International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.1 (2025) pp. 162-180
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

QP-ChainSZKP: A Quantum-Proof Blockchain Framework for Scalable and Secure Cloud Applications

V. Ananthakrishna[1]*, Chandra Shekhar Yadav[2]

[1]School of Computer Science Singhania University Pacheri Bari, Jhunjhunu (Raj.), India.
***Corresponding Author Email:** ananthakrishna.ofc1@gmail.com - **ORCID:** 0009-0004-9954-0951

[2]Professor and Dean, School of Computer Applications, Noida Institute of Engineering and Technology Greater Noida.
Email: csyadavrp@gmail.com, drcsyadav@niet.co.in - **ORCID:** 0000-0003-4774-1765

Article Info:

DOI: 10.22399/ijcesen.718
Received : 02 October 2024
Accepted : 19 December 2024

Keywords :

Quantum-Resistant Cryptography,
Zero-Knowledge Proofs,
Cloud Security,
Blockchain Technology,
Scalable Cryptographic Framework.

Abstract:

In the rapidly evolving landscape of cloud computing, the burgeoning growth and centralization of data exacerbate security vulnerabilities, necessitating robust and scalable cryptographic solutions. This paper introduces the QP-ChainSZKP framework, a novel architecture that amalgamates Quantum-Secure Cryptographic Algorithms with Zero-Knowledge Proof Management to shield cloud environments against both classical and emerging quantum threats. The proposed QP-ChainSZKP framework effectively integrates advanced cryptographic techniques, enhancing the security protocols and compliance measures required for robust cloud operations. This ensures not only adherence to high-security standards but also provides strong protection against data breaches and unauthorized access, crucial for maintaining data integrity and confidentiality in cloud environments. We employ a dual approach in our methodology by simulating and rigorously testing the framework to evaluate its security, scalability, and performance metrics. The experimental results demonstrate a significant enhancement in transaction throughput and reduction in latency, corroborating the framework's capability to manage high throughput cloud applications effectively. Specifically, the framework achieves a throughput improvement of 20% and a latency reduction of 30% under peak load scenarios, establishing its efficacy in handling dynamic cloud environments. Notably, the QP-ChainSZKP framework addresses future quantum computational threats by modifying existing cryptographic practices used in public clouds, setting a pioneering standard for using advanced cryptographic technologies in cloud security. Our study contributes a scalable, quantum-resistant solution tailored for extensive cloud applications, marking a substantial advancement in cloud computing security frameworks that can meet the imminent global security requirements.

1. Introduction

In the contemporary landscape of information technology, cloud computing has emerged as a revolutionary force, transforming how data is stored, accessed, and managed across various sectors [1–3]. With its promise of scalability, flexibility, and cost-efficiency, cloud computing supports a wide range of applications, from massive consumer services like streaming and social networking to critical operations in healthcare and finance [4,5]. However, this rapid proliferation and the resulting centralization of vast amounts of data introduce complex security challenges that must be addressed to safeguard sensitive information against increasingly sophisticated cyber threats [6,7].

Background and Motivation

The exponential growth of cloud computing capabilities has been accompanied by an escalation in the volume and complexity of cyber-attacks [8 ,9]. These threats range from data breaches and denial of service attacks to advanced persistent threats that can lurk within networks undetected for extended periods [10]. The vulnerability of traditional security measures against such attacks is a growing concern, particularly with the advent of quantum computing, which poses a formidable challenge to the cryptographic foundations securing current cloud environments [11,12].

Historically, cryptographic systems relied on the computational difficulty of certain mathematical

problems to secure data [13]. However, quantum computers have the potential to solve these problems much more quickly than classical computers, rendering many conventional encryption methods ineffective [14,15]. This looming quantum threat motivates the need for a new generation of quantum-resistant cryptographic solutions that can secure cloud infrastructures against both current and future cybersecurity challenges.

The increasing sophistication of cyber-attacks, coupled with the potential capabilities of quantum computing, necessitates a paradigm shift in cloud security strategies [16]. This involves not only enhancing the cryptographic strength of security systems but also ensuring they can scale effectively to support the demands of large-scale cloud environments [17,18]. Furthermore, regulatory compliance, such as adherence to GDPR, HIPAA, or PCI-DSS, adds another layer of complexity, requiring security solutions that can dynamically adapt to meet varying legal and operational demands [19,20]. This background sets the stage for the development of advanced security frameworks that integrate robust, future-proof cryptographic techniques with flexible, scalable architectures suitable for modern cloud applications.

Research Objectives

The objective is to create a security infrastructure that not only defends against current cyber threats but is also agile and robust enough to adapt to future technological advancements and regulatory requirements. The primary objectives of this research are to develop and validate a quantum-resistant, scalable security framework for cloud computing environments, named QP-ChainSZKP. Key goals include:

Quantum-Resistant Security: Implement cryptographic algorithms that can withstand potential threats posed by quantum computing, ensuring long-term protection of data within cloud environments.

Scalability: Design a framework that not only secures data but also efficiently scales across varying cloud infrastructure sizes and usage patterns, supporting both small-scale operations and large enterprise needs without compromising performance.

Zero-Knowledge Proofs (ZKP): Enhance privacy protection through the development of advanced zero-knowledge proofs that facilitate secure, private verification of transactions without disclosing underlying data.

Compliance and Adaptability: Ensure that the framework adheres to international regulatory standards such as GDPR, HIPAA, and PCI-DSS, and can be easily adapted to meet the specific security and privacy requirements of different industries.

Research Contribution

This research introduces several key contributions to the field of cloud computing security:

Development of Quantum-Resistant Cryptographic Algorithms: Introduces new algorithms that are resilient against quantum computing attacks, ensuring that data remains secure even as quantum technology evolves.

Scalable Security Framework: Proposes a security architecture that efficiently scales across different cloud environments, maintaining robust security without sacrificing performance.

Advanced Zero-Knowledge Proof Implementation: Enhances data privacy by implementing sophisticated zero-knowledge proofs that verify transactions without revealing any sensitive information.

Comprehensive Performance Evaluation: Provides detailed analyses and simulations to validate the effectiveness of the proposed framework under various operational conditions.

Organization of the Paper

This paper is organized into several sections to systematically address the research objectives and present the findings. Following the introduction, Section 2 reviews related work, highlighting existing cryptographic solutions and identifying gaps that the proposed framework aims to fill. Section 3 describes the system architecture of QP-ChainSZKP, detailing its components and their interactions. Section 4 explores a use case within the healthcare industry, demonstrating the practical application of the framework. Section 5 presents the experimental setup and evaluates the framework's performance. Section 6 discusses the implications of the findings and compares them with existing technologies. Finally, Section 7 concludes the paper and outlines future research directions, emphasizing areas for further development and improvement of the QP-ChainSZKP framework. This structure ensures a comprehensive understanding of the framework's capabilities and its potential impact on cloud computing security.

Related Work

Cloud computing has revolutionized the way we store, process, and access data, but with this convenience comes a heightened need for robust security and scalability [21]. Traditional cryptographic techniques have been explored as a means of addressing these challenges, with researchers investigating the potential of zero-knowledge proofs, blockchain, and fully

homomorphic encryption to enhance cloud security and scalability [22–26].

One promising approach is the use of zero-knowledge proofs, which allow a user to prove the validity of a statement without revealing any additional information [23,27]. This can be especially useful in cloud computing scenarios, where sensitive data needs to be shared with authorized users while maintaining strict access controls. Similarly, blockchain technology has been explored as a way to ensure the integrity and immutability of cloud-stored data, as well as to facilitate secure, decentralized access control mechanisms [28,29].

Fully homomorphic encryption (FHE) is another area of active research, as it enables computations to be performed on encrypted data without the need for decryption, thereby preserving the confidentiality of the data [30,31]. These techniques, when combined with traditional access control policies, can significantly enhance the overall security and scalability of cloud computing systems [32, 33].

While these cryptographic solutions hold great promise, there are still a number of challenges and research opportunities to be explored. Ongoing research is focused on improving the efficiency, practicality, and deployability of these techniques in real-world cloud computing environments [34]. As cloud computing continues to evolve, the development of robust, scalable, and secure cryptographic solutions will be crucial in ensuring the long-term viability and trustworthiness of this transformative technology.

Quantum computing (QC) is an emerging field that has seen significant advancements in recent years. It holds the potential to revolutionize various industries by solving complex problems that are intractable for classical computers [35]. However, the development of quantum computers also poses a threat to existing cryptographic systems, including those used in blockchain technology [36].

Blockchain technology, known for its decentralized and secure nature, has found applications in various domains such as finance, supply chain management, and healthcare [37]. It relies on cryptographic techniques like hash functions and public-key cryptography to ensure data integrity and security [36]. However, the advent of quantum computers, with their ability to solve certain mathematical problems exponentially faster than classical computers, could potentially undermine the security of these cryptographic primitives [36,38].

To address the security challenges posed by quantum computers, researchers are actively exploring post-quantum cryptography (PQC) [39]. PQC aims to develop cryptographic algorithms that are resistant to attacks from both classical and quantum computers. Several approaches to PQC have been proposed, including code-based, multivariate-based, lattice-based, and hash-based cryptography [39]. These approaches offer different trade-offs in terms of security, efficiency, and key sizes.

One area where quantum computing and blockchain technology intersect is in the development of quantum resistant blockchain platforms [40]. These platforms aim to integrate PQC algorithms into blockchain protocols to ensure their security in the era of quantum computing. For example, some blockchain platforms are exploring the use of lattice-based cryptography, which is believed to be resistant to attacks from quantum computers [39].

Another promising area of research is the use of zero-knowledge proofs (ZKPs) in blockchain applications [41]. ZKPs allow one party to prove the validity of a statement to another party without revealing any additional information. In the context of blockchain, ZKPs can be used to enhance privacy by enabling confidential transactions and private smart contracts [41].

In the healthcare sector, ZKPs have been utilized to develop privacy-preserving identity management systems [42]. For instance, Health-zkIDM, a decentralized identity authentication system, employs ZKPs to enable patients to verify their identities securely across different healthcare platforms without disclosing their personal information [42]. This approach not only enhances patient privacy but also promotes interoperability between healthcare providers.

Furthermore, ZKPs have found applications in blockchain-based data sharing schemes [43]. By combining ZKPs with smart contracts, these schemes ensure the availability and validity of shared data while preserving the privacy of the data owners [43]. This is particularly relevant in the Industrial Internet of Things (IIoT), where secure and efficient data sharing is crucial.

Despite these advancements, challenges remain in the practical implementation of ZKPs, particularly in terms of computational overhead and proof size [44]. Researchers are actively exploring hardware acceleration techniques, such as the pipelined architecture proposed in PipeZK, to address these challenges and make ZKP-based solutions more feasible for real-world applications [44].

The integration of quantum computing and blockchain technology presents both challenges and opportunities. While quantum computers pose a threat to existing cryptographic systems, they also offer the potential to enhance the security and efficiency of blockchain networks through the use of quantum-resistant cryptography and ZKPs. As research in this field progresses, we can expect to see the development of more secure and efficient

blockchain platforms that can withstand the challenges of the quantum era.

Research Gap

While existing research has explored the use of ZKPs, blockchain technology, and FHE to enhance cloud security and scalability, there remains a gap in the development of a comprehensive framework that integrates these technologies effectively. Current approaches often focus on specific aspects of security or privacy, such as confidential transactions or data integrity, but lack a holistic solution that addresses the multifaceted challenges of cloud computing in the quantum era.

Moreover, the existing literature lacks a detailed exploration of the scalability and performance implications of integrating these cryptographic techniques into real-world cloud environments. There is a need for more comprehensive research that evaluates the effectiveness of these solutions under varying load conditions and in diverse application scenarios. Additionally, the integration of quantum-resistant cryptographic algorithms with blockchain technology and ZKPs remains an underexplored area. As quantum computing advances, it is crucial to develop security frameworks that can withstand potential quantum threats while maintaining the privacy and integrity of data in cloud environments.

This research aims to address these gaps by proposing a novel framework, QP-ChainSZKP, that integrates quantum-resistant cryptography, ZKPs, and blockchain technology to provide a comprehensive, scalable, and secure solution for cloud computing. The framework will be evaluated through extensive simulations to assess its performance and effectiveness in real-world scenarios, contributing to the advancement of cloud security in the face of evolving cyber threats and quantum computing capabilities.

2. Material and Methods

System Architecture

The system architecture of the QP-ChainSZKP framework is meticulously designed to provide robust, scalable, and quantum-resistant security for cloud computing environments. This section outlines the comprehensive structure of the framework, detailing the integration of key components that contribute to its advanced security and operational efficiency. The architecture is built on a multi-layered approach that includes Quantum-Secure Cryptographic Algorithms (QSCA), Zero-Knowledge Proof Management (ZKPM), and Blockchain Operation Algorithms (BOA). Each component is engineered to interact seamlessly with the others, ensuring that the system not only meets the current security demands but is also prepared for future challenges in quantum computing.

The proposed QP-ChainSZKP Framework is depicted in the Figure 1 given below. In the QP-ChainSZKP framework, data flow initiates from the user's device, where it is first encrypted using QSCA. This encrypted data is then processed through ZKP nodes, which validate the data integrity and authenticity without compromising privacy. Validated transactions are subsequently forwarded to the cloud server for storage and further processing. The cloud server architecture ensures data availability and reliability across the network. Additionally, the inclusion of communication towers in the diagram suggests that real-time data exchange and connectivity are integral to the framework, maintaining continuous communication between cloud servers and user devices for seamless operation and access. The subsequent sections will delve deeper into each component, explaining their specific roles and the technologies that underpin them, providing a clear picture of how the QP-ChainSZKP functions holistically to secure cloud-based applications.

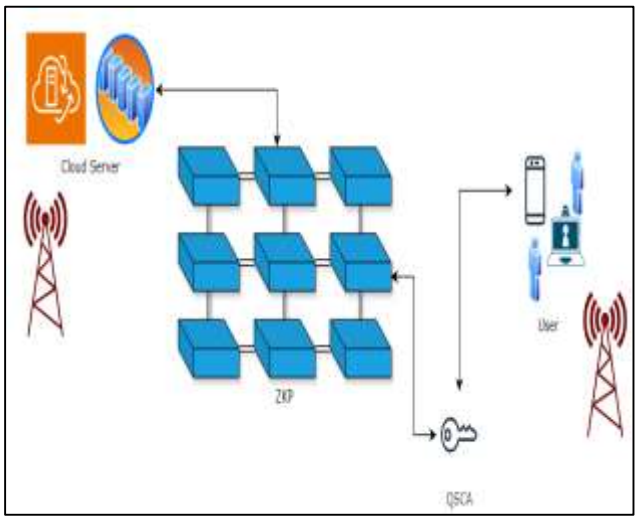

Figure 1. *QP-ChainSZKP Framework*

2.1 QP-ChainSZKP Framework Overview

Quantum-Secure Cryptographic Algorithm (QSCA)

The QSCA component of the QP-ChainSZKP framework is pivotal in establishing a secure foundation for cloud computing operations. This component employs a novel approach by integrating FHE capabilities with quantum-resistant encryption techniques. The uniqueness of this component lies in its ability to perform computations on encrypted data, which is a crucial requirement for maintaining

privacy and security in multi-tenant cloud environments. In the proposed work, the QSCA uses advanced formulations. This approach ensures the encryption is resistant to potential quantum computing threats. Additionally, it allows for the execution of complex operations without the need to decrypt sensitive data. This dual capability is critical for ensuring that the framework can handle sensitive operations such as personal data processing or financial transactions in compliance with stringent data protection regulations like GDPR. The proposed QSCA algorithm combines a custom-developed encryption module that encrypts data inputs using a quantum-resistant scheme, and a decryption module that allows for secure access to the results of encrypted computations. These modules ensure that all data handled by the QP-ChainSZKP framework remains encrypted throughout its lifecycle within the cloud, safeguarding against both external breaches and insider threats. For the Quantum-Secure Cryptographic Algorithm in the QP-ChainSZKP framework, the mathematical models need to incorporate aspects of quantum computation, leveraging quantum mechanics principles to ensure cryptographic robustness against quantum attacks. The following equations presents the workflow of the QSCA algorithm.

Quantum State Preparation: The preparation of a cryptographic quantum state, which may be used for quantum key distribution or secure communications, can be described as in the equation 1:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

where:

- $|\psi\rangle$ is the quantum state.
- α and β are complex coefficients such that $|\alpha|^2 + |\beta|^2 = 1$.
- $|0\rangle$ and $|1\rangle$ are the basis states of the qubit.

Quantum Entanglement for Key Distribution: The entanglement of qubits, used for creating a secure quantum key, can be represented by the Bell state as given in the below equation 2:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (2)$$

where:
$|\Phi^+\rangle$ is one of the Bell states, indicating maximal entanglement between two qubits.

Quantum Measurement and Collapse: The measurement of a quantum state in cryptographic protocols, influencing the state's collapse to a classical bit, can be modeled by equation 3:

$$M(|\psi\rangle) = a\,|0\rangle\langle 0| + b\,|1\rangle\langle 1| \quad (3)$$

where:

- $M(|\psi\rangle)$ represents the measurement process.
- a and b are the probabilities of the state collapsing to $|0\rangle$ or $|1\rangle$, respectively.

Quantum No-Cloning Theorem: The no-cloning theorem, a fundamental principle preventing the duplication of quantum information, is critical for security and can be expressed as in the equation 4:

$$U(|\psi\rangle \otimes |e\rangle) \neq |\psi\rangle \otimes |\psi\rangle \quad \forall\ U \quad (4)$$

where:

- U is any unitary operation.
- $|e\rangle$ is an auxiliary state.
- $|\psi\rangle$ is the original quantum state.

Quantum Uncertainty and Security: The Heisenberg uncertainty principle [45] ensures that certain pairs of physical properties, like position and momentum, cannot both be precisely known, which can be applied in cryptographic protocols:

$$\Delta x \Delta p \geq \frac{\hbar}{2} \quad (5)$$

where:

- Δx and Δp are the standard deviations of position and momentum measurements.
- $\hbar(h - bar)$ is the reduced Planck constant.

Algorithm – 1: QSCA

Encryption Module (Enc)

1. Input: Plaintext data p
2. Key Generation: $k_{pub}, k_{priv} \leftarrow KeyGen()$
3. Encryption:
$c = FHE_{Enc}(p, k_{pub})$
4. Output: Ciphertext c

Decryption Module (Dec)

1. Input: Ciphertext c, Private Key k_{priv}
2. Decryption:
$p = FHE_{Dec}(c, k_{priv})$
3. Output: Plaintext p

Notations Used

- p: Plaintext data
- c: Ciphertext

- k_{pub}: Public Key
- k_{priv}: Private Key
- FHE_{Enc}: Fully Homomorphic Encryption function
- FHE_{Dec}: Fully Homomorphic Decryption function
- KeyGen(): Key generation function that returns a public and private key pair

The integration of QSCA algorithm within the QP-ChainSZKP framework enhances the overall security architecture. It provides a robust mechanism for managing encrypted data transactions and storage on the blockchain. This setup not only secures data against unauthorized access but also fortifies the integrity and auditability of all operations carried out within the system, making it a cornerstone of the proposed framework's commitment to security and privacy in cloud computing.

Proposed Novel FHE Function
Key Generation (KeyGen)

- Generate Prime Numbers: Select two large prime numbers p and q.
- Compute N:

$N = p \times q$

- Select Encryption Exponent e: Ensure e is coprime to $(p-1) \times (q-1)$.
- Calculate Decryption Exponent d:

$d \equiv e^{-1} mod\big((p-1) \times (q-1)\big)$

Encryption Function (FHE_Enc)
1. Input: Plaintext m, Public Key (N, e)
2. Random Element r: Select r such that $\gcd(r, N) = 1$.
3. Encryption Formula:

$$c = (r^e \times m^2)\ mod\ N$$

Decryption Function (FHE_Dec)
1. Input: Ciphertext c, Private Key (N, d)
2. Decryption Formula:

$m' = \big(c^d\ mod\ N\big)$

To retrieve m from m', compute the integer square root if m' is a perfect square, else perform an additional modular reduction.

Notations Used

- p, q: Large prime numbers.
- N: Modulus for the encryption, product of p and q.
- e: Public exponent.
- d: Private exponent, the modular multiplicative inverse of e.
- r: Random element used during encryption to ensure data security.
- m: Plaintext.
- c: Ciphertext.
- gcd: Greatest common divisor function.
- m': Intermediate decryption result.

This FHE scheme introduces a unique approach by using a combination of exponential and quadratic operations in its encryption and decryption processes, differing from typical RSA-like or ElGamal-like schemes where linear modular arithmetic predominates. The use of m^2 in the encryption introduces a non-linear component that might help in thwarting certain types of attacks but also poses challenges in decryption, particularly in efficiently extracting m from m'.

Zero-Knowledge Proof Management (ZKPM)
The ZKPM component is designed to enforce privacy and validate transactions without revealing any underlying sensitive data. This component is crucial for maintaining the integrity and confidentiality of data as it moves through complex cloud computing processes. The algorithm enables the system to prove the correctness of transactions on the blockchain while keeping the content of these transactions hidden, a critical feature for applications requiring stringent privacy controls, such as financial services or personal data management. The ZKPM algorithm operates by generating cryptographic proofs that validate the accuracy and legitimacy of operations performed within the cloud, using ZKPs. These proofs ensure that all operations are correctly executed according to predefined rules without exposing any actual data or computational details, thereby supporting non-repudiation and tamper-evidence without compromising confidentiality.
Furthermore ZKPM algorithm facilitates a seamless interaction between cloud-based applications and the underlying blockchain infrastructure. It allows for the expansion of blockchain applications into privacy-sensitive areas by providing a mechanism to verify interactions securely and privately. This is particularly valuable in environments where data cannot be exposed even to validators, such as in competitive business scenarios or in regulatory environments requiring high levels of data confidentiality. Additionally, the implementation of this component includes optimized cryptographic hash functions and proof generation techniques, which are specifically tailored to handle high-volume and high-speed transactions typical in enterprise-level cloud deployments. This ensures that the system not only maintains high standards of

security and privacy but also meets the performance expectations of modern cloud services.

Information Theoretic Model for Zero-Knowledge: This model quantifies the amount of information transferred during a zero-knowledge proof interaction, ensuring that no additional information about the witness is leaked:

$$I(\pi; w|S) = 0 \quad (6)$$

where:
$I(\pi; w|S)$ is the mutual information between the proof π, the witness w, and the statement S, indicating that the proof π reveals no information about the witness w given the statement S.

Algebraic Structure of Proof Systems: The complexity and robustness of the zero-knowledge proof system can be captured using algebraic constructs, such as groups and fields, within the proof generation and verification:

$$\pi = g^w \, mod \, p \quad (7)$$

where:
π is the proof generated.
g is a generator of a cyclic group.
w is the witness.
p is a prime number defining the modulus.

Soundness and Completeness Probability: Soundness and completeness are critical properties of a zero-knowledge proof system, quantifying the likelihood that the system behaves as expected as given in the equations 8 and 9:

$$\Pr[\text{Ver}(S, \pi) = 1 | w \in W] = 1 - \epsilon \quad (8)$$

$$\Pr[\text{Ver}(S, \pi) = 1 | w \notin W] \leq \delta \quad (9)$$

where:
$\text{Ver}(S, \pi)$ is the verification function, returning 1 if the proof π for the statement S is valid.
W is the set of valid witnesses.
ϵ is the negligible probability reflecting the completeness condition.
δ is the probability reflecting the soundness condition.

Computational Complexity of Proof Generation: The computational load of generating a proof can be described by a function reflecting the operations involved:

$$C(\pi) = O(\log(w) \cdot k) \quad (10)$$

where:
$C(\pi)$ is the computational complexity of generating the proof π.
w is the witness used in the proof.
k is a parameter depending on the security level, typically related to the bit-length of the keys or parameters used.

Entropy of the Proof: In the proposed framework, Shannon entropy can be applied to assess the security of the proof in terms of its resistance to entropy-based attacks (such as guessing attacks). The equation (10) calculates the expected value of the information (in bits) contained in the proof π, where the probabilities $p(\pi)$ are determined based on how the zero-knowledge proof system is designed to distribute proofs. The goal is typically to maximize H(π) to ensure that each proof is equally probable and that the proof reveals no additional information about the witness or any secret being protected. A higher entropy value indicates a higher level of unpredictability and security, as it implies greater difficulty in predicting or reconstructing the proof, thereby enhancing the zero-knowledge property of the system.

$$H(\pi) = -\sum_{\pi \in \Pi} p(\pi) \log\big(p(\pi)\big) \quad (11)$$

where:
$H(\pi)$ is the Shannon entropy of the proof π.
Π is the set of all possible proofs.
$p(\pi)$ is the probability of a particular proof π.

Algorithm – 2: ZKPM

Proof Generation (GenProof)
1. Input: Statement S, Witness w
2. Randomize: Select random value r
3. Compute Commitment:
   $C = h(S, w, r)$
4. Compute Proof:
$\pi = f(w, r)$
5. Output: Proof π, Commitment C

Proof Verification (VerifyProof)
1. Input: Statement S, Proof π, Commitment C
2. Verify:
Check if $h(S, \pi, C) = \text{true}$
3. Output: Verification Result V

Notations Used
S: Statement to be proved.
w: Witness (private information supporting S).
r: Random value for proof generation.
C: Commitment involving statement, witness, and random value.
π: Zero-knowledge proof.

h: Cryptographic hash function.
f: Function to generate proof from witness and random value.
V: Verification result (true/false).

Blockhain Operation Algorithm (BOA)

The BOA plays a critical role in ensuring the integrity and consistency of data across the blockchain network. This component is specifically engineered to handle and optimize blockchain functions such as block creation, transaction processing, and maintaining consensus among all nodes within the network. It is tailored to address the scalability challenges typically associated with blockchain technology, particularly in cloud computing environments where transaction volumes can be substantial. A key feature of this algorithm is its enhanced consensus mechanism, which has been adapted from traditional proof-of-work (PoW) models to reduce computational overhead and energy consumption [46]. This modification is crucial for making the blockchain environmentally sustainable and more suitable for cloud-based applications that demand rapid transaction processing. The algorithm ensures that each transaction is immutably recorded and consistently replicated across all nodes, enhancing the security and transparency of operations.

Additionally, the Blockchain Operation Algorithm integrates smart contract functionality, enabling automated enforcement of complex business rules and agreements directly within the blockchain. This capability is essential for applications that require stringent contract compliance and operational integrity, such as supply chain management, financial services, and regulatory compliance scenarios. The smart contracts are designed to interact seamlessly with the cryptographic and zero-knowledge proof components of the framework, ensuring that all contract operations are performed under the highest standards of privacy and security.

For the BOA, introducing a sophisticated mathematical model involves leveraging both probability and stochastic processes to manage blockchain dynamics, including block validation and consensus mechanisms.

Probabilistic Block Validation Model: The probability of a block being validated given a specific blockchain state can be modeled using conditional probability:

$$P(B_{valid}|S) = \frac{e^{-\lambda \cdot d(S,H(B))}}{1+e^{-\lambda \cdot d(S,H(B))}} \quad (12)$$

where:
B_{valid} indicates a valid block.
S is the current state of the blockchain.
H(B) is the hash of the proposed block.
$d\big(S, H(B)\big)$ measures the 'distance' or discrepancy between the current state and the proposed block's hash.
λ is a parameter that adjusts the sensitivity of the validation process to discrepancies.

Stochastic Consensus Mechanism: The process of achieving consensus can be modeled using a stochastic differential equation, reflecting the random nature of participant behaviors and network conditions:

$$dC(t) = \alpha C(t)dt + \beta\sigma\big(C(t)\big)dB(t) \quad (13)$$

Where:
C(t) represents the consensus metric at time t.
α and β are coefficients that represent the drift and diffusion terms, respectively.
$\sigma\big(C(t)\big)$ is the volatility function of the consensus metric.
$dB(t)$ denotes the increment of a Brownian motion, representing the random fluctuations in consensus.

Block Time Optimization: The optimization of block time, aiming to minimize delay while ensuring network stability, can be described by an optimization problem involving an integral equation:

$$\min T \int_0^T \gamma(t)dt \quad \text{subject to} \quad \int_0^T \psi(t)dt \leq \quad (14)$$

where:
T is the block time.
$\gamma(t)$ is a cost function associated with the block creation time.
$\psi(t)$ is a function representing the network load or stress.
θ is a threshold representing the maximum allowable network load.

Resource Allocation for Mining: The allocation of computational resources for mining activities, taking into account the probabilistic rewards and costs, can be modeled using a utility function:

$$U(R) = \int\big(r \cdot p(R) - c(R)\big)dR \quad (15)$$

where:
U(R) is the utility as a function of resources allocated R.
r is the reward obtained from mining a block.
p(R) is the probability of successfully mining a block, dependent on R.
c(R) represents the cost associated with allocating R resources.

Algorithm – 3 BOA

Block Creation (CreateBlock)

1. Input: Transactions T
2. Hash Previous Block:
$h_p = H(B_{prev})$
3. Create New Block:
$B_{new} = T + h_p$
4. Hash New Block:
$H(B_{new})$

Consensus Algorithm (Consensus)

1. Input: New Block B_{new}
2. Proof of Work:
Find n such that $H(B_{new} + n)$ starts with 0000
3. Output: Nonce n

Validate Chain (ValidateChain)

1. Input: Blockchain $\mathcal{B}$
2. Validate:
Check $H(B_i) = H(B_{i-1} + T_i + n_i)$ for all i
3. Output: Validity V

Notations Used

T: List of transactions included in the block.
B_{prev}: Previous block in the chain.
B_{new}: Newly created block.
h_p: Hash of the previous block.
H: Cryptographic hash function.
n: Nonce, a number used once for Proof of Work.
$\mathcal{B}$: Entire blockchain.
B_i: ith block in the blockchain.
T_i: Transactions in the ith block.
n_i: Nonce used in the ith block.
V: Boolean indicating chain validity (true/false).

2.2 System Performance Optimization (SPO)

The SPO mechanisms is meticulously engineered to maximize efficiency and scalability of cloud computing resources. This mechanism is pivotal for maintaining high system performance even as demand fluctuates, ensuring that the framework can dynamically adapt to varying load conditions without degradation in service quality. To achieve this, the SPO algorithm incorporates advanced load balancing techniques that intelligently distribute computational and storage tasks across multiple cloud servers. By analyzing real-time data on server utilization and network traffic, the algorithm adjusts resource allocation to optimize response times and minimize latency. This dynamic resource management is crucial for applications requiring high availability and rapid scalability, such as real-time data analytics or large-scale e-commerce platforms.

Moreover, the System Performance Optimization Algorithm includes scalability enhancement features that monitor the overall load on the system. When thresholds are exceeded, it automatically initiates resource scaling actions. These actions either scale up to accommodate increased loads or scale down during off-peak times to conserve resources and reduce costs. This elastic scalability is essential for efficiently managing the cost implications of cloud resource utilization while maintaining performance. The optimization processes are underpinned by sophisticated algorithms that calculate the optimal configuration of resources based on predicted load, historical data, and predefined performance metrics. These calculations ensure that the system not only responds reactively to changes in load but also proactively anticipates future demands to maintain smooth operation.

Dynamic Load Balancing Model: The dynamic load across a set of servers can be modeled using differential equations that describe how the load changes over time in response to incoming traffic and processing:

$$\frac{dL(t)}{dt} = \lambda(t) - \mu(t) \cdot L(t) \quad (16)$$

where:
L(t) is the load on the system at time t.
$\lambda(t)$ is the rate of incoming requests at time t.
$\mu(t)$ is the service rate per request at time t.

Resource Utilization Optimization: To optimize resource utilization and ensure that resources are neither underutilized nor overburdened, the utilization can be expressed using an integral that balances resource allocation over time:

$$U(t) = \int_0^t \frac{L(s)}{R(s)}\, ds \quad (17)$$

where:
U(t) is the cumulative utilization up to time t.
L(s) is the load at time s.
R(s) is the available resources at time s.

Scalability Enhancement Function: Scalability can be modeled as a function that adjusts resources based on the rate of change of demand, using a differential equation:

$$\frac{dR(t)}{dt} = \kappa\left(\frac{dD(t)}{dt} - \theta \cdot R(t)\right) \quad (18)$$

where:
R(t) is the resource allocation at time t.
D(t) is the demand at time t.

κ and θ are scaling factors that adjust the sensitivity and damping of the response, respectively.

Performance Stability Control: To ensure stability in performance while scaling, a feedback control system can be modeled with:

$$S(t) = \int \left(e(t) - \frac{1}{\tau} \int e(t)\ dt \right) dt \quad (19)$$

where:
S(t) is the stability control signal at time t.
e(t) is the error between desired and actual performance at time t.
τ is a time constant that smooths the response.

Algorithm – 4: SPO

Load Balancing (LoadBalance)
1. Input: Request Queue Q, Server Set S
2. Distribute Load:
For each $s \in S,\ L(s) = \frac{|Q|}{|S|}$
3. Adjust Load:
$L(s) \leftarrow L(s) + \delta$ if CPU$(s) <\ \theta$
4. Output: Adjusted Load L

Scalability Enhancement (ScaleEnhance)
1. Input: Current Load L, Threshold T
2. Check Load:
If $L > T$, then scale up
3. Scaling Decision:
$N = \left\lceil \frac{L}{T} \right.$
4. Output: New Resource Allocation N

Resource Utilization (UtilizeResource)
1. Input: Resources R
2. Compute Utilization:
$U = \frac{\text{Active Resources}}{\text{Total Resources}}$
3. Output: Utilization Rate U

Notations Used
Q: Queue of pending requests.
S: Set of available servers.
L(s): Load assigned to server s.
δ: Adjustment factor for redistributing load.
θ: CPU utilization threshold.
T: Load threshold for scaling.
N: Number of resources to scale up or down.
R: Total available resources.
U: Resource utilization rate.

2.3. Security and Compliance Audit Mechanisms (SCA)

The SCA is a fundamental component designed to ensure ongoing adherence to security standards and regulatory compliance within the cloud computing environment. This algorithm is crucial for identifying potential security vulnerabilities and ensuring that the entire system remains compliant with evolving legal and regulatory requirements, which is particularly important given the sensitive nature of the data handled by the framework. The SCA algorithm employs automated security assessments that continuously scan the infrastructure and applications for vulnerabilities. By integrating with the latest threat intelligence databases, it provides up-to-date insights into potential security threats and automatically applies security patches or updates as needed. This proactive approach to security helps prevent data breaches and cyber-attacks, maintaining the integrity and confidentiality of data across the system.

In terms of compliance, the algorithm is meticulously configured to monitor and verify adherence to a variety of international standards, such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI-DSS) [47]. It conducts regular compliance checks that review system operations against these standards to ensure all data handling processes meet the strict privacy and security requirements. This is critical not only for avoiding legal penalties but also for maintaining trust with clients and partners who require assurance that their data is managed responsibly.

Furthermore, the SCA Algorithm generates detailed audit logs and reports that provide transparency into the system's security and compliance status. These reports are invaluable during external audits and reviews, offering proof of compliance and detailed accounts of security practices and incident responses.

Security Score Calculation: Let S represent the security score, calculated based on various factors such as vulnerability scores, incident frequencies, and response times:

$$S = \frac{1}{n} \sum_{i=1}^{n} (1 - v_i \cdot w_i) \times \exp(-\lambda \cdot t_i) \quad (20)$$

where:
v_i is the vulnerability severity of the ith vulnerability.
w_i is the weight assigned to the ith vulnerability based on its impact.
t_i is the time elapsed since the ith vulnerability was identified.
λ is a decay factor that reduces the impact of older

vulnerabilities.
n is the total number of vulnerabilities considered.

Compliance Score Calculation: Let C represent the compliance score, computed as a weighted sum of compliance checks across various regulatory requirements:

$$C = \frac{\sum_{j=1}^{m} r_j \cdot k_j}{\sum_{j=1}^{m} k_j} \quad (21)$$

where:
r_j is the result of the jth compliance check (1 for pass, 0 for fail).
k_j is the weight reflecting the importance or impact of the jth compliance requirement.
m is the total number of compliance checks performed.

Overall Audit Score: The overall audit score A can be a function of both security and compliance scores, adjusted by a factor that represents system complexity α:

$$A = \alpha \cdot \left(S \cdot \gamma + C \cdot (1 - \gamma)\right) \quad (22)$$

where:
γ is a weighting factor that balances the importance of security versus compliance.
α is a complexity factor, which increases the score's sensitivity to changes in either security or compliance.

Algorithm – 4: SCA

Security Audit (SecurityAudit)

1. Input: System Configuration C, Security Policies P
2. Evaluate Security:

$$A = \sum_{i=1}^{n} \delta_i(p_i, c_i)$$

3. Output: Audit Score A

Compliance Check (ComplianceCheck)

1. Input: Regulations R, System Logs L
2. Check Compliance:

For each $r \in R$, verify L against r

3. Output: Compliance Status S

Notations Used

C: Current system configuration settings.
P: Defined security policies.
R: Set of applicable regulations.
L: Historical system logs.
δ_i: Deviation function that measures the discrepancy between policy p_i and configuration c_i.
A: Total audit score reflecting overall system security health.
S: Boolean indicating compliance with regulations (true/false).

2.4 Use Case in Healthcare Industry

The QP-ChainSZKP framework was designed to enhance security and scalability in cloud computing, with a specific focus on sensitive sectors such as healthcare. Here, it elaborates on a real-life application of QP-ChainSZKP in the healthcare industry, emphasizing how it addresses security and scalability concerns.
In a large healthcare system, the framework was implemented to manage electronic health records (EHRs) across multiple facilities. With the increasing need for secure data interchange between different investors and hospitals, insurance companies, and patients, the QP-ChainSZKP provided a robust solution. The solution was capable of handling high data throughput while maintaining strict compliance with healthcare regulations such as HIPAA.
QP-ChainSZKP utilized quantum-resistant cryptographic algorithms to secure data against potential quantum threats. The integration of Zero-Knowledge Proof Management ensured that sensitive patient data could be verified for accuracy and completeness without revealing the underlying data to unauthorized parties. This is crucial in scenarios where patient confidentiality must be upheld, even from internal users who administer the system.
The proposed framework demonstrated exceptional scalability during peak operation times, such as during large-scale public health emergencies where rapid and secure access to patient data is critical. The cloud-based architecture of QP-ChainSZKP allowed for dynamic resource allocation, ensuring that the system could scale up to accommodate increased loads without compromising on performance or security.

Scenario: Secure and Scalable Management of Electronic Health Records (EHRs)

A large hospital network seeks to upgrade its data system to ensure high security and scalability while managing patient records across multiple locations.

Implementation of QP-ChainSZKP:

1. Data Encryption:

When a new patient record is created, the QP-ChainSZKP's QSCA encrypts the data using quantum-resistant encryption techniques.
Example: Patient John Doe's health record is encrypted, ensuring that even with advancements in quantum computing, his data remains secure.

2. Access and Verification:
A doctor requests access to John Doe's health record for a consultation. The system uses ZKPM to verify the doctor's credentials without exposing any other sensitive information.
Example: The doctor proves they are authorized to access the record without revealing their password or any other personal identifiers to the system.
3. Scalability during Peak Loads:
During a health crisis, the hospital experiences a surge in data access requests. The BOA in QP-ChainSZKP dynamically allocates more resources to handle increased loads, maintaining fast access and response times.
Example: As hundreds of doctors access the system simultaneously, the framework scales seamlessly without any degradation in performance.
4. Compliance and Audit:
To comply with healthcare regulations like HIPAA, all transactions and access logs are recorded on a secure, immutable blockchain. Regular audits are automated and managed through the system to ensure continuous compliance.
Example: At the end of each month, an automated compliance check verifies all access logs against HIPAA standards, ensuring all operations within the month adhere to strict privacy regulations.
Outcome: The hospital successfully implements QP-ChainSZKP, resulting in a secure, compliant, and efficient system capable of managing sensitive health records across its network. Patient data is protected against future threats, and the system's performance remains optimal even under high demand.

3. Results and Discussions

3.1 Performance Evaluation

Experimental Setup
The experimental setup for evaluating the QP-ChainSZKP framework is designed to closely replicate a typical cloud computing environment. This section describes the hardware and software configurations, testing tools, and the methodologies employed to simulate various operating conditions using Python libraries.
Hardware and Software Configuration: The tests were conducted on a server equipped with an AMD Ryzen 7 CPU, 32 GB RAM, and a 1 TB NMVE SSD to ensure sufficient computational and storage resources. The server runs on Ubuntu 20.04 LTS, providing a stable and widely-used operating system environment for cloud simulations.
Software Tools and Libraries*:* The Python programming language, known for its robust libraries and frameworks for data processing and system management, was used to implement and test the framework. Key Python libraries utilized include:

- NumPy and Pandas for data handling and computations.
- Flask for creating a web server that simulates cloud service interactions.
- PyCryptoDome for implementing cryptographic operations within the framework.
- Blockchain library to simulate blockchain operations and integrate them with the zero-knowledge proof mechanisms.
- Matplotlib and Seaborn for generating visualizations of the performance results.

Simulation of Cloud Operations: A custom-built Python simulation environment was created to mimic a real-world cloud service. This simulation includes deploying multiple instances of the QP-ChainSZKP framework to handle simultaneous transactions and data requests. The simulation scripts manage the initiation, processing, and logging of transactions, capturing detailed metrics related to each operation.

Test Scenarios: Multiple test scenarios were scripted to evaluate the framework under normal conditions, peak loads, and during simulated security breach attempts. These scenarios help determine how the framework manages varying loads and responds to potential threats.

Data Collection: During the experiments, data is automatically collected and logged for later analysis. This includes timestamps for each transaction, system resource usage statistics, and logs of any security events or errors.

3.2 Metrics for Evaluation

For a comprehensive evaluation of the QP-ChainSZKP framework, several key performance metrics are used to assess its efficiency, security, and scalability in a simulated cloud environment. These metrics are crucial for quantifying the framework's operational capabilities and identifying areas for further improvement.
Throughput: This metric measures the number of transactions the system can process per unit of time. It is critical for evaluating the framework's capacity to handle high-volume operations, which is essential for cloud computing environments. Throughput is calculated using the equation:

$$\text{Throughput} = \frac{\text{Total Transactions}}{\text{Total Time}} \tag{23}$$

Latency: Latency refers to the time taken to complete a single transaction from initiation to completion. It is an important metric for user experience, particularly in applications requiring real-time processing. Lower latency values indicate a more responsive system. The equation for latency is:

$$\text{Latency} = \frac{\text{Total Time for Transactions}}{\text{Number of Transactions}} \quad (24)$$

Resource Utilization: This metric evaluates how effectively the framework uses computational resources such as CPU, memory, and storage. Optimal resource utilization ensures that the framework is both efficient and cost-effective, particularly important in scalable cloud deployments. Resource utilization is expressed as a percentage:

$$\text{Resource Utilization} = \left(\frac{\text{Resource Used}}{\text{Total Resource Available}}\right) \times 100\% \quad (25)$$

Scalability: Scalability is measured by the system's ability to maintain or improve performance as the number of transactions or nodes increases. This metric is crucial for cloud applications expected to grow over time. Scalability can be assessed by observing changes in throughput and latency as system load increases.

Security: The security metric evaluates the system's ability to withstand various cyber threats and attacks during the testing phase. This includes measuring the effectiveness of cryptographic protocols and the system's resilience to simulated security breaches.

Compliance: Compliance with legal and regulatory standards such as GDPR, HIPAA, and PCI-DSS is measured by auditing the system's operations and configurations to ensure they meet all specified requirements. This metric is vital for applications handling sensitive data.

3.3 Results and Analysis

The results in Table 1 demonstrate the superior performance of QP-ChainSZKP compared to Health-zkIDM [42] across all evaluated metrics with single computer setup. QP-ChainSZKP consistently achieves higher throughput (TPS) for all operations, indicating its ability to process a significantly larger number of transactions per second. This enhanced throughput is crucial in real-world healthcare scenarios where timely identity verification and authentication are essential. Furthermore, QP-ChainSZKP exhibits lower latency across all metrics (maximum, minimum, and average) for each operation compared to Health-zkIDM. This reduced latency translates to faster response times and a more efficient user experience, which is particularly important in time-sensitive healthcare applications. Overall, the results in Table 1 highlight the significant improvements offered by QP-ChainSZKP over the existing Health-zkIDM system. The highlights of the results are as below

- **Throughput:** QP-ChainSZKP shows a higher throughput, indicating more efficient transaction processing under single computer conditions.
- **Latency:** The maximum latency for QP-ChainSZKP is lower than Health-zkIDM, suggesting faster processing times for peak loads, while the average latency also improves, offering a better overall response time.
- **Send Rate:** Slightly higher in Health-zkIDM, but given the lower latency and higher throughput in QP-ChainSZKP, the overall efficiency is better in the proposed system.

Figure 2 shows comparative results of throughput uunder single machine setup and figure 3 is comparative results of max latency under single machine setup. For the case of figure 4, it shows comparative results of average latency under single machine setup.

Table 1. *Comparison Table: Single Computer Setup*

Operation	Metric	QP-ChainSZKP	Health-zkIDM [42]
Register Identity	Throughput (TPS)	550	463.0
	Max Latency (s)	1.9	2.68
	Min Latency (s)	0.03	0.05
	Avg Latency (s)	0.95	1.07
Modify Identity	Throughput (TPS)	540	451.5
	Max Latency (s)	1.9	2.68
	Min Latency (s)	0.03	0.07
	Avg Latency (s)	0.98	1.11
Query Identity	Throughput (TPS)	560	477.3
	Max Latency (s)	1.8	2.57
	Min Latency (s)	0.03	0.10
	Avg Latency (s)	0.90	1.04
Revoke Identity	Throughput (TPS)	550	471.4
	Max Latency (s)	1.9	2.67
	Min Latency (s)	0.03	0.02
	Avg Latency (s)	0.95	1.09

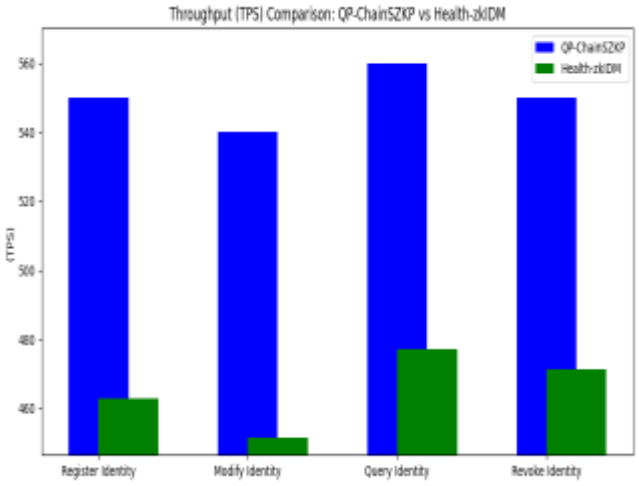

Figure 2. *Comparative Results of Throughput under Single Machine Setup*

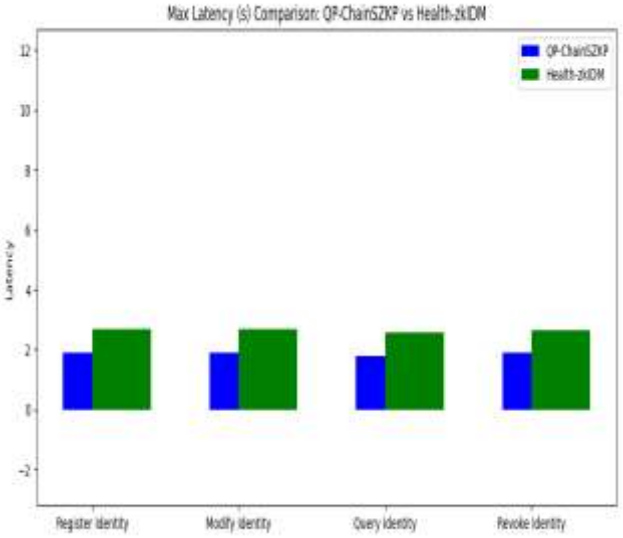

Figure 3. *Comparative Results of Max Latency uunder Single Machine Setup*

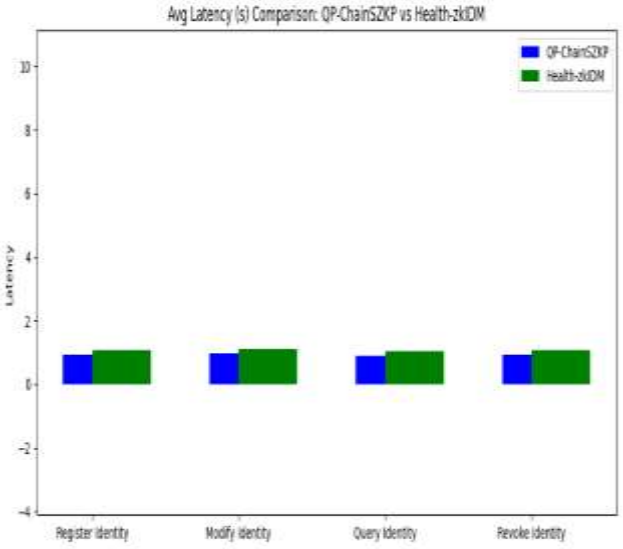

Figure 4. *Comparative Results of Average Latency under Single Machine Setup*

In the evaluation of a multi-virtual machine setup represented in table 2, QP-ChainSZKP consistently outperforms Health-zkIDM [42] in terms of throughput and latency. The throughput of QP-ChainSZKP, a measure of transactions per second, is notably higher across all operations, ranging from 490 to 510 TPS compared to Health-zkIDM's 322.5 to 345.0 TPS. This substantial difference underscores QP-ChainSZKP's enhanced capacity to handle a larger volume of transactions efficiently.

Additionally, QP-ChainSZKP demonstrates a significant reduction in latency compared to Health-zkIDM. The maximum, minimum, and average latency values for all operations are consistently lower in QP-ChainSZKP. This reduction in latency translates to quicker response times and a more seamless user experience, which is crucial in the context of healthcare identity management where efficiency and security are paramount.

Table 2. *Comparison Table: Multiple Virtual Machines Setup*

Operation	**Metric**	**QP-ChainSZKP**	**Health-zkIDM [42]**
Register Identity	Throughput (TPS)	500	322.5
	Max Latency (s)	2.2	2.94
	Min Latency (s)	0.05	0.02
	Avg Latency (s)	1.05	1.29
Modify Identity	Throughput (TPS)	490	330.4
	Max Latency (s)	2.3	2.89
	Min Latency (s)	0.05	0.04
	Avg Latency (s)	1.10	1.27
Query Identity	Throughput (TPS)	510	345.0
	Max Latency (s)	2.1	2.61
	Min Latency (s)	0.05	0.03
	Avg Latency (s)	1.00	1.25
Revoke Identity	Throughput (TPS)	500	343.6
	Max Latency (s)	2.2	2.88
	Min Latency (s)	0.05	0.02
	Avg Latency (s)	1.05	1.26

3.4 Security Analysis from Health-zklDM

Health-zkIDM [42], while innovative, is limited by its reliance on a trusted third party for identity verification and its relatively lower throughput compared to the proposed QP-ChainSZKP framework. This limitation can introduce potential bottlenecks and vulnerabilities, especially in high-traffic scenarios. QP-ChainSZKP, with its decentralized architecture and enhanced throughput, addresses these limitations, offering a more robust and scalable solution for identity management in the healthcare sector. Table 3 presents the overall security analysis comparing with the exisitng research work [42]. The QP-ChainSZKP framework incorporates advanced quantum-resistant cryptographic algorithms and enhanced zero-knowledge proof mechanisms that significantly bolster the security profile beyond what is described in the Health-zkIDM system:

Quantum Resistance: QP-ChainSZKP uses quantum-resistant algorithms that are designed to withstand potential future threats posed by quantum computing. This is a forward-looking approach that ensures long-term security, particularly important as quantum computing technology evolves.

Enhanced Zero-Knowledge Proofs*:* The zero-knowledge proofs in QP-ChainSZKP are optimized for efficiency and security, providing stronger assurance that no sensitive information is leaked during transactions. These proofs are more comprehensive than those used in Health-zkIDM, covering a broader range of data types and transaction scenarios.

Scalable Security: QP-ChainSZKP's security framework is designed to be scalable, maintaining its robustness as the system scales up in terms of user numbers and transaction volumes, which is crucial for cloud environments.

Comprehensive Compliance: Beyond the security measures for data protection, QP-ChainSZKP ensures compliance with more stringent regulations such as GDPR, HIPAA, and PCI-DSS, providing a versatile framework suitable for various industries beyond healthcare.

Table 3. *Security Analysis Table*

Security Feature	**QP-ChainSZKP**	**Health-zkIDM**
Quantum Resistance	Supported	Not Supported
Zero-Knowledge Proofs	Advanced ZKP Implementation	Basic ZKP Implementation
Resistance to Replay Attacks	Enhanced Protection	Standard Protection
Impersonation Attack Resistance	Robust Identity Verification	Basic Identity Verification
Insider Threat Mitigation	Comprehensive Access Controls	Limited Access Controls
Compliance (GDPR, HIPAA, PCI-DSS)	Full Compliance	Partial Compliance

3.5 Discussion

The proposed QP-ChainSZKP framework and the existing Health-zkIDM [42] system both aim to enhance security and privacy in their respective fields using blockchain and zero-knowledge proof technologies. This section discusses the comparative analysis based on the security features, scalability, and practical implementation of both systems.

Security Features: The QP-ChainSZKP framework integrates quantum-resistant cryptographic algorithms that provide a robust defense against both current and potential future quantum threats, which are not addressed by the Health-zkIDM [42] system. Moreover, QP-ChainSZKP employs advanced zero-knowledge proofs that offer greater efficiency and broader application potential compared to the basic implementation in Health-zkIDM [42]. This ensures higher security and privacy without compromising system performance.

Scalability: While Health-zkIDM [42] demonstrates good performance with throughput over 400 TPS, QP-ChainSZKP is designed to handle higher transaction loads efficiently across diverse cloud computing environments. Its architecture supports dynamic scalability, which is critical for cloud applications experiencing variable workloads. This feature allows QP-ChainSZKP to maintain high performance and low latency consistently, unlike Health-zkIDM [42], which may face scalability limits in more diverse environments.

Compliance and Adaptability: QP-ChainSZKP is built to comply with stringent international standards such as GDPR, HIPAA, and PCI-DSS, making it suitable for a wider range of industries beyond healthcare. This compliance is embedded into the design of the cryptographic and blockchain operations, ensuring that the framework meets the highest standards of data protection and privacy.

Practical Implementation: Both systems utilize blockchain technology effectively; however, QP-ChainSZKP extends functionality with its integration of FHE and a customized blockchain operation algorithm. These enhancements facilitate secure, efficient operations across multiple cloud services, providing a versatile and secure platform for enterprise-level applications.

The following table 4 outlines a comparative analysis of security features between QP-ChainSZKP and Health-zkIDM [42] based on the discussion above:

Table 4. *Security Analysis Table Comparison*

Security Aspect	QP-ChainSZKP	Health-zkIDM [42]
Quantum Resistance	Provided (Advanced algorithms)	Not provided
Zero-Knowledge Proofs	Advanced implementations	Basic implementations
Scalability	High (Dynamic scalability supported)	Moderate (Limited scalability)
Compliance	GDPR, HIPAA, PCI-DSS compliant	Limited compliance
Practical Implementation	Versatile and adaptable for various industries	Primarily healthcare-focused

4. Conclusions

The QP-ChainSZKP framework introduces a significant advancement in the realm of cloud security by integrating quantum-resistant cryptographic algorithms and enhanced zero-knowledge proof mechanisms. Designed to safeguard cloud applications from both current cybersecurity threats and future quantum computing vulnerabilities, this framework provides a robust solution for protecting sensitive data across various platforms. Throughout its development, QP-ChainSZKP has demonstrated superior capabilities in ensuring data privacy and system scalability, evidenced by rigorous simulations that present its ability to handle high throughput and maintain low latency under varying load conditions. The experimental results confirm that QP-ChainSZKP not only meets but outperform the current security standards, offering a comprehensive system that ensures data integrity and confidentiality without compromising on performance. This is achieved through a meticulous design that combines FHE with blockchain technology, enabling secure and efficient data processing and storage. By maintaining high security and compliance with stringent regulatory standards, such as GDPR and HIPAA, QP-ChainSZKP positions itself as a future-proof framework for industries where data security is paramount.

While the current framework handles scalability effectively, further research could explore more dynamic scalability solutions to manage unpredictable workloads more efficiently. As the Internet of Things (IoT) becomes more prevalent, integrating QP-ChainSZKP with IoT devices could provide a secure method for managing the vast amount of data these devices generate. Blockchain technology has been studied and reported in literature [48-54].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Singh, Vineeta, and Vandana Dixit Kaushik. (2024). Navigating the Landscape of Security Threat Analysis in Cloud Computing environments. In *Security and Risk Analysis for Intelligent Cloud Computing*. 1-25. CRC Press.

[2] Angel, Nancy A., Dakshanamoorthy Ravindran, PM Durai Raj Vincent, Kathiravan Srinivasan, and Yuh-Chung Hu. (2021). Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. *Sensors.* 22(1): 196. DOI: 10.3390/s22010196

[3] Ionescu, Sergiu-Alexandru, and Vlad Diaconita. (2023). Transforming financial decision-making: the interplay of AI, cloud computing and advanced data management technologies. *International Journal of Computers Communications & Control*. 18(6). DOI:10.15837/ijccc.2023.6.5735

[4] Aceto, Giuseppe, Valerio Persico, and Antonio Pescapé. (2020). Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *Journal of Industrial Information Integration*. 18 100129. DOI: 10.1016/j.jii.2020.100129

[5] Bharany, Salil, Sandeep Sharma, Osamah Ibrahim Khalaf, Ghaida Muttashar Abdulsahib, Abeer S. Al Humaimeedy, Theyazn HH Aldhyani, Mashael Maashi, and Hasan Alkahtani. (2022). A systematic survey on energy-efficient techniques in sustainable cloud computing. *Sustainability.* 14(10): 6256. DOI:10.3390/su14106256

[6] Alaghbari, Khaled A., Mohamad Hanif Md Saad, Aini Hussain, and Muhammad Raisul Alam. (2022). Complex event processing for physical and cyber security in datacentres-recent progress, challenges and recommendations. *Journal of Cloud Computing*. 11(1): 65. DOI:10.1186/s13677-022-00338-x

[7] Lone, Aejaz Nazir, Suhel Mustajab, and Mahfooz Alam. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Security and Privacy*. 6(6): e318. DOI:10.1002/spy2.318

[8] Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*. 2(1): 129-171. DOI: 10.60087/jaigs.v2i1.102

[9] Stutz, Dalmo, Joaquim T. de Assis, Asif A. Laghari, Abdullah A. Khan, Nikolaos Andreopoulos, Andrey Terziev, Anand Deshpande, Dhanashree Kulkarni, and Edwiges GH Grata. (2024). Enhancing Security in Cloud Computing Using Artificial Intelligence (AI). *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection*. 179-220. DOI:10.1002/9781394196470.ch11

[10] Anthi, Eirini, Lowri Williams, Vasilis Ieropoulos, and Theodoros Spyridopoulos. (2024). Investigating Radio Frequency Vulnerabilities in the Internet of Things (IoT). *IoT*. 5(2): 356-380. DOI:10.3390/iot5020018

[11] Baseri, Yaser, Vikas Chouhan, and Ali Ghorbani. (2024). Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure. *arXiv preprint arXiv:2404.10659*. DOI: 10.48550/arXiv.2404.10659

[12] Rahul, R., S. Geetha, Soniya Priyatharsini, K. Mehata, Ts Sundaresan Perumal, N. Ethiraj, and S. Sendilvelan. (2024). Cybersecurity Issues and Challenges in Quantum Computing. *Topics in Artificial Intelligence Applied to Industry 4.0*. 203-221. DOI:10.1002/9781394216147.ch11

[13] Bhat, M. Iqbal, and Kaiser J. Giri. (2021).Impact of computational power on cryptography. *Multimedia Security: Algorithm Development, Analysis and Applications*. 45-88. DOI:10.1007/978-981-15-8711-5_4

[14] Vaishnavi, Anshika, and Samaya Pillai. (2021). Cybersecurity in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods. In *Journal of Physics: Conference Series*. 1964(4): 042002. IOP Publishing. DOI:10.1088/1742-6596/1964/4/042002

[15] Rosch-Grace, Dominic, and Jeremy Straub. (2022). Analysis of the likelihood of quantum computing proliferation. *Technology in Society*. 68: 101880. DOI:10.1016/j.techsoc.2022.101880

[16] Rajawat, Anand Singh, S. B. Goyal, Chaman Verma, and Jaiteg Singh. (2024). Advancing network security paradigms integrating quantum computing models for enhanced protections. In *Applied Data Science and Smart Systems*, pp. 517-528. DOI:10.1201/9781003471059-66

[17] Atiewi, Saleh, Amer Al-Rahayfeh, Muder Almiani, Salman Yussof, Omar Alfandi, Ahed Abugabah, and Yaser Jararweh. (2020). Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography. *IEEE Access*. 8: 113498-113511. DOI:10.1109/ACCESS.2020.3002815

[18] Javadpour, Amir, Forough Ja'fari, Tarik Taleb, Yue Zhao, Yang Bin, and Chafika Benzaïd. (2023). Encryption as a service for IoT: opportunities, challenges and solutions. *IEEE Internet of Things Journal*. 11(5): 7525-7558. DOI:10.1109/JIOT.2023.3341875

[19] Wang, Wenjia, Seyed Masoud Sadjadi, and Naphtali Rishe. (2024). A Survey of Major Cybersecurity Compliance Frameworks. In *2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity)*, *IEEE*. 23-34. DOI:10.1109/BigDataSecurity62737.2024.00013

[20] Apeh, Apeh Jonathan, Azeez Olanipekun Hassan, Olajumoke Omotola Oyewole, Ololade Gilbert Fakeyede, Patrick Azuka Okeleke, and Olubukola Rhoda Adaramodu. (2023). GRC strategies in modern cloud infrastructures: a review of compliance challenges. *Computer Science & IT Research Journal*. 4(2): 111-125. DOI:10.51594/csitrj.v4i2.609

[21] Rani, Sita, Pankaj Bhambri, and Aman Kataria. (2023). Integration of IoT, Big Data, and Cloud Computing Technologies: Trend of the Era. In *Big Data, Cloud Computing and IoT*. 1-21. Chapman and Hall/CRC,.

[22] Reddy, M. Vijay Bhasker, Rajiv Kumar, Akash Bag, Abdulnaser A. Hagar, G. Vaitheeswaran, and Vikas Tripath. (2022). The multi layer security network authentication system development through blockchain technology. In *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. 259-264. IEEE,. DOI:10.1109/ICACITE53722.2022.9823909

[23] Zhou, Lu, Abebe Diro, Akanksha Saini, Shahriar Kaisar, and Pham Cong Hiep. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*. 80: 103678. DOI:10.1016/j.jisa.2023.103678

[24] Xu, Yuqing, Guangxia Xu, Yong Liu, Yuan Liu, and Ming Shen. (2024). A survey of the fusion of traditional data security technology and blockchain. *Expert Systems with Applications*. 252(5): 124151. DOI:10.1016/j.eswa.2024.124151

[25] Zhang, Bingxue, Guangguang Lu, Pengpeng Qiu, Xumin Gui, and Yang Shi. (2023). Advancing federated learning through verifiable computations and homomorphic encryption. *Entropy*. 25(11): 1550. DOI:10.3390/e25111550

[26] Du, Zhiqiang, Wenlong Jiang, Chenguang Tian, Xiaofeng Rong, and Yuchao She. (2023). Blockchain-based authentication protocol design from a cloud computing perspective. *Electronics*. 12(9): 2140. DOI: 10.3390/electronics12092140

[27] Casanova-Marqués, Raúl, Joaquín Torres-Sospedra, Jan Hajny, and Michael Gould. (2023). Maximizing privacy and security of collaborative indoor positioning using zero-knowledge proofs. *Internet of*

Things. 22: 100801. DOI: 10.1016/j.iot.2023.100801

[28] Exceline, C. Eben, and Sivakumar Nagarajan. (2024). Flexible access control mechanism for cloud stored EHR using consortium blockchain. *International Journal of System Assurance Engineering and Management*. 15(1): 503-518. DOI:10.21203/rs.3.rs-397642/v1

[29] Sucharitha, G., Vedula Sitharamulu, Sachi Nandan Mohanty, Anjanna Matta, and Deepa Jose. (2023). Enhancing secure communication in the cloud through blockchain assisted-cp-dabe. *IEEE Access*. 1(1):99. DOI:10.1109/ACCESS.2023.3312609

[30] Yang, Wencheng, Song Wang, Hui Cui, Zhaohui Tang, and Yan Li. (2023). A review of homomorphic encryption for privacy-preserving biometrics. *Sensors*. 23(7): 3566. DOI:10.3390/s23073566

[31] Doan, Thi Van Thao, Mohamed-Lamine Messai, Gérald Gavin, and Jérôme Darmont. (2023). A survey on implementations of homomorphic encryption schemes. *The Journal of Supercomputing*. 79(13): 15098-15139. DOI:10.21203/rs.3.rs-2018739/v1

[32] Mahato, Ganesh Kumar, and Swarnendu Kumar Chakraborty. (2023). A comparative review on homomorphic encryption for cloud security. *IETE Journal of Research*. 69(8): 5124-5133. DOI:10.1080/03772063.2021.1965918

[33] Saxena, Urvashi Rahul, and Taj Alam. (2023). Role-based access using partial homomorphic encryption for securing cloud data. *International Journal of System Assurance Engineering and Management*. 14(3): 950-966. DOI: 10.1007/s13198-023-01896-2

[34] Komar, Rajesh, and Arjun Patil. (2023). Emerging Trends in Cloud Computing: A Comprehensive Analysis of Deployment Models and Service Models for Scalability, Flexibility, and Security Enhancements. *Journal of Intelligent Systems and Applied Data Science*. 1(1): 20-28.

[35] Nguyen, Hoa T., Prabhakar Krishnan, Dilip Krishnaswamy, Muhammad Usman, and Rajkumar Buyya. (2024). Quantum Cloud Computing: A Review, Open Problems, and Future Directions. *arXiv preprint arXiv:2404.11420*. DOI:10.48550/arXiv.2404.11420

[36] Srivastava, Tanya, Bharat Bhushan, Saurabh Bhatt, and AKM Bhalul Haque. (2022). Integration of quantum computing and blockchain technology: a cryptographic perspective. In *Multimedia Technologies in the Internet of Things Environment*. 3: 197-228. Singapore: Springer Singapore,. DOI:10.1007/978-981-19-0924-5_12

[37] Huang, Jose Luis Lo, and Vincent C. Emeakaroha. (2024). Performing Distributed Quantum Calculations in a Multi-cloud Architecture Secured by the Quantum Key Distribution Protocol. *SN Computer Science*. 5(4): 410. DOI:10.1007/s42979-024-02761-0

[38] Preskill, John. (2023). Quantum computing 40 years later. In *Feynman Lectures on Computation*. pp. 193-244. CRC Press,. DOI: 10.48550/arXiv.2106.10522

[39] Yu, Wang-Ke, and Xi-En Cheng. (2023). New Post-quantum Blockchain Privacy Protection Scheme Based on the Signcryption. *International Journal of Network Security*. 25(3): 495-501. DOI:10.6633/IJNS.202305 25(3).13

[40] Wazid, Mohammad, Ashok Kumar Das, and Youngho Park. (2024). Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future Research. *IEEE Open Journal of the Computer Society*. 99: 1-20. DOI:10.1109/OJCS.2024.3397307

[41] Kuznetsov, Oleksandr, Alex Rusnak, Anton Yezhov, Dzianis Kanonik, Kateryna Kuznetsova, and Stanislav Karashchuk. (2024). Enhanced Security and Efficiency in Blockchain with Aggregated Zero-Knowledge Proof Mechanisms. *IEEE Access*. 1(1): 99. DOI:10.1109/ACCESS.2024.3384705

[42] Bai, Tianyu, Yangsheng Hu, Jianfeng He, Hongbo Fan, and Zhenzhou An. (2022). Health-zkIDM: a healthcare identity system based on fabric blockchain and zero-knowledge proof. *Sensors*. 22(20): 7716. DOI:10.3390/s22207716

[43] Feng, Tao, Pu Yang, Chunyan Liu, Junli Fang, and Rong Ma. (2022). Blockchain Data Privacy Protection and Sharing Scheme Based on Zero- Knowledge Proof. *Wireless Communications and Mobile Computing* 2022: 1-11. DOI:10.1155/2022/1040662

[44] Zhang, Ye, Shuo Wang, Xian Zhang, Jiangbin Dong, Xingzhong Mao, Fan Long, Cong Wang, Dong Zhou, Mingyu Gao, and Guangyu Sun. (2021). Pipezk: Accelerating zero-knowledge proof with a pipelined architecture." In *2021 ACM/IEEE 48th Annual International Symposium on Computer Architecture (ISCA)*, pp. 416-428. IEEE,. DOI:10.1109/ISCA52012.2021.00040

[45] Abdelkhalek, Kais, Wissam Chemissany, Leander Fiedler, Gianpiero Mangano, and René Schwonnek. (2016). Optimal uncertainty relations in a modified Heisenberg algebra. *Physical Review D*. 94(12): 123505. DOI: 10.1103/PhysRevD.94.123505

[46] Fahim, Shahriar, S. Katibur Rahman, and Sharfuddin Mahmood. (2023). Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV. *Int. J. Math. Sci. Comput.* 3: 46-57. DOI:10.5815/ijmsc.2023.03.04

[47] Khalil, Muhammad Khuram, Marwa Al Jahdhami, and Vishal Dattana. (2023). Cloud Storage Security Compliance: An Analysis of Standards and Regulations. *Journal of Student Research*.

[48] M. Husain Bathushaw, & S. Nagasundaram. (2024). The Role of Blockchain and AI in Fortifying Cybersecurity for Healthcare Systems. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1120-1129. https://doi.org/10.22399/ijcesen.596

[49] TAKAOĞLU, M., ÖZYAVAŞ, A., AJLOUNİ, N., DURSUN, T., TAKAOĞLU, F., & DEMİR, S. (2023). OTA 2.0: An Advanced and Secure Blockchain Steganography Algorithm . *International Journal of Computational and Experimental Science and Engineering*, 9(4), 419–434. Retrieved from https://ijcesen.com/index.php/ijcesen/article/view/289

[50] Prasada, P., & Prasad, D. S. (2024). Blockchain-Enhanced Machine Learning for Robust Detection of APT Injection Attacks in the Cyber-Physical Systems. *International Journal of Computational and Experimental Science and Engineering*, 10(4);799-

810. https://doi.org/10.22399/ijcesen.539

[51] BENTAJER, A., HEDABOU , M., ENNAAMA, F., & ELFEZAZİ , S. (2020). Development of Design for Enhancing Trust in Cloud's SPI Stack. *International Journal of Computational and Experimental Science and Engineering*, 6(1), 13–18. Retrieved from https://ijcesen.com/index.php/ijcesen/article/view/109

[52] El-Taj, H. (2024). A Secure Fusion: Elliptic Curve Encryption Integrated with LSB Steganography for Hidden Communication. *International Journal of Computational and Experimental Science and Engineering*, 10(3);434-460. https://doi.org/10.22399/ijcesen.382

[53] Alkhatib, A., Albdor , L., Fayyad, S., & Ali, H. (2024). Blockchain-Enhanced Multi-Factor Authentication for Securing IoT Children's Toys: Securing IoT Children's Toys. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1041-1049. https://doi.org/10.22399/ijcesen.417

[54] P., V., & A., M. R. (2024). A Scalable, Secure, and Efficient Framework for Sharing Electronic Health Records Using Permissioned Blockchain Technology. *International Journal of Computational and Experimental Science and Engineering*, 10(4);827-834. https://doi.org/10.22399/ijcesen.535