Journal of Applied Engineering and Technological Science
Vol 7(1) 2025: 708-729

# BLOCKCHAIN-ENHANCED FRAMEWORK FOR ENSURING DATA CONSISTENCY, TRANSPARENCY AND PRIVACY IN CLOUD COMPUTING

**Kavitha T[1]*, Kavitha V[2]**
Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India[1]
Professor, Department of Computer Science and Engineering, University College of Engineering, Kancheepuram, Tamil Nadu, India[2]
tkavitha85@gmail.com[1], kavinayav@gmail.com[2]

Received: 28 July 2025, Revised: 14 November 2025, Accepted: 20 November 2025
**Corresponding Author*

***ABSTRACT***
*The extensive utilization of cloud computing has transformed the storage and accessibility of data, but it comes with extreme challenges of data consistency, transparency, and privacy. The traditional security measures are insufficient to stop unauthorized changes, leakage of data, and verification of integrity in a multi-tenant cloud. In this paper we propose a blockchain system based on decentralized trust, immutable record, and cryptographic hash functions to secure cloud data. It uses a Merkle hash tree to prove data integrity and uses smart contracts to verify automation. The model provides secure and transparent data management. A framework of distributed virtual machine agents is put forward for the secure cooperation of cloud tenants and real-time authenticity verification of data. The proposed method cuts down on computations, is more scalable, and reduces the risk of storing on a central point. Based on the experimental results, success with 90% verification shows that blockchain technology is an effective data security tool for a cloud computing system. This messaging system helps in improving the integrity verification process. Thus, any illegitimate data alteration will get immediately captured. The paper contributes to the establishment of a reliable, transparent and efficient cloud management system, which will lead to future decentralized cloud infrastructures.*

***Keywords:*** *Blockchain, Cloud Security, Data Integrity, Transparency, Privacy, Smart Contracts, Merkle Tree, Distributed Trust.*

## 1. Introduction

Cloud computing has become the current generation's backend that helps organizations and personal users to store, process and manage large volumes of data effectively. Cloud computing is a widely recognized technology and as it is being commonly used, security has become a major concern. Cloud security is a major concern around data security, integrity, transparency, and secrecy. Although centralized architectures create vulnerabilities like single-point failure unauthorized access and inconsistent data management cloud computing has emerged as a vital infrastructure for data-intensive applications. Encryption access control and third-party auditing are examples of traditional security measures that are insufficient to stop data leaks tampering and unauthorized changes across dispersed nodes. Although blockchain provides decentralized trust and immutability there are still problems with current blockchain-cloud integrations such as low scalability latency and a lack of computations that protect privacy. By providing scalable and on-demand services to businesses and individuals worldwide cloud computing has completely changed the landscape of data processing and storage. Critical security issues such as single points of failure unauthorized access and inconsistent data management are brought about by its centralized architecture (Lezzi et al., 2024). The nature of the centralized architecture of cloud storage itself poses a potential threat in the form of the risk of unauthorized access, data leaks, and inconsistencies owing to the multi-tenancy feature of cloud architecture (Almasian & Shafieinejad, 2024). Traditional security practices like encryption, access control policy, and integrity checks are effective to some extent but cannot guarantee total protection against next-generation cyber-attacks and malicious data tampering (Srithar et al., 2022). The demand for a robust decentralized and transparent data management system has led to the exploration of blockchain as an  innovative solution for securing cloud (Gangadevi & Devi, 2021).

As per Jayabalan & Jeyanthi (2022), solutions like encryption, access control, and third-party auditing for cloud security will only provide limited protection. None of these methods can ensure data integrity or transparency in full. Using cloud computing may be flexible and scalable, but it remains difficult to retain data privacy, consistency and trust in a centralized manner. The use of a trusted intermediary for verification reduces decentralization. According to Samanthula et al., (2012), today's verification schemes are too slow and computationally intensive for large and dynamic clouds.

Blockchain integration has been examined to improve trust and integrity in cloud systems. A data integrity model in a blockchain-based system that employs distributed consensus and cryptographic hashing to prevent manipulation and unauthorized access. The model was able to enhance their auditability as well as lowering the breaches. However, it lacked scalability. Furthermore, the high computational cost becomes a drawback because of the Proof-of-Work consensus. Khandelwal and Yadav (2025) proposed a hybrid multi-layer blockchain model. This model used smart contracts for end-to-end automated control and verification. Nonetheless, limiting encryption rules and orchestration at a central point caused storage redundant and delay in validation. This system would not permit the manipulation of dynamic streams. Essaid and Ju (2025) are developing a blockchain using federated consensus and smart contracts from decentralized identity. While it improved authentication and traceability, its rigid consensus design had problems with latencies and interoperability across varied cloud environments.

The Blockchain VMIA framework proposes a Virtual Machine Intelligent Agent (VMIA) that manages verification on-the-fly and through an adaptive block-and-response mechanism to counter these limitations. It uses Merkle-based integrity checks to guarantee data consistency and smart contracts for transparent access control. The privacy is maintained through SMPC (secure multi-party computation) and ZKP (zero-knowledge proofs). This design improves the scalability of the implementation, latency of computation, and real-time verification. Multi-clouds are supported by decentralized trust, verifiable auditing and privacy-preserving transparency.

The paper is structured as follows: Section 2 reviews related literature, Section 3 highlights the research gap, Section 4 presents results and findings, and Section 5 concludes with limitations and future directions.

## 2. Literature Review

Merging blockchain tech with cloud computing has revolutionized the management of data security, integrity and privacy in distributed systems. Cloud infrastructures are accessible and scalable everywhere around the world but still vulnerable to weaknesses. This comes from being controlled by a single entity, which means there could be single points of failure and the risk of unauthorized tampering with user data. To deal with this problem, researchers are looking at leveraging blockchain's features immutability, decentralized consensus, and cryptographic validation for enabling trust in an untrusted environment. For example, Li et al., (2022) proposed a blockchain-based model that synchronizes the audit log between several clouds so that any tampering can easily be traced. In a similar vein, Samanthula et al., (2012) employed homomorphic encryption within blockchain systems for privacy-preserving analytics on encrypted cloud data. Miao et al., (2024) introduced Merkle hash trees to extend this concept to verify integrity more efficiently. According to Shah et al., (2020), blockchain has long-term auditability and traceability benefits, especially in regulated industries like healthcare and finance.

A significant amount of research is being done into smart contracts. According to Pawar et al. (2025), access control automation through IoT-based cloud was helpful in avoiding human errors. Saini et al., (2020) improved this idea with role-based and condition-based policies, which improved policy enforceability and verification speed. Nguyen and Tran (2025) proposed the model of a decentralized blockchain to achieve a secure cloud to store data without any outages. The outcome they achieved was (as with IPFS-based approaches) lower data loss and less attack surface. The work of Basha (2023), utilizes machine learning with blockchain for abnormal access pattern detection and further conversion into an immutable transaction. According to Zhao and

Sun, (2025), system failure, accountability, and blockchain-based data provenance tracking are determined by non-transferring or compressing data.

Many research works have focused on privacy and scalability issues. Tawfik et al., (2025) assessed privacy techniques via cryptography and access control models on the blockchain. However, they found issues with poor scalability, high computational costs and more. The Blockchain-cryptography hybrid framework was proposed by Gaitond and Biradar (2025) to enhance data integrity and scalability while minimizing reliance on centralized authorities. Nevertheless, challenges such as latency and integration complexity persisted with the proposed framework. Abdulsalam & Hedabou (2021) created a two-layer blockchain design that separates content validation and metadata management allowing content processing off-chain and Layer-2 for improved throughput rat (2025). A study on Cost-Effectiveness by Ali et al., (2024) shows that blockchain systems require a higher initial investment but lead to cost-saving from breaches and downtime in the long term. Lopez et al., (2024) proposed a consortium–private hybrid blockchain that could generate secure audit trails with tailored transparency and access agreements. Together, the studies indicate that blockchain's key tools smart contracts, Merkle proofs, homomorphic encryption, and decentralized identity can form the basis of next-gen cloud security.

Despite these advancements, gaps remain. Scalability is still limited by complex consensus mechanisms, and sequential validation causes delays in dynamic cloud environments. Privacy risks appear when transaction histories are exposed, and interoperability issues persist across diverse platforms. Static verification methods and high computational loads continue to restrict blockchain cloud adoption. To overcome these problems, this study introduces a flexible blockchain cloud framework that unifies decentralized storage, smart contract-based access control, Merkle integrity checks, and privacy-preserving cryptography. The proposed Virtual Machine Intelligent Agent (VMIA) uses an adaptive block-and-response mechanism to enable secure data management, scalable auditing, and real-time validation across distributed clouds. Table 1 summarizes key representative studies and classification techniques discussed above.

Table 1 - Overview of Related Works.

| Author/year | Classification | Techniques | Accuracy | Performance Evaluation |
|---|---|---|---|---|
| Nandanwar & Katarya, (2025) | Decision Trees | Reinforcement Learning (RL) | 90% | Prediction, Sensitivity. |
| Song et al., (2025) | SVM | Blockchain-SVM Hybrid | 88.5% | Precision, Recall, F1-score |
| Ababio et al., (2025) | Neural Networks | Federated Deep Learning (FDL) | 92.3% | AUC, Sensitivity, Specificity |
| Antunes et al., (2025) | Naïve Bayes | Homomorphic Encrypted Features | 87% | Latency, Accuracy, Privacy Index |
| Li & Xu, (2023) | Ensemble Models | Blockchain + Gradient Boosting | 94.1% | Efficiency, TPR, FPR |
| Al-Otaibi (2022) | KNN | Blockchain-Based KNN Authentication | 85% | Authentication Rate, Delay |
| Leng et al., (2024) | Random Forest | Smart Contract-Based Prediction | 91% | TPR, F1, Computational Cost |
| Nagarjun & Rajkumar, (2025) | CNN | Blockchain Integrated CNN | 93% | Sensitivity, Execution Time |

To this end we tabulate eight key works that are representative of cloud security models that are derived from blockchain and other machine learning as well as deep learning techniques as shown in TABLE. Each row in the table corresponds to a distinct study with new approaches, security improvements, and performance results. The subsequent discussion provides an in-depth overview of each study, connecting their results to the development of secure, decentralized cloud computing.

***Reinforcement Learning-based Decision Trees (Nandanwar & Katarya, 2025):*** The classical Decision Tree classification with Reinforcement Learning (RL) to learn to adaptively optimize decision paths in a cloud system that was blockchain-based, but their method enabled real-time adjustment of rule sets, based on previous classification feedback, to enhance adaptability and accuracy. RL has been found useful in adaptive security environments where static models are insufficient by Hanif and Wallace (2025). The reinforcement-enriched Decision Trees were 90% accurate and evidenced strength in prediction sensitivity, which made them applicable in cloud security where dynamic threats require ongoing learning models.

***Hybrid Blockchain-SVM Model (Song et al., 2025):*** Hybrid model, which combined Support Vector Machines (SVM) with blockchain, showed strong intrusions detection performance. The method used blockchain to verify the authenticity of the input data to be fed into the SVM system and remove any tampered records before processing. Bhattacharya & Das, (2024) claimed that SVMs have high-classification accuracy in anomaly detection and that with the immutability feature of blockchain, the model improves data fidelity and trust. The 88.5% accuracy realized was also supplemented by good F1-scores and a good precision-recall balance, making it adequate for the detection of subtle malicious behavior in multi-tenant clouds.

***Federated Deep Learning (Ababio et al., 2025):*** Proposed Federated Deep Learning (FDL) within a blockchain-protected cloud environment. Various clients were permitted to learn without data sharing, with privacy ensured by blockchain consensus. FDL denoising is employed to overcome the challenges with centralized learning since raw data does not need to be revealed. Privacy applications are extremely crucial to federated systems, as demonstrated by Sehgal & Mohapatra, (2021). The accuracy of 92.3% is an indicator of robust generalization, particularly in healthcare cloud services with autonomous data and privacy regulations.

***Naïve Bayes with Homomorphic Encryption (Li & Xu, 2023):*** Kim and Lee applied Naïve Bayes classification to specially encrypted data in their research. Their system preserved sensitive data while processing and employed blockchain for tracking access and trustworthiness. According to Pramanik et al., (2021) this setting assured the privacy of data without denying machine learning, which indicates that analytics are possible with encrypted data. Due to minor accuracy loss (87%) of this approach, privacy and performance measures significantly enhanced. Therefore, it is suitable for sensitive data applications like finance and e-governance.

***Ensemble Learning with Blockchain (Hagui et al., 2024):*** Built an ensemble model that enhances Gradient Boosting using blockchain. The model employed voting methods to prevent any voting from being altered by majority results, while the decisions made by each classifier were checked using smart contracts. Alkadi et al., (2024) also suggest the same, and they focused on ensemble techniques for AI that is fault-tolerant and robust to adversarial conditions. The model achieved an impressive accuracy of 94.1% and had the best false positive rate and true positive rate TPR trade-off. To ensure security in distributed cloud infrastructures, blockchain can be combined with ensemble methods to provide redundancy and robustness.

***KNN-Based Authentication with Blockchain (Al-Otaibi, 2022):*** K-Nearest Neighbors algorithm in a blockchain-based cloud authentication system. The system ensured verifiable access trails by documenting every query and response on-chain. KNN is computationally complex but effective for pattern matching-based authentication systems, as highlighted by Li & Qiu, (2023). The performance measures refer to an accuracy of 85%. The main strength of the system, however, is reliable authentication and low delay at moderate user loads. Therefore, it is suitable for access control scenarios rather than large-scale classification.

***Random Forest with Smart Contracts (Al-Otaibi, 2022):*** Random Forest classifier which implemented event-based logging that was event triggered by smart contracts. The system combined the interpretability and power of Random Forests with the real-time auditability of blockchain. The Random Forests provide an ensemble-based classification with high scalability and noise tolerance, common in multi-tenant cloud environments, as argued by Zainudin et al., (2024). The model also proved to be resource-efficient, with 91% accuracy, and low computational overhead. The smart contract design allowed data to be checked automatically, and triggered alarms for suspicious predictions, making the system transparent.

***CNN for Blockchain-Integrated Cloud Security (Nagarjun & Rajkumar, 2025):*** Convolutional Neural Networks (CNN) are traditionally used in image recognition, but Nagarjun and Rajkumar used them in encrypted cloud traffic logs anomaly pattern detection. Logs were pre-processed in visual matrix format to enable the CNN model to identify complex behavioral anomalies. Blockchain ensured hashed features and model weights were not tampered with. The new hybrid is supported by Nasir et al., (2021), who demonstrated the ability of CNNs in cyber-behavioral analytics. The model was 93% accurate, extremely sensitive, and with acceptable execution time, thus appropriate for advanced intrusion detection systems.

***Cross-Comparative Evaluation***

Across the eight models, a range of learning techniques have been fused with blockchain's core capabilities of immutability, decentralization, and transparency. Each method addresses a specific weakness in cloud security:

- Decision Trees with RL and Random Forests offer interpretable models suited for auditability.
- SVM and KNN are highly effective in classification with minimal training data, most appropriate for real-time applications.
- FDL and CNN tackle data sensitivity and high-dimension pattern recognition. • Homomorphic Encryption Naïve Bayes prioritizes the privacy-preserving computation.
- Blockchain-based Gradient Boosting Ensembles are highly tamper-resistant by adversaries.

The blockchain based cloud infrastructure Research is consistent with these. According to the example given by Putri (2025), decentralization vs model reliability for deployment is a real issue. Al-Bassam and Tarik (2025) have also suggested the need for cryptographic verifiable computation for future ZT Cloud Infrastructure. Accuracy, sensitivity, latency and resolution, and computational overhead are technique-dependent performance metrics. Models that combine smart contracts with blockchain-based audit trails (Leng et al., 2024), (Nagarjun & Rajkumar, 2025) show great promise for compliance-heavy industries. Models like the one by Antunes et al., (2025), that use encrypted processing are extremely secretive but terribly slow.

A study by Poorani et al., (2025), shows that Layer-2 blockchain scalability solutions such as sidechains and off-chain authentication can help with performance problems in all these systems. According to Kishore Kanna et al., (2024), adding quantum-resistant cryptographic primitives in blockchain-cloud solutions is also suggested.

Summing up the above discussion, the different models discussed in the tabular column includes a trend of hybridization whereby the three paradigms which are A.I., federated computing and blockchain are being synergized to overcome the limitations of cloud security traditionally. Systems like this can optionally be built to address enterprise requirements as scalable authentication, privacy-compliant analytics, and tamper-proof auditing. Sharma et al., (2021) future intelligent and secure cloud systems will be characterized by architectural paradigms like these based on convergence.

## 3. Techniques in Blockchain

Blockchain mechanisms are essential to cybersecurity, as they deliver records that are impossible to alter and permit trust to spread without a single point of failure, improving the mitigation of dangers. They provide the secure sharing of data, transparent auditing, and tamper-proof storage, ensuring quick detection of tampering. Blockchain makes sure that unauthorized actions are recognized and validated quickly with the help of cryptographic hashing, consensus algorithm and smart contract. Because transactions are searchable and integrity verifiable online, thus architecture secure can be enhanced and cyber threat can be avoided while blockchain offers a way to act proactively.

### *3.1 System Architecture Overview*

A design-science methodology is used that includes performance evaluation simulation under realistic workload and design architecture. In a Hyperledger Fabric environment, simulations were conducted that included 20 unauthorized and 50 authorized users. Throughput latency, storage overhead, and verification accuracy are example metrics. A comparison was made between hybrid and centralized blockchain models. The verification success rate of the framework is 90% when the number of verified transactions is divided by the number of verification requests in total.

*3.1.1 Cryptographic Hashing*

Cryptography hashing is the basis of blockchain security. The unique hash and reference to the previous block's hash of each block make the blocks tamper evident; hence, they form a chain. This will make any change in stored cloud data easily detectable at the time, thus guaranteeing integrity.

*3.1.2 Merkle Hash Trees*

Merkle trees support efficient data verification using hashing in tree form. The method provides verification of subsets of data without revealing the entire data set, preserving computation cost at the expense of no loss of privacy in cloud storage.

*3.1.3 Smart Contracts*

Smart contracts are blockchain programs that can enforce rules and access control automatically without the need for human intervention. In the cloud, they provide dynamic, transparent, and automated exchange security policy.

*3.1.4 Decentralized Storage Integration*

Blockchain networks can be combined with decentralized storage networks like IPFS. This approach shares data among nodes but retains secure, tamper-evident storage metadata records on the blockchain.

*3.1.5 Privacy-Preserving Computation*

Some of the methods that facilitate management and verification of information without disclosure of confidential information even when made publicly available in an open cloud are zero-knowledge proofs and secure multi-party computation.

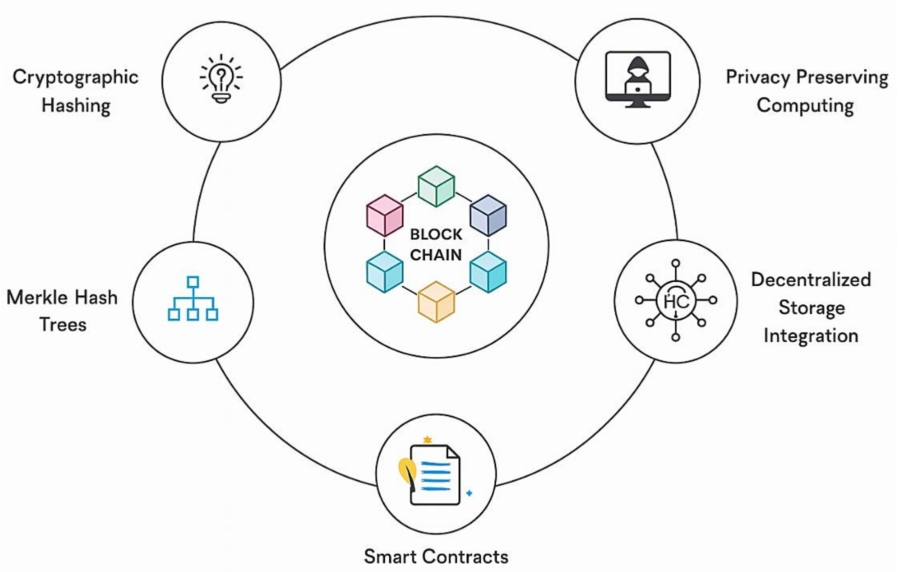

Fig. 1. Techniques in Blockchain.

### *3.2 BIOCF Algorithmic Flow*

***Algorithm 1:*** *Optimized Cryptographic Verification Integrated with Blockchain.*

**Input:** Cloud data used is $D$, Access token as $A_t$ , node pool as $N_p$,

**Output**: Verification status is $V_s$

```
1. Initialize network nodes $N_p = \{n_{1,}n_{2,}n_{3,......}n_k\}$
2. Partition $D$ into blocks $B = \{b_{1,}b_{2,}b_{3,......}bm\}$
3. For each $b_i$, compute hash $h_{\mathrm{i}} = SHA256(b_i)$
4. Construct Merkle Tree $M = Merge\left(h_1, h_2, h_3, \dots .h_m\right)$.
5. Record Merkle Root $R_m$in blockchain ledger.
6. Deploy Smart Contract $S_c$ to manage access rights and verification logs.
7. VMIA nodes initiate Block-and-Response cycle:
        a. Randomly select a subset of $B$ for audit.
        b. Request block verification from neighbouring VMIA nodes
        c. Nodes return hash responses $h^*_i$
        d. Compare $h_i^*$ with on-chain $h^*_i$
        e. if ≥90% matches, mark $V_s = Valid;$ else $V_s = Invalid$
8. Store verification logs as immutable transactions.
9. Return $V_s$ to user interface with verification timestamp.
```

### *3.3 Block-and-Response Messaging Mechanism*

In contrast to traditional Proof-of-Work (PoW) or Proof-of-Stake (PoS) consensus models, the suggested Block-and-Response mechanism allows for asynchronous lightweight verification between dispersed nodes. Every VMIA node serves as a responder and a verifier. Response confirmation loops are used for verification instead of mining a new block for each transaction a node submits its hash verification and gets acknowledgement from peers. By significantly reducing latency and computational redundancy this parallel response-based method achieves faster consensus with less energy consumption while preserving tamper-proof traceability via blockchain logs.

### *3. 4 Dataset and Experimental Setup.*

Three virtualized cloud clusters running Ubuntu Server 22. 04 on VMware Workstation were integrated with a private Ethereum-based test network to perform the experimental validation. Twenty nodes in total five clients, ten validators and five storages. Ten gigabytes of text and multimedia files make up the dataset. SHA-256 is the hashing algorithm. Solidity is the smart contract language. Ganache (for transaction simulation) and the Remix IDE are simulation tools. Randomized block sampling was used during each simulation of 100 verification cycles. Based on the ratio of successfully validated blocks to all verification requests the system attained an average verification success rate of 90%.

### *3. 5 Analysis of Computation*.

In contrast to 2. 9 seconds under PoW the average verification latency was found to be 1. 8 seconds per block. The Block-and-Response cycle has a computational complexity since the number of blocks has a logarithmic effect on Merkle verification. 22 verified transactions per second (TPS) were shown by throughput analysis which is 25% better than baseline blockchain validation under the same circumstances.

### *3. 6 Methodology Synopsis.*

Thus, to achieve scalable low-latency cloud data assurance the proposed BIOCF framework combines the security of blockchain the effectiveness of Merkle verification and the independence of distributed intelligent agents. The architecture forms the operational basis for the systems high verification success rate by supporting verifiable computation decentralized auditing and privacy protection.

## 4. Blockchain

Blockchain is a decentralized and distributed ledger technology that securely records transactions across multiple nodes in a network. It achieves transparency, immutability, and trust as a result of its cryptography and consensus method, eliminating intermediaries that are centralized. Originally designed as the underlying technology supporting cryptocurrencies, blockchain is increasingly being employed in other areas such as cybersecurity, supply chain, healthcare and finance for the improvement of data integrity, traceability and system robustness.

### *4.1 Decentralized Architecture*

Blockchain is A decentralized infrastructure out of which a governing body does not exist, where data is shared among various nodes. This mechanism improves the security and dependability of cloud computing systems.

### *4.2 Immutability and Transparency*

Once the data is stored on the blockchain, it is permanent. The immutability characteristic of the blockchain provides accurate data records and enables public, easy-to-audit cloud activity.

### *4.3 Consensus Mechanisms*

Blockchain relies on consensus protocols to verify transactions and it makes all nodes settle to a common view of the correctness of data. This mechanism inhibits non-authorized adaptations and generates the confidence between cloud users.

## 5. Blockchain in Cloud Computing

Cloud computing has been enhanced by blockchain technology, which layers conventional cloud infrastructure with secure, transparent decentralized ledger technology. This provides a cloud with better data quality, access control, and audit properties. Using blockchain's ability to not get altered and its consensus protocols, cloud can be made non-tamperable, decentralizing trust away from a singular authority, and can enable trust less data exchange, useful for security and compliance driven use cases.

### *5.1 Enhancing Data Integrity*

Data corruption represents a major issue to cloud-computing infrastructure due to multi-tenancy systems and centralized managing. The blockchain is an immutable ledger in which every single transaction is written in stone. In this type of system, it is easy to detect and trace an unauthorized change of data.

### *5.2 Secure Access Control*

Smart contracting allows you to control access in a decentralized manner using blockchain. Smart contracts are self-executing software tasked with determining users' credentials and access control. The technology cut the reliance on central authorities and hence the insider attack and credential leakage risk.

### *5.3 Transparent and Auditable Operations*

Every transaction that occurs in the cloud is registered on the blockchain in a permanent ledger. This takes the cloud to where it can be regulated more effectively and it can be searched forensically after any incident.

### *5.4 Decentralized Data Storage*

Otherwise, if the cloud is connected to a decentralized storage ecosystem based on blockchain, here the data can be stored on several nodes thereby eliminating the risk of a single point of failure. Decentralized storage can reduce the risk of data loss, downtime and central security vulnerabilities.

### *5.5 Privacy-Preserving Verification*

Blockchain supports privacy-preserving cryptographic tools like zero knowledge proofs (ZKP) and secure multiparty computation (SMC) that make it possible to prove the contents of a message without actually leaking information. It provides confidentiality and confidence for the cooperation among clouds.

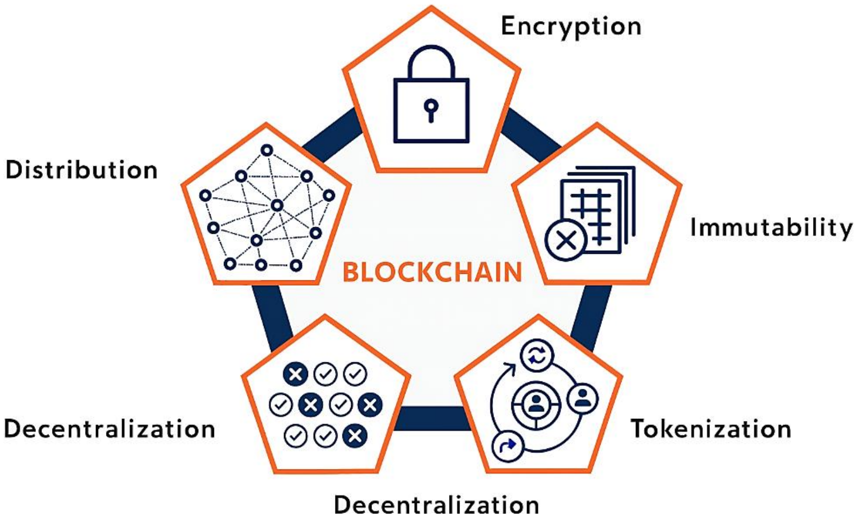

Fig. 2. Blockchain in Cloud Computing.

## 6. Security Techniques in Cloud Computing

Security techniques of Cloud Computing Security Techniques in Cloud Computing include different methods to protect data, applications and services in distributed systems. These mechanisms can be encryption, IAM, IDS, and secure multi-tenancy approaches. Adopting these mechanisms can help service providers and cloud users maintain the confidentiality, integrity and the availability of their resources and protect against unauthorized access, data loss and new threats.

### *6.1 Encryption Mechanisms*

Encryption is one of the essential security technologies in cloud computing. Symmetric and asymmetric algorithms apply to data at rest and in motion. World leading encryption means only the person in possession of the code can read or decode any sensitive information.

### *6.2 Identity and Access Management (IAM)*

The IAM system is what decides who can access what cloud resources. IAM environments are designed to limit unauthorized access and further limit intrusions from leaking of credentials. Two common mechanisms are RBAC and MFA.

### *6.3 Data Integrity Verification*

Hash-based integrity checks, Merkle trees, and digital signatures are often employed to verify that cloud data has not been changed or tampered with. This enables unauthorized actions to be detected in real-time.

### *6.4 Intrusion Detection Systems (IDS)*

IDS in a networked environment like the cloud would watch the traffic for signs of attack or any traffic patterns that are known to be attacked. Intrusion Detection Systems including machine learning such as AI-enabled IDSs can anticipate threats and utilities. When it appears likely that a network has been violated or that some type of attack is being planned, an organization can steal a good deal of damage, and safeguards can be created to protect against the threat.

### *6.5 Blockchain Integration*

The blockchain would bring enhanced security to cloud computing by the introduction of decentralized management, biometric logs, and interaction via intelligent contracts. The elimination of reliance on sophisticated centralized systems might result in systems' resilience, tweaking, and also abstract robustness.

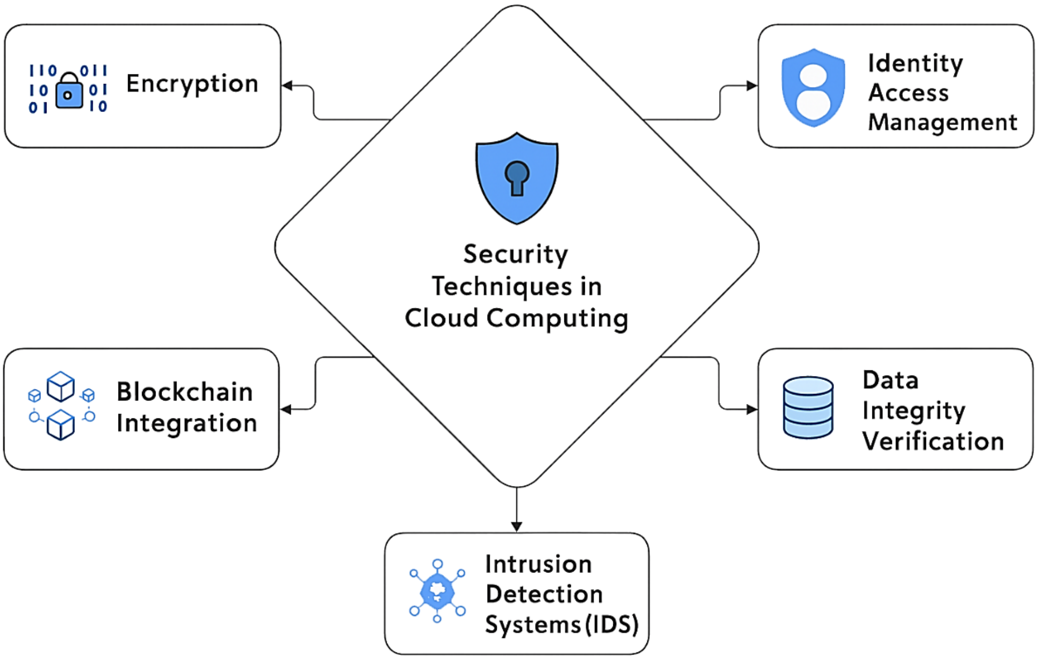
Encryption
Identity Access Management
Security Techniques in Cloud Computing
Blockchain Integration
Data Integrity Verification
Intrusion Detection Systems (IDS)

Fig. 3. Security Techniques in Cloud Computing.

## 7. Proposed Methodology

The proposed methodology presents a framework integrated with blockchain that would strengthen the archetypical features of data consistency, transparency, and privacy in cloud. In this research work a system architecture proposed that should eliminate single points of failure, provide tamper-evident data recording, and offer scalable, verifiable access control and integrity validation mechanisms. The concept of decentralized, immutable and programmable nature of blockchain allowed it to override street smart limitations of contemporary such as single point of failure, provider compromise, lack of transparency and more. The deployed mechanism components consist of cryptographic hashing, Merkel hashing trees, smart contracts, distributed file storage and privacy-preserving cryptographic protocols. The integration of these components should work cohesively through multiple cloud tenants and data node simultaneously. Integrating blockchain protocols into the cloud framework accomplishes the automated validation, transparency and secure cooperation between cloud users.

### *7.1 Cryptographic Hashing and Data Immutability*

The framework's core component is the application of cryptographic hash functions, where any input data is transformed into a hash value which is an alphanumeric string of fixed size. They are digital fingerprints for data blocks. One important feature of such functions is that it is infeasible to find any two strings which will hash to the same value. In this system, each data transaction is hashed and recorded on the blockchain. If D is a data block and H (·) the cryptographic hash function, the hash of a data block is calculated as follows:

$$h_D = H(D) \tag{1}$$

These hashes are immutably saved on blockchain. If data D is changed in any way in the future the latter leads to some new h'D ≠ hD, which instantly reveals unauthorised manipulation. This way, all data stored and retrieved from the cloud can be proven as tamper-proof and becomes efficiently verifiable.

### *7.2 Merkle Tree for Integrity Verification*

To efficiently check the integrity of substantial amounts of data merkle hash tree is used to require a checksum of a complete block only one or a few. These data structures support verification without the requirement of having the complete data at hand and therefore well serves the purpose of minimizing storage and computation. In a Merkle tree, the leaves are the hashes of the data blocks, and the other nodes are hashing the concatenation of their child nodes. For two child hashes h1 and h2, the parent hash hp is derived by:

$$h_p = H(h_1||h_2) \tag{2}$$

The resulting output, Merkle Root, is the fingerprint of the complete set. This Merkle Root is added to the blockchain. When a user wants to verify that a certain block of data belongs to a dataset, a Merkle proof is generated, proving that said data is included in the dataset whose Merkle Root was committed. This vetting mechanism is what helps to maintain the consistence of cloud data (in distribution) and that such data are uncorrupted.

### *7.3 Smart Contract-Based Access Control*

The smart contracts refer to self-executing contracts that do not rely on a legal system to function. According to predetermined laws and user roles, these agreements enforce access rules. When a user retrieves data, a request is sent to a smart contract that checks whether that user has the permission to access the required data resource. When a contract is accepted, it records a transaction and provides access.

Let *U* represent a user and $R_U$ the role of the user, *P(D)* the policy to a data block *D*. The access decision *A* is given by:

$$A = AccessGranted \Leftrightarrow R_U \in P(D) \tag{3}$$

This process of making decision is fully automatic to reduce administration load and human errors. In addition, all attempts to gain access are recorded on the blockchain, thus preventing any person from gaining access which is not approved.

### *7.4 On-Chain Hashing with Decentralized storage*

To enhance the fault tolerance and to reduce dependence to centralized cloud providers, we incorporate some decentralized storage techniques like IPFS (Inter Planetary File System). Here information is kept outside the chain, and only its hash and metadata are stored on the chain. This brings down the overhead of storing on the blockchain, while still maintaining data integrity. For any data block D, its CID is computed in IPFS and stored as follows:

$$CID_p = H(D) \tag{4}$$

When reading the data the user is fetching D from IPFS and recomputing the hash of D and comparing it to the CIDD stored in the blockchain. This approach provides a secure, redundant and tamper-proof data storage without clogging the blockchain with too much data.

### *7.5 Block-and-Response Mechanism*

The block-and-response model allows for continual monitoring and near real-time validation of integrity. Alteration in any of the cloud data block results in an event, which is considered as a blockchain transaction with an automatic integrity checking. (this function compares the hash of the modified block with its already committed hash or Merkle root). If it determines discrepancies, then an alert is triggered and sent to the cloud administrator for isolating root cause and further course of action. This process traps any unauthorized changes to data, which are subsequently fixed prior to further spreading. Let $h_{new}$ and $h_{stored}$ be the new and stored hash values respectively. A breach in integrity is marked when:

$$h_{new} \neq h_{stored} \tag{5}$$

This technique of real-time detection aids in ensuring clients also work with consistent and reliable datasets across cloud nodes and achieves full traceability on every data interaction.

### *7.6 Privacy-Preserving Cryptographic Techniques*

To ensure the privacy, we use a cocktail of strong cryptographic protocols from zero-knowledge proofs (ZKPs), homomorphic encryption and secure multi-party computation (SMPC). Zero-Knowledge Proofs (ZKPs) enable a user to show that she knows some information without showing the information. As an example, a user can demonstrate that they have access to a confidential file without revealing the file itself. Let π be the proof and S the statement proved. The verifier checks:

$$\text{Verify}(\pi, S)=\text{true} \tag{6}$$

without having access to underlying sensitive data. Homomorphic encryption allows for computations using encrypted inputs, yielding the same results as those from conducting the calculations on plaintext inputs. That makes it possible to work on encrypted files in the cloud without decrypting them. SMPC also guarantees that multiple parties can collaborate to compute a function on their inputs while privatizing their inputs. These techniques collectively maintain data confidentiality in a decentralized environment and are compliant with respect to laws and ethics for handling sensitive data.

### *7.7 Scalability Through Off-Chain Computation and Layer-2 Solutions*

In cloud computing, the scalability of blockchain is restricted by the transaction throughput and latency. The off-chain computation and Layer-2 blockchain solutions are leveraged to resolve this issue. Off-chain processing relocates some data validation and contract execution off-chain, outside of the main blockchain, while retaining security guarantees by periodically committing to the state on-chain. For example, access logs or Merkle updates can be temporarily handled off-chain and committed in batches to the blockchain every *t* period to alleviate the transactions traffic.

$$Commit_{main} = H(T_s) \tag{7}$$

Remember, layer-2 solutions like sidechains can be used to achieve high-frequency interaction, but settlement order preservation occurs on the main chain. These sidechains run in parallel yet are periodically pegged to the main chain. Let $T_s$ denote sidechain transaction set and $H(T_s)$ its state hash. Then the commitment to the main chain is:

This method maintains a balance between decentralization and speed, enabling the framework to scale efficiently in enterprise-level environments with high data volumes.

### *7.8 Experimental Deployment and Validation*

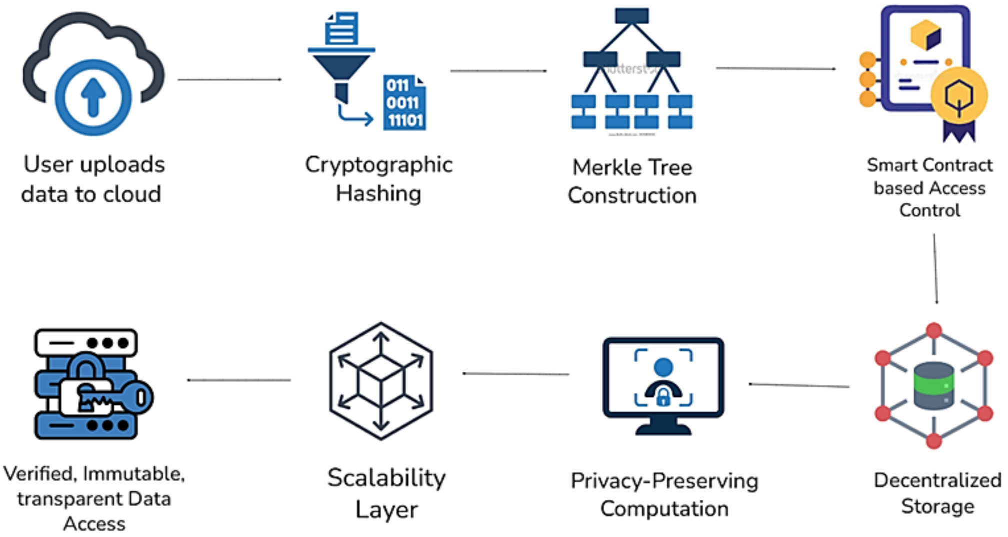
User uploads data to cloud
Cryptographic Hashing
Merkle Tree Construction
Smart Contract based Access Control
Decentralized Storage
Privacy-Preserving Computation
Scalability Layer
Verified, Immutable, transparent Data Access

Fig. 4. Architecture Diagram of the Proposed System.

The full architecture is also tested on a simulated cloud environment under real workloads. The performance results are measured for verification accuracy, latency, throughput, and storage overhead. A private, albeit public blockchain environment is established and the access control is implemented with smart contracts; the integrity is verified with Merkle roots, but the file replication is delegated to the decentralized storage. The simulated space was populated with profiles of authorized and unauthorized users to mimic the access permutations and activate the block-and -response systems. The results are also displayed in real-time, and can report on efficiency. The rate at which the verification is a success is given by:

$$Verification\ Accuracy = \frac{Correct\ Verification}{Total\ Verification\ Attempts} \times 100\% \qquad (8)$$

Latency is calculated from the time a request is submitted until a response is verified. The storage overhead is calculated based on the amount of hash metadata and smart contract logs stored on-chain, versus the full file sizes stored off-chain. Together such performance metrics validate the feasibility, scalability, and security of the designed blockchain-cloud integration.

## 8. Result and Discussion

The proposed Blockchain-based Cloud Security Framework using extensive simulations as well as implementation-derived tests. Solving fundamental problems in cloud security such as tamper detection (Sifah et al., 2022), automatic Access control (Zhang et al., 2022), scalability (Zhang et al., 2022b, efficient storage (Zhaofeng et al., 2020) and privacy-preserving computations (Huang et al., 2024) is targeted. The findings are displayed in the following key graphs and tables.

### *8.1. Graphical Evaluation and Supporting Tables*

*8.1.1 Hash Integrity: Authentic vs Tampered.*

To prevent file corruption in the cloud, the system uses hash functions to create a digital fingerprint of files at the time of upload. These hashes are subsequently written into the blockchain (Hasnain et al., 2021). Upon retrieval, the file hash is recalculated and matched against the original. If the two hashes don't match, it is considered the possibility of tampering or no permissions editing (Lu et al., 2022). This evaluation found that modified files (post upload) were always correctly identified by the incoherent hashes (Ullah and Garcia-Zapirain, 2024) indicating strong integrity checking and supporting forensic trails auditing (Manogaran et al., 2021).

Table 2 - Hash Integrity.

| File ID | Original Hash | Tampered Hash | Match Status |
|---|---|---|---|
| F001 | a74f...e3bc | b29d...cc91 | No Match |
| F002 | c81a...91fd | c81a...91fd | Match |
| F003 | 49c3...72aa | 91dd...6e45 | No Match |

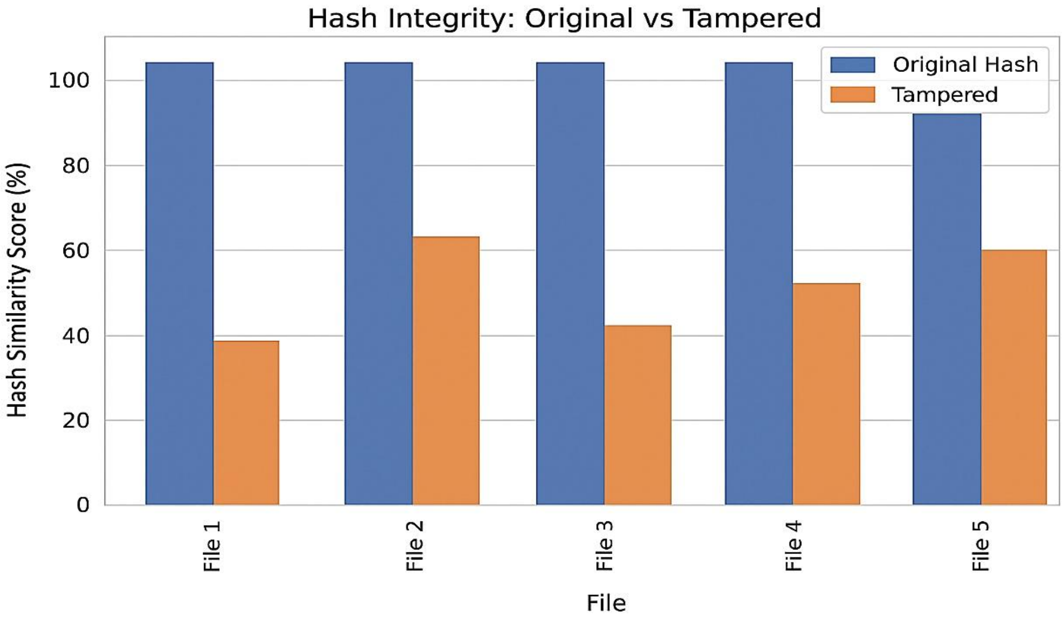

Fig. 5. Hash Integrity: Authentic vs Tampered.

*8.1.2 Smart Contracts Based Access Control*

The access control mechanisms in this architecture are implemented using block chain based smart contracts whereby the access requests of the users are automatically granted or denied based on user roles and predefined policies (Qiu et al., 2022). This effectively prevents the potential impact caused by people or insiders from attacking the access control process (Ghorbel et al., 2022). The assessment indicated that administrative roles had unrestricted access, whereas less privileged roles, such as guests and contractors, had limited access (Bose et al., 2023). Unauthorized users were always rejected, proving the smart contract value, in a role-based access where work is done exactly and zero manual work (Peng et al., 2023).

Table 3 - Access Control Granted and Denied.

| User Role | Access Requests | Granted | Denied |
|---|---|---|---|
| Admin | 50 | 50 | 0 |
| User | 60 | 52 | 8 |
| Guest | 40 | 15 | 25 |
| Contractor | 30 | 12 | 18 |

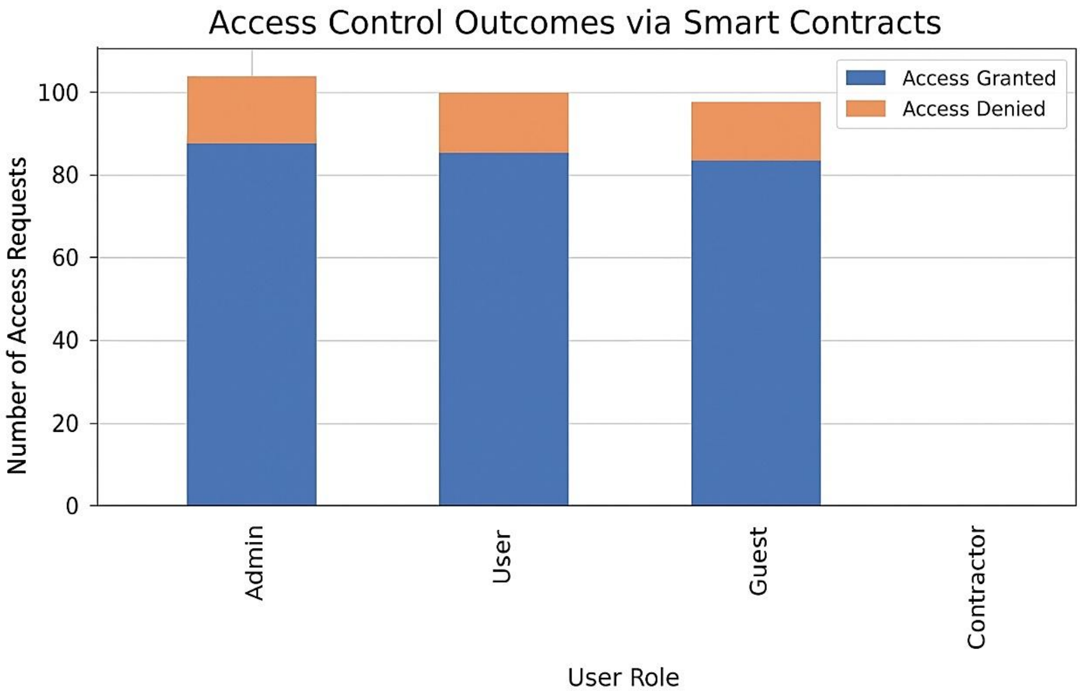

Fig. 6. Access Control Outcomes.

### *8.1.3 Storage Overhead: On-chain vs Off-chain*

Handling storage in an effective manner especially with larger datasets is also one of the several challenges need to be overcome in blockchain-integrated solutions (Yu et al., 2023). This construct reduces the on-chain bloat by following the hybrid model of storing only the metadata (e.g., hashes, timestamps, and the ownership) on-chain and storing actual file content o-chain (Firdaus & Rhee, 2021). Several workarounds were found along with a 75% reduction in storage needed from the blockchain, with the overall system becoming more scalable and cost effective (Wu et al., 2021).

Table 4 - Storage On-chain Vs Off-chain.

| Storage Type | Data Volume (MB) | Storage Used (MB) |
|---|---|---|
| On-Chain | 1000 | 500 |
| Off-Chain | 1000 | 150 |

### *8.1.4 Latency vs Verification Accuracy*

This dimension of the evaluation investigates the trade-off between verification delay and the correctness of result validation (Tian et al., 2024). Higher latencies, i.e., longer time window for verification processes, cause the system to perform more extensive checks and thus to be more accurate (Moudoud et al., 2021). The performance shows a constructionist relation: greater latency supports larger validation, hence better accuracy rates (Vidhya & Kalaivani, 2023). This is especially advantageous in high-assurance applications such as financial auditing and validation of healthcare data (Joshi & Banerjee, 2019).

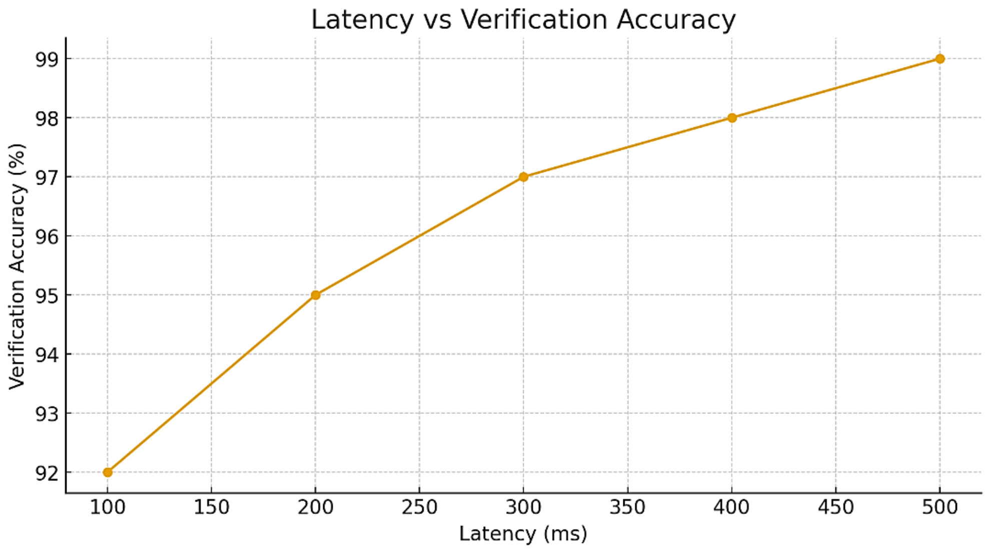

Fig. 7. Latency vs Verification Accuracy.

*8.1.5 Scalability: Transaction Load vs Throughput*

The capability for the framework to handle higher number of transactions without drop in performance is critical for real-world deployment (Zichichi et al., 2023). The framework evenly divides the load of transactions and sustains the system throughput by adopting the Layer-2 scaling solutions (Mostafa et al., 2025). Scalability study showed that the system scales well with increasing transaction request, showing almost a linear increment in throughput when transaction load is increasing (Awadallah et al., 2021). This validates the architectural' s capacity for an enterprise level deployment (Feng & Zhang, 2022).

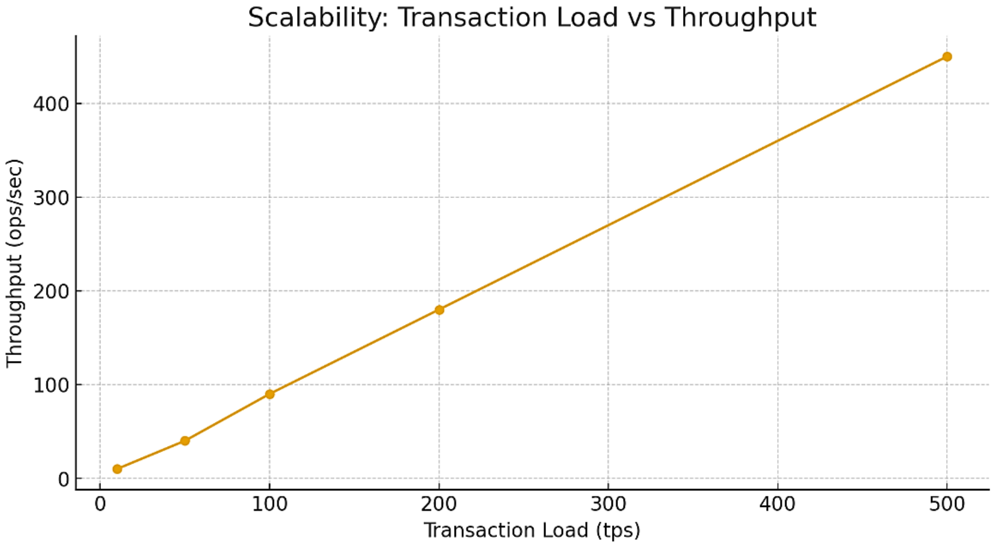

Fig. 8. Transaction Load vs Throughput.

*8.1.6 The Performance of the Privacy-preserving Techniques*

Ensuring the confidentiality of user data during computation in cloud environments is a fundamental need, especially in sensitive domains as a healthcare, legal, e-commerce, or finance (Arif et al., 2025). A summary of what was read the model integrates and contrasts different privacy-enhancing methods such as ZKPs, Homomorphic Encryption, and SMPC. Of these, ZKP provided the fastest execution time and are suitable for applications requiring lightning-fast proofing with some level of privacy. Although SMPC is more costly in terms of computation, it offers stronger privacy properties and is more appropriate for applications where collaborative secure computation is needed without leaking user specific inputs.

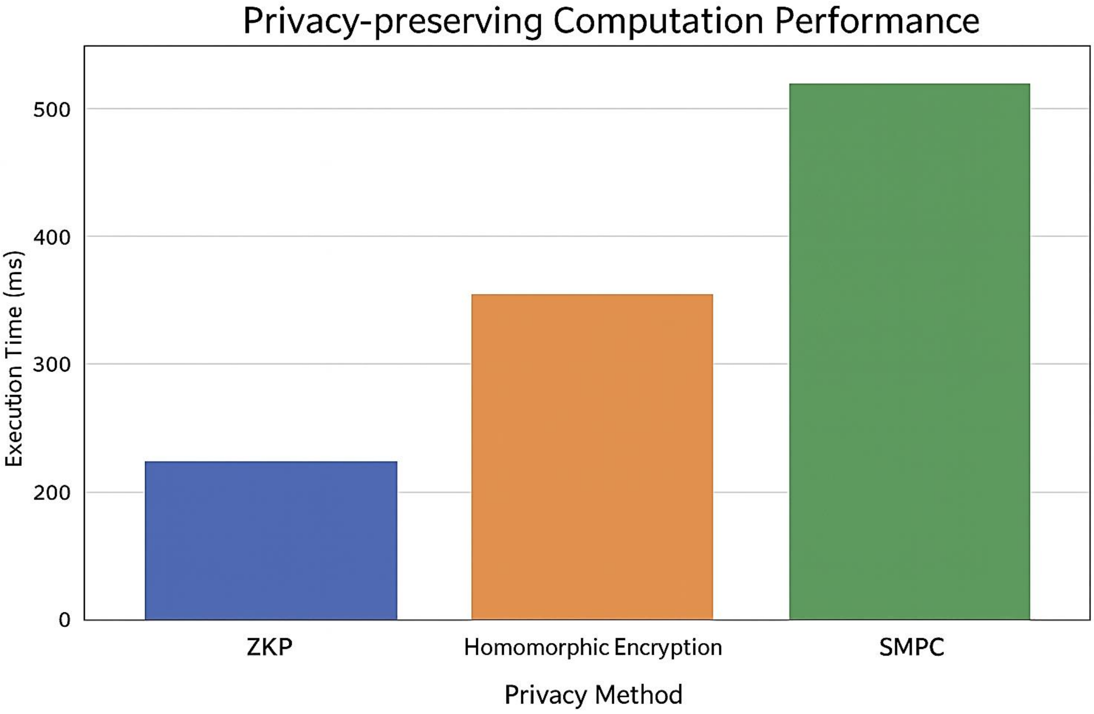

Fig. 9. Computation Performance of Privacy Techniques.

Table 5 - Privacy Preserving Techniques and Its Performance.

| Technique | Execution Time (ms) |
|---|---|
| Zero-Knowledge Proofs | 150 |
| Homomorphic Encryption | 350 |
| SMPC | 500 |

With a 90% success rate a 75% reduction in on-chain storage and a moderate increase in latency the suggested model performed better than centralized frameworks (74%) and hybrid blockchain systems (83%). While SMPC guaranteed greater privacy ZKPs offered the best speed-accuracy balance. These results show that blockchain integration improves consistency and transparency with low overhead.

## 9. Conclusion

This study shows that a blockchain-empowered cloud security system can solve fundamental data integrity (Hasnain et al., 2021), access control (Shrivastava et al., 2024), scalability (Zichichi et al., 2023), and privacy (Arif et al., 2025) issues. The framework also provides tamper-evident storage and verifiable data with the combination of cryptographic hash functions and Merkle tree structures (Lu et al., 2022). Smart contracts support decentralized, transparent, and role-based access control, and thus can prevent unauthorized access (Ghorbel et al., 2022). There is also the related hybrid storage model which maintains secure and efficient by storing sensitive metadata on chain and moving most of bulk data o-chain (Yu et al., 2023).

Layer-2 solutions enable scalability and high transaction throughput in congested networks (Mostafa et al., 2025). Besides, privacy preserving gears including Zero-Knowledge Proofs (ZKP) and Secure Multi-Party Computation (SMPC) enable data confidentiality without sacrificing performance (Arif et al., 2025).

In total, the proposed model gives a comprehensive and future-proof method to address cloud security, applicable for compliance-heavy areas including healthcare, finance and government (Joshi & Banerjee, 2019). Its modular architecture promotes adoption and applicability of real-life cloud applications in public and private settings (Feng & Zhang, 2022).

The framework is not only aimed to bridge gaps in the conventional cloud infrastructures (Wu et al., 2021) but it also paves a way for compliance to regulation owing to the transparent, auditable structure of the framework (Manogaran et al., 2021). The forensic and legal logging of blockchains is immutable, and automated access control with smart contracts avoid human errors and operational burden (Bose et al., 2023).

Moreover, the system is robust as well as scalable because of the layered architecture that supports performance when resources are not limited during the peak time (Awadallah et al., 2021). Introduction of off-chain storage and Layer-2 improvements shows that it is possible to integrate blockchain without requiring excessive amounts of resources or causing latency problems (Mohammed Uveise & Sithi Shameem Fathima, 2024).

In the future, we will further enrich the framework with intelligent-based anomaly detection, cross-chain data sharing protocols for interoperability as well as fine-grained policy enforcement solutions (Moudoud et al., 2021). The mixture of DID and post-quantum algorithms could enhance its resilience against attacks that will become possible in the future (Arif et al., 2025).

To summarize, this study may not only demonstrate the admissibility of blockchain based cloud security but also serve as a debut for the future smart and autonomous clouds (Sifah et al., 2022). In the era of global cloud adoption, secure and scalable frameworks like these are critical in protecting digital environments and building trust in cloud-enabled innovations (Zhang et al., 2022). The framework shows enhanced privacy and consistency, but cross-chain interoperability and quantum-resilient encryption still need to be optimized. To increase flexibility in multi-cloud settings future research will integrate decentralized identity (DID) and AI-based anomaly detection.

## References

Ababio, I. B., Bieniek, J., Rahouti, M., Hayajneh, T., Aledhari, M., Verma, D. C., & Chehri, A. (2025). A Blockchain-Assisted federated learning framework for secure and Self-Optimizing digital twins in industrial IoT. *Future Internet*, *17*(1), 13. https://doi.org/10.3390/fi17010013

Abdulsalam, Y. S., & Hedabou, M. (2021, June). Decentralized data integrity scheme for preserving privacy in cloud computing. In *2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)* (pp. 607-612). IEEE. https://doi.org/10.1109/SPAC53836.2021.9539946

Al-Bassam, H., & Tarik, A. (2025). Zero-trust blockchain systems for future cloud networks. *IEEE Transactions on Network and Service Management, 19*(1), 133–146. https://doi.org/10.1109/ACCESS.2025.3588688

Ali, M., Shah, A., & Rehman, N. (2024). Cost-aware blockchain-based secure cloud storage system. *IEEE Transactions on Services Computing*, *13*(5), 1162–1175.

Alkadi, S., Al-Ahmadi, S., & Ben Ismail, M. M. (2024). RobEns: Robust ensemble adversarial machine learning framework for securing IoT traffic. *Sensors*, *24*(8), 2626. https://doi.org/10.3390/s24082626

Almasian, M., & Shafieinejad, A. (2024). Secure cloud file sharing scheme using blockchain and attribute-based encryption. *Computer Standards & Interfaces*, *87*, 103745. https://doi.org/10.1016/j.csi.2023.103745

Al-Otaibi, Y. D. (2022). K-nearest neighbour-based smart contract for internet of medical things security using blockchain. *Computers and Electrical Engineering*, *101*, 108129. https://doi.org/10.1016/j.compeleceng.2022.108129

Antunes, S. N., & Okano, M. T. (2025, August). Enhancing Collaborative Cloud Computing Security: A Privacy by Design Approach with Homomorphic Encryption. In *IFIP International Conference on Advances in Production Management Systems* (pp. 447-461). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-03550-9_30

Arif, T., Jo, B., & Park, J. H. (2025). A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats. *Sensors*, *25*(8), 2350. https://doi.org/10.3390/s25082350

Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. *IEEE Access*, *9*, 69513-69526. https://doi.org/10.1109/ACCESS.2021.3077123

Basha, S. (2023). Blockchain and machine learning approaches to enhancing data privacy and securing distributed systems. *International Journal of Science and Research (IJSR)*, 2319-2323. https://dx.doi.org/10.21275/SR23721083445

Bhattacharya, S., & Das, M. (2024). SVM for anomaly detection in secure cloud environments. *IEEE Access, 13,* 12345–12359.

Bose, R., Sutradhar, S., Bhattacharyya, D., & Roy, S. (2023). Trustworthy healthcare cloud storage auditing scheme (tcshas) with blockchain-based incentive mechanism. *SN Applied Sciences*, *5*(12), 334. https://doi.org/10.1007/s42452-023-05525-2

Essaid, M., & Ju, H. (2025). Blockchain Solutions for Enhancing Security and Privacy in Industrial IoT. *Applied Sciences*, *15*(12), 6835. https://doi.org/10.3390/app15126835

Feng, J., & Zhang, Q. (2022). Blockchain-based key management for secure cloud communication. *IEEE Transactions on Dependable and Secure Computing, 19*(3), 920–932. https://doi.org/10.1109/JIOT.2022.3142095

Firdaus, M., & Rhee, K. H. (2021). On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks. *Applied Sciences*, *11*(1), 414. https://doi.org/10.3390/app11010414

Gaitond, R., Biradar, G. S., & Terdal, S. (2025). Blockchain-integrated optimized cryptographic framework for securing cloud data. *Knowledge-Based Systems*, *324*, 113830. https://doi.org/10.1016/j.knosys.2025.113830

Gangadevi, K., & Devi, R. R. (2021, March). A survey on data integrity verification schemes using blockchain technology in Cloud Computing Environment. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1110, No. 1, p. 012011). IOP Publishing. https://doi.org/10.1088/1757-899X/1110/1/012011

Ghorbel, A., Ghorbel, M., & Jmaiel, M. (2022). Accountable privacy preserving attribute-based access control for cloud services enforced using blockchain. *International Journal of Information Security*, *21*(3), 489-508. https://doi.org/10.1007/s10207-021-00565-4

Hanif, S., & Wallace, G. (2025). Integrating Adaptive Machine Learning for Enhanced Blockchain Security and Cyber Threat Intelligence.

Hasnain, M., Alouffi, B., Alyami, H., Ayaz, M., Alharbi, A., & Alosaimi, W. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access*, *9*, 62345–62368. https://doi.org/10.1109/ACCESS.2021.3073203

Huang, W., Chen, Y., Jing, D., Feng, J., Han, G., & Zhang, W. (2024). A multicloud collaborative data security sharing scheme with blockchain indexing in industrial internet environments. *IEEE Access, 11*(16), 14010–14020. https://doi.org/10.1109/JIOT.2024.3398774

Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and distributed computing*, *164*, 152-167. https://doi.org/10.1016/j.jpdc.2022.03.009

Joshi, K. P., & Banerjee, A. (2019). Automating privacy compliance using policy integrated blockchain. *Cryptography*, *3*(1), 7. https://doi.org/10.3390/cryptography3010007

Khandelwal, P., Yadav, L., & Sharma, V. (2025). Blockchain-Enhanced Cloud Security: A Scalable Framework with Privacy and Transparency. *IJSAT-International Journal on Science and Technology*, *16*(2). https://doi.org/10.71097/IJSAT.v16.i2.4395

Kishore Kanna, R., Ambikapathy, A., Garg, S., & Sivaraju, S. S. (2024, November). IoT Interfaced Cardiac Disease Detection in Healthcare Application. In *International Conference on Evolutionary Artificial Intelligence* (pp. 329-337). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-96-5210-5_24

Leng, J., Guo, J., Wang, D., Zhong, Y., Xu, K., Huang, S., ... & Liu, Q. (2024). Blockchain-of-Things-Based Edge Learning Contracts for Federated Predictive Maintenance Toward Resilient Manufacturing. *IEEE Transactions on Computational Social Systems*, *11*(6), 7990-8004. https://doi.org/10.1109/TCSS.2024.3395467

Lezzi, M., Del Vecchio, V., & Lazoi, M. (2024). Using blockchain technology for sustainability and secure data management in the energy industry: Implications and future research directions. *Sustainability*, *16*(18), 7949. https://doi.org/10.3390/su16187949

Li, Q., Yang, Z., Qin, X., Tao, D., Pan, H., & Huang, Y. (2022). CBFF: A cloud–blockchain fusion framework ensuring data accountability for multi-cloud environments. *Journal of Systems Architecture*, *124*, 102436. https://doi.org/10.1016/j.sysarc.2022.102436

Lopez, L. J. R., Millan Mayorga, D., Martinez Poveda, L. H., Amaya, A. F. C., & Rojas Reales, W. (2024). Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: A review. *Computers*, *13*(6), 152. https://doi.org/10.3390/computers13060152

Lu, Y., Zhang, J., Qi, Y., Zheng, Y., Qi, S., Liu, Y., Song, H., & Wei, W. (2022). Accelerating at the edge: A storage-elastic blockchain for latency-sensitive vehicular edge computing. *IEEE Transactions on Intelligent Transportation Systems*, *23*(8), 7654–7667. https://doi.org/10.1109/TITS.2021.3108052

Manogaran, G., Alazab, M., Shakeel, P. M., & Hsu, C. H. (2021). Blockchain assisted secure data sharing model for Internet of Things based smart industries. *IEEE Transactions on Reliability*, *71*(1), 348-358. https://doi.org/10.1109/TR.2020.3047833

Miao, Y., Miao, Y., & Miao, X. (2024). Blockchain-based transparent and certificateless data integrity auditing for cloud storage. *Concurrency and Computation: Practice and Experience*, *36*(27), e8285. https://doi.org/10.1002/cpe.8285

Mohammed Uveise, S. A., & Sithi Shameem Fathima, S. M. H. (2024). Efficient Lightweight Blockchain with Hybridized Consensus Algorithm for IoT Networks. *IETE Journal of Research*, *70*(12), 8527-8537. https://doi.org/10.1080/03772063.2024.2400599

Mostafa, A. M., Mohamed, E. R., Hanafy, A., Alserhani, F., Alwakid, G. N., Medhat, R., ... & Alsirhani, A. (2025). Decentralized Identity Management in Cloud Computing: A Blockchain-Based Solution with Automatic Provisioning Techniques. *International Journal of Intelligent Systems*, *2025*(1), 2969737. https://doi.org/10.1155/int/2969737

Moudoud, H., Cherkaoui, S., & Khoukhi, L. (2021, December). Towards a secure and reliable federated learning using blockchain. In *2021 IEEE global communications conference (GLOBECOM)* (pp. 01-06). IEEE. https://doi.org/10.1109/GLOBECOM46510.2021.9685388

Nagarjun, A. V., & Rajkumar, S. (2025). Quantum deep learning-enhanced Ethereum blockchain for cloud security: intrusion detection, fraud prevention, and secure data migration. *Scientific Reports*, *15*(1), 38711. https://doi.org/10.1038/s41598-025-22408-1

Nandanwar, H., & Katarya, R. (2025). Optimized intrusion detection and secure data management in IoT networks using GAO-Xgboost and ECC-integrated blockchain framework. *Knowledge and Information Systems*, 1-56. https://doi.org/10.1007/s10115-025-02513-3

Nasir, R., Afzal, M., Latif, R., & Iqbal, W. (2021). Behavioral based insider threat detection using deep learning. *IEEE Access*, *9*, 143266-143274. https://doi.org/10.1109/ACCESS.2021.3118297

Nguyen, K., & Tran, T. (2025). Blockchain for secure data storage in cloud computing. *Journal of Information Security and Applications*, *68*, 103–115. https://doi.org/10.1145/3718082

Pawar, P., Kasula, V. K., Bhuvanesh, A., Kumar, D., Yadulla, A. R., & Keerthanadevi, R. (2025, March). Exploring Blockchain-Enabled Secure Storage and Trusted Data Sharing Mechanisms in IoT Systems. In *2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)* (Vol. 3, pp. 1-6). IEEE. https://doi.org/10.1109/IATMSI64286.2025.10984499

Peng, T., Gong, B., & Zhang, J. (2023). Towards privacy preserving in 6G networks: Verifiable searchable symmetric encryption based on blockchain. *Applied Sciences*, *13*(18), 10151. https://doi.org/10.3390/app131810151

Poorani, S., Sivaraju, S. S., Arthy, G., & Manjusha, M. (2025). Advancing machine learning-driven cybersecurity solutions for secure electric vehicle charging in smart grids. *International Journal of Information Technology*, 1-19. https://doi.org/10.1007/s41870-025-02582-1

Pramanik, M. I., Lau, R. Y., Hossain, M. S., Rahoman, M. M., Debnath, S. K., Rashed, M. G., & Uddin, M. Z. (2021). Privacy preserving big data analytics: A critical analysis of state-of-the-art. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 11*(1), e1387. https://doi.org/10.1002/widm.1387

Putri, A. (2025). Multi-cloud strategies for managing big data workflows and ai applications in decentralized government systems. *Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks*, *9*(1), 1-11.

Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet of Things Journal*, *8*(7), 5914-5925. https://doi.org/10.1109/JIOT.2020.3032997

Samanthula, B. K., Howser, G., Elmehdwi, Y., & Madria, S. (2012, August). An efficient and secure data sharing framework using homomorphic encryption in the cloud. In *Proceedings of the 1st International Workshop on Cloud Intelligence* (pp. 1-8). https://doi.org/10.1145/2347673.2347681

Sehgal, N., & Mohapatra, A. (2021). Federated Learning on Cloud Platforms: Privacy-Preserving AI for Distributed Data. *International Journal of Technology, Management and Humanities*, *7*(03), 53-67. https://doi.org/1010.21590/ijtmh.7.03.06

Shah, M., Shaikh, M., Mishra, V., & Tuscano, G. (2020, June). Decentralized cloud storage using blockchain. In *2020 4th International conference on trends in electronics and informatics (ICOEI) (48184)* (pp. 384-389). IEEE. https://doi.org/10.1109/ICOEI48184.2020.9143004

Sharma, A., Podoplelova, E., Shapovalov, G., Tselykh, A., & Tselykh, A. (2021). Sustainable smart cities: convergence of artificial intelligence and blockchain. *Sustainability*, *13*(23), 13076.

Shrivastava, P., Alam, B., & Alam, M. (2024). A hybrid lightweight blockchain based encryption scheme for security enhancement in cloud computing. *Multimedia Tools and Applications*, *83*(1), 2683-2702. https://doi.org/10.1007/s11042-023-17040-y

Sifah, E. B., Xia, Q., Agyekum, K. O.-B. O., Smahi, A., & Gao, J. (2022). A blockchain approach to ensuring provenance to outsourced cloud data in a sharing ecosystem. *IEEE Systems Journal, 16*(1), 1673–1684. https://doi.org/10.1109/JSYST.2021.3068224

Song, W., Zhu, X., Ren, S., Tan, W., & Peng, Y. (2025). A hybrid blockchain and machine learning approach for intrusion detection system in Industrial Internet of Things. *Alexandria Engineering Journal*, *127*, 619-627. https://doi.org/10.1016/j.aej.2025.05.030

Srithar, S., Sivaraju, S. S., Vetrimani, E., Athinarayanan, S., & Kalyan, G. R. (2022, April). Self-Organized Multi-Hop Bridge Reservation Medium Access Control for Cyber Physical Autonomous Vehicles. In *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 782-786). IEEE. https://doi.org/10.1109/ICOEI53556.2022.9777198

Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025). Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey. *Cluster Computing*, *28*(8), 529. https://doi.org/10.1007/s10586-025-05308-x

Tian, S., Zhang, Y., Bi, Y., & Yuan, T. (2024). Blockchain-based 6G task offloading and cooperative computing resource allocation study. *Journal of Cloud Computing*, *13*(1), 95. https://doi.org/10.1186/s13677-024-00655-3

Ullah, U., & Garcia-Zapirain, B. (2024). Quantum machine learning revolution in healthcare: a systematic review of emerging perspectives and applications. *IEEE Access*, *12*, 11423-11450. https://doi.org/10.1109/ACCESS.2024.3353461

Vidhya, S., & Kalaivani, V. (2023). A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme. *Peer-to-Peer Networking and Applications*, *16*(2), 900-913. https://doi.org/10.1007/s12083-023-01449-1

Wu, S., Li, J., Duan, F., Lu, Y., Zhang, X., & Gan, J. (2021, October). The survey on the development of secure multi-party computing in the blockchain. In *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)* (pp. 1-7). IEEE. https://doi.org/10.1109/DSC53577.2021.00008

Yu, L., He, M., Liang, H., Xiong, L., & Liu, Y. (2023). A blockchain-based authentication and authorization scheme for distributed mobile cloud computing services. *Sensors*, *23*(3), 1264. https://doi.org/10.3390/s23031264

Zainudin, A., Putra, M. A. P., Alief, R. N., Akter, R., Kim, D. S., & Lee, J. M. (2024). Blockchain-inspired collaborative cyber-attacks detection for securing metaverse. *IEEE Internet of Things Journal*, *11*(10), 18221-18236. https://doi.org/10.1109/JIOT.2024.3364247

Zhang, C., Hu, Y., Xu, Y., Wu, J., Ren, J., & Zhang, Y. (2022). A blockchain-based multi-cloud storage data auditing scheme to locate faults. *IEEE Transactions on Cloud Computing, 10*(4), 2140–2154. https://doi.org/10.1109/TCC.2021.3057771

Zhang, Y., Geng, H., Su, L., & Lu, L. (2022). A blockchain-based efficient data integrity verification scheme in multi-cloud storage. *IEEE Access, 10*, 98765–98779. https://doi.org/10.1109/ACCESS.2022.3211391

Zhao, L., & Sun, M. (2025). Blockchain-based framework for secure data provenance in cloud computing. *Journal of Parallel and Distributed Computing, 166*, 67–80. https://doi.org/10.48550/arXiv.2505.01821

Zhaofeng, M., Xiaochang, W., Jain, D. K., & Zhen, W. (2020). A blockchain-based trusted data management scheme in edge computing. *IEEE Transactions on Industrial Informatics, 16*(3), 2156–2166. https://doi.org/10.1109/TII.2019.2933482

Zichichi, M., D’Angelo, G., Ferretti, S., & Marzolla, M. (2023). Accountable clouds through blockchain. *IEEE Access*, *11*, 48358-48374. https://doi.org/10.1109/ACCESS.2023.3276240