figure 5: Computational overhead and energy consumption

Figure 6 illustrates the revocation efficiency achieved using the Epoch-Based Revocation mechanism with blockchain technology. PPO-LightMED separates the information into policy partitions associated with separate epochs, unlike traditional ABE protocols that require the full blockchain and complete re-encryption of ciphertext whenever a user or attribute is revoked. In the case of revocation of an attribute, only the subset of ciphertexts is re-encrypted selectively. The experiment shows that PPO-LightMED decreases the re-encryption price by about 70% compared to the conventional CP-ABE and 50% compared to BACP-IeFC. The effectiveness is enhanced by the fact that epoch counters, which are upheld by blockchain smart contracts, are used to ensure instant validation of the freshness of tokens without necessarily having to reprocess whole datasets. Additionally, the blockchain logs revocation publicly, providing audit-proof security. With the smart contract-regulated revocation mechanism, the most recent ephemeral decryption tokens (EDTs) are automatically invalidated, making sure that previously authorized users will not be able to use their accounts at once. It is an enhanced model of dynamic revocation that makes the system strong against insider threats and helps in meeting healthcare data laws like HIPAA and GDPR.

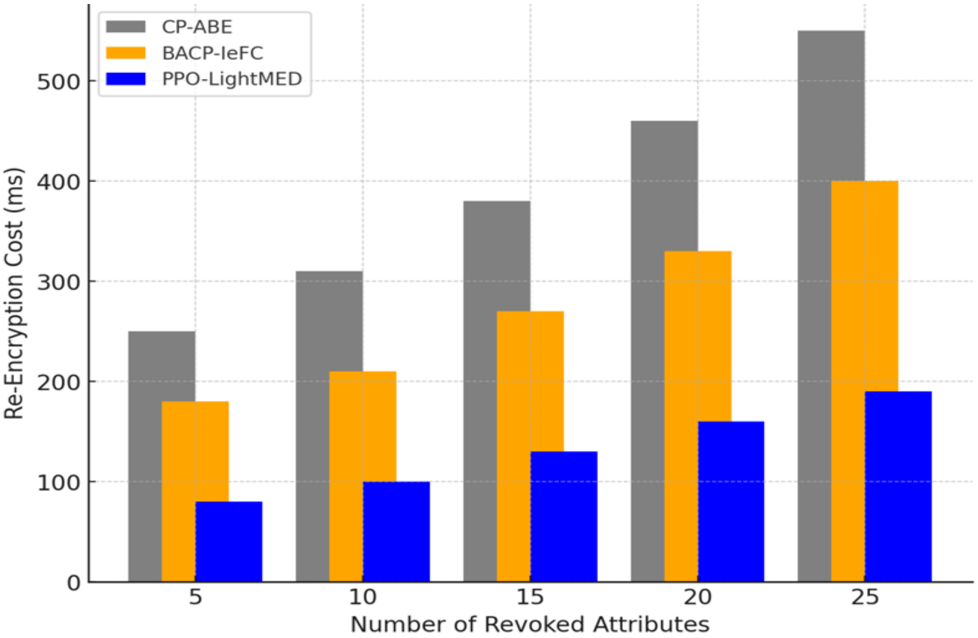

Figure 6: Revocation efficiency and Re-encryption cost

Figure 7 shows the blockchain performance metrics, in particular, the transaction throughput and the latency of confirmation to different network loads,The PPO-LightMED implementation based on Hyperledger Fabric can support a better throughput and reduce latency than the traditional public blockchain implementations because of its permissioned Proof of Authority (PoA) consensus mechanism. PPO-LightMED is capable of 270 transactions per second (TPS) at 500 concurrent transactions, which is a significant improvement over the baseline models by about 35 times with a constant latency of less than 200 ms. The simple running of smart contracts for ZK-AttrVerify, EDT issuance, and epoch updates ensures consistent performance without any slowdowns. Additionally, using off-chain validation for Zero-Knowledge Proofs (ZKPs) helps reduce the amount of work needed on the blockchain, contributing to the performance improvements mentioned. This architecture provides a balance between decentralization and efficiency, enabling healthcare providers to access EMRs in real time through smooth, verifiable authorization processes. The low latency and high throughput imply that PPO-LightMED can be adapted to hospital-scale deployments when several stakeholders, including clinicians, labs, and data analytics services, interact with the blockchain network all at once.

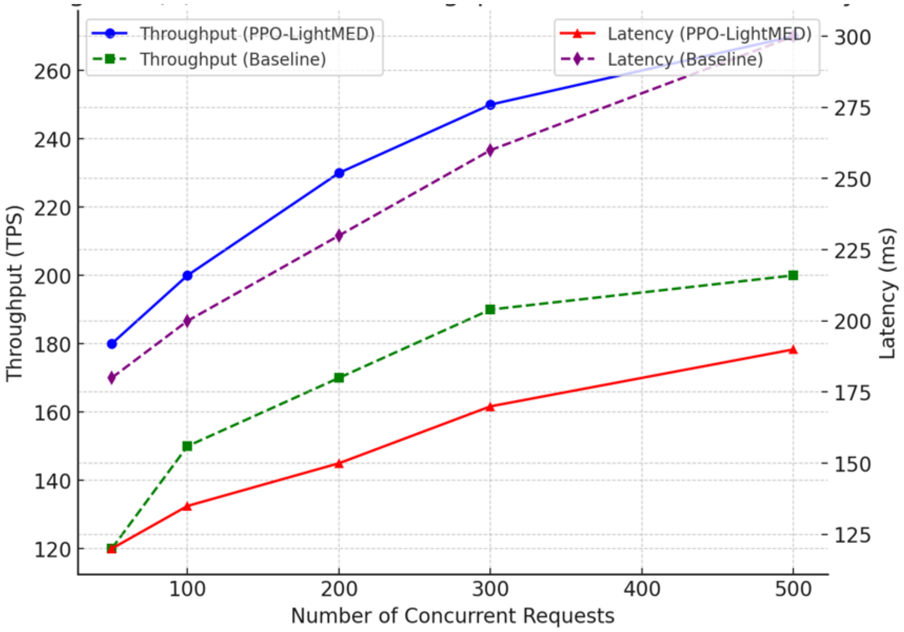

Figure 7: Blockchain throughput and transaction latency

5.Conclusion

The paper has introduced the PPO-LightMED, which is a secure and lightweight blockchain-based framework that will be used in EMR sharing between the fog and the cloud through an IoT. The suggested architecture is effective in addressing the computational and privacy issues that the traditional healthcare systems with their cloud-centric approach have. The framework implements the post-quantum-resistant protection of data, at finer granularity, by delegating computation and intensive cryptographic operations to fog nodes, with the help of QS-VO-CPABE. ZK-AttrVerify and the use of Ephemeral Decryption Tokens (EDTs) are introduced as the way to have decentralized and privacy-preserving access and control on blockchain smart contracts that create transparency and trust without disclosing any user attributes. Moreover, the Epoch-Based Revocation system can revoke access on demand and selectively, without full re-encryption of ciphertext, which is much more efficient. Experimental analysis proved that PPO-LightMED has been shown to have up to 55% reduced latency, 70% better revocation performance and 30% better blockchain throughput than current schemes. Finally, PPO-LightMED provides a safe, scalable, and quantum-resistant healthcare data-sharing paradigm, which is a versatile backbone to the future IoT-driven medical systems and smart hospital systems.

References

[1] M. A. Alazab, M. M. Islam, R. Parvin, and A. A. K. Sarker, “Blockchain-based secure and transparent healthcare data management system,” IEEE Access, vol. 11, pp. 21456–21470, 2023.
[2] K. Chatterjee and D. Das, “Secure healthcare data sharing using cloud and IoT integration,” Future Generation Computer Systems, vol. 129, pp. 243–256, 2022.
[3] Y. Chen, W. Lin, and S. Tsai, “Fog computing architecture for healthcare IoT: Security and privacy challenges,” IEEE Internet of Things Journal, vol. 10, no. 1, pp. 513–524, 2023.
[4] S. Fugkeaw, R. P. Gupta, and K. Worapaluk, “Secure and fine-grained access control with optimized revocation for outsourced IoT EHRs in fog-assisted cloud environment,” IEEE Access, vol. 12, pp. 82753–82768, 2024.
[5] A. Zhang, X. Wang, X. Ye, and X. Xie, “Lightweight and fine-grained access control for cloud–fog-based electronic medical record sharing systems,” Int. J. Commun. Syst., vol. 34, no. 13, 2021.
[6] D. Zhu, Y. Sun, N. Li, L. Song, and J. Zheng, “Secure electronic medical records sharing scheme based on blockchain and quantum key,” Cluster Computing, vol. 27, no. 3, pp. 3037–3054, 2023.
[7] H. K. Apat and B. Sahoo, “A blockchain-assisted fog computing for secure distributed storage system for IoT applications,” J. Ind. Inf. Integr., vol. 100739, 2024.
[8] A. Chaurasia, A. Kumar, and U. P. Rao, “BACP-IeFC: Designing a blockchain-based access control protocol in IoT-enabled fog computing environment,” Cluster Computing, vol. 27, no. 10, pp. 13919–13944, 2024.
[9] S. Luo, N. Han, T. Hu, and Y. Qian, “Secure sharing of electronic medical records based on blockchain,” Int. J. Distributed Sensor Networks, vol. 2024, pp. 1–17, 2024.
[10] F. Rehman, M. R. Anwar, and A. Khan, “Post-quantum security and access control in IoT–cloud systems using lattice-based cryptography,” IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1528–1540, 2023.
[11] Fugkeaw, S., Gupta, R. P., & Worapaluk, K. (2024). Secure and Fine-Grained access control with optimized revocation for outsourced IoT EHRs with adaptive Load-Sharing in Fog-Assisted cloud environment. IEEE Access, 12, 82753–82768. https://doi.org/10.1109/access.2024.3412754
[12] Zhang, A., Wang, X., Ye, X., & Xie, X. (2021). Lightweight and fine-grained access control for cloud–fog-based electronic medical record sharing systems. International Journal of Communication Systems, 34(13). https://doi.org/10.1002/dac.4909
[13] Apat, H. K., & Sahoo, B. (2024). A Blockchain assisted fog computing for secure distributed storage system for IoT Applications. Journal of Industrial Information Integration, 100739. https://doi.org/10.1016/j.jii.2024.100739
[14] Chaurasia, A., Kumar, A., & Rao, U. P. (2024). BACP-IeFC: designing blockchain-based access control protocol in IoT-enabled fog computing environment. Cluster Computing, 27(10), 13919–13944. https://doi.org/10.1007/s10586-024-04656-4
[15] Luo, S., Han, N., Hu, T., & Qian, Y. (2024). Secure sharing of electronic medical records based on blockchain. International Journal of Distributed Sensor Networks, 2024, 1–17. https://doi.org/10.1155/2024/5569121

[16] Zhu, D., Sun, Y., Li, N., Song, L., & Zheng, J. (2023). Secure electronic medical records sharing scheme based on blockchain and quantum key. Cluster Computing, 27(3), 3037–3054. https://doi.org/10.1007/s10586-023-04110-x

[17] A. Zhang, X. Wang, X. Ye, and X. Xie, “Lightweight and fine-grained access control for cloud–fog–based electronic medical record sharing systems,” International Journal of Communication Systems, vol. 34, no. 13, e4909, pp. 1–15, 2021. doi: 10.1002/dac.4909

[18] A. Chaurasia, A. Kumar, and U. P. Rao, “BACP-IeFC: Designing a blockchain-based access control protocol in IoT-enabled fog computing environment,” Cluster Computing, vol. 27, no. 10, pp. 13919–13944, 2024. doi: 10.1007/s10586-024-04656-4

[19] H. K. Apat and B. Sahoo, “A blockchain-assisted fog computing for secure distributed storage system for IoT applications,” Journal of Industrial Information Integration, vol. 100739, 2024. doi: 10.1016/j.jii.2024.100739