Journal of Industrial Information Technology and Application *ISSN(Online): 2586-0852*
Vol.10 No. 1

Enhancing Cloud Data Security Through Blockchain Integration: A Secure And Transparent Framework

K. Ramy and R. Anandhi

Dept of Computer Science, Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, India

Abstract. come an essential technology for today's data storage and service offerings. However, concerns regarding security, privacy, integrity, and transparency have created barriers for widespread acceptance of cloud computing as a viable option. The traditional mechanisms of securing a cloud service rely heavily on centralised solutions; consequently, these security mechanisms are more susceptible to cyber-attacks, unauthorised users, and limited ability to audit activity within the cloud. This study will look at how integrating blockchain technology with cloud computing may complement the traditional models of securing clouds, and that by using blockchain technology, it provides a highly secure method for increasing security in a cloud environment

Keywords; Blockchain technology; Cloud computing security; Smart contracts; Data integrity; Decentralized systems

Cite this paper as : Soumya Yattinahalli, Vijaya Ramineni, Ramya M S, and Dr Prakash Kuppuswamy (2026) "A Temporal and Explainable Machine Learning Framework for Probabilistic and Extreme Rainfall Prediction", Journal of Industrial Information Technology and Application, Vol. 10. No. 1, pp.1275-1295

* Corresponding author: ramya.dgvc2024@gmail.com
Received: Jan.13. 2026 Accepted: Feb. 5. 2026 Published: Mar. 31. 2026

1. Introduction

A. Cloud Computing

Cloud computing enables users to access data and applications over the internet, eliminating the need for local servers or personal computing resources. It provides flexible, on-demand scalability, allowing users to leverage computing power, storage, and software as needed.

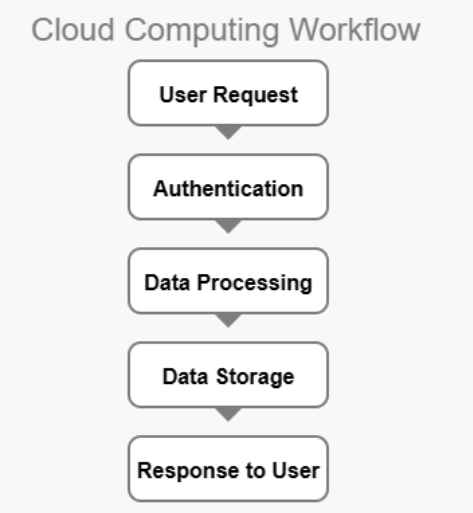

Figure 1. Workflow of Cloud Computing

Figure 1. represents the workflow in cloud computing that involves five key steps:

- Initiation of the user request
- Authentication of the initiated request
- Processing of the submitted request
- Accessing of the data storage for preparing response
- The response is sent back to the user

A typical cloud architecture comprises three components: a back-end platform (servers or storage), a front-end platform (clients or mobile devices), and the network

(intranet or internet) that connects them. Given the exponential growth of data, researchers have been focusing on addressing the complexities of data storage, security, and usability in cloud systems.

B. Service Models

"Cloud services" refers to a wide range of on-demand services delivered over the internet to companies and customers. Cloud service models refer to different categories of cloud computing services that provide varying levels of control and management.

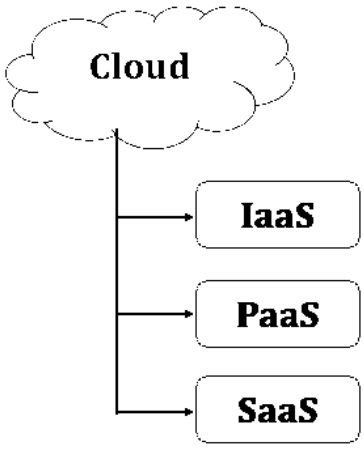

Figure 2. Services of Cloud Computing

Figure 2. refers a simpler version of the cloud computing services, with a minimal design connecting IaaS, PaaS, and SaaS to the central cloud.

- **Infrastructure as a Service (IaaS)**: It offers basic computing infrastructure for the required users. The infrastructure may be virtual machines, storage, networking etc. Users are responsible for managing the operating systems, applications, and data. **Examples**: Amazon Web Services (AWS)

- **Platform as a Service (PaaS)**: It offers a platform allowing the developers to build, test, and deploy applications without worrying about underlying platform. **Example**: Google App Engine

- **Software as a Service (SaaS)**: It offers access to software applications over the internet. The provider manages everything from the infrastructure to the software. **Examples**: Salesforce, Gmail, Microsoft Office 365.

The increasing reliance on mobile apps for storing sensitive information such as personal identification data, financial details, and medical records has made data security a crucial concern. Securing stored data involves protecting them from the unauthorized access, disclosure, modification, or destruction. Furthermore, ensuring the safe storage and protection of such sensitive information is of utmost importance. This paper aims to explore the challenges and limitations associated with implementing blockchain technology to enhance the security of data storage in Android mobile applications.

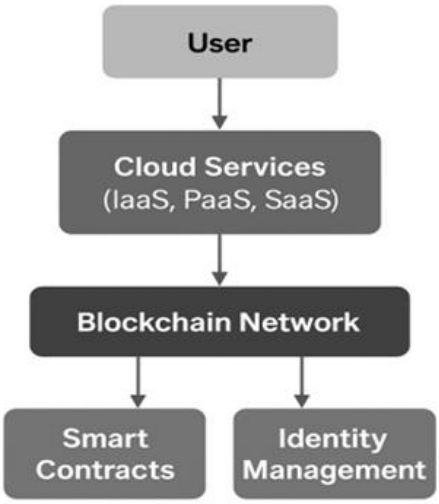

Figure 3. Blockchain Cloud Architecture

Figure 3. presents a layered model integrating blockchain technology with cloud services. At the top, the User layer represents end-users initiating service requests. These requests flow into the Cloud Services layer, which includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Beneath this lies the Blockchain Network layer, which ensures secure and decentralized processing. This layer connects to two essential modules: Smart Contracts, which execute automated agreements, and Identity Management, which verifies user credentials and access rights. Arrows between the components indicate the logical flow of data and control across

layers, illustrating a trust-enhanced cloud computing environment powered by blockchain.

C. Blockchain Technology

Blockchain technology provides the distributed ledger for storing the data or transactions that has the power to completely transform a wide range of businesses. It is a tamper-proof, transparent, and secure method of storing data. Blockchain is built on a computer network that shares a transaction ledger and authenticates each transaction before adding it to the ledger. This makes it very difficult to hack or corrupt the data stored on a blockchain.

Blockchain has become one of the most talked-about innovations, gaining prominence as a versatile technology applied in numerous fields. Since its inception, blockchain has developed into a groundbreaking technology with the potential to revolutionize how we interact, process digital payments, and track transactions. One of its key advantages is the ability to reduce costs by removing the need for a centralized authority to oversee and regulate exchanges between the participants. Each transaction is cryptographically secured and verified by other entities, ensuring that records remain tamper-proof, synchronized, and shared in real time. Additionally, blockchain technology is recognized for its wide applicability in software development, business, and trade sectors.

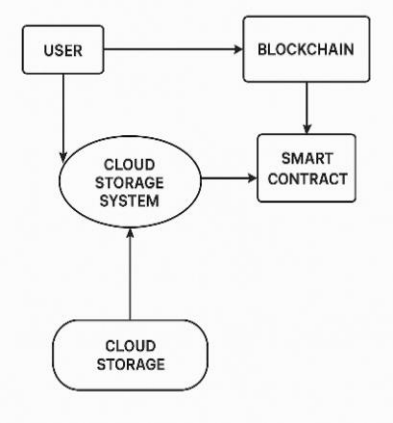

Figure 4. Data Flow Diagram

Figure 4. represents The Data Flow Diagram (DFD) of the Blockchain-Enabled Cloud Storage System illustrates how user data is securely managed through the

integration of blockchain and cloud technologies. In this system, the user initiates data operations that are first verified and recorded on the blockchain to ensure integrity and transparency. The blockchain interacts with smart contracts, which automate access control and data-sharing policies. Simultaneously, the user's data is directed to a cloud storage system for actual storage. The cloud storage system retrieves or stores the data based on the logic dictated by smart contracts, ensuring that all data transactions are traceable, tamper-proof, and comply with predefined rules.

2. Features Of Blockchain Technology

Blockchain technology offers several key features that make it a powerful and secure platform for data management and transactions. Some of the main features shown in Figure 3. are explained as below:

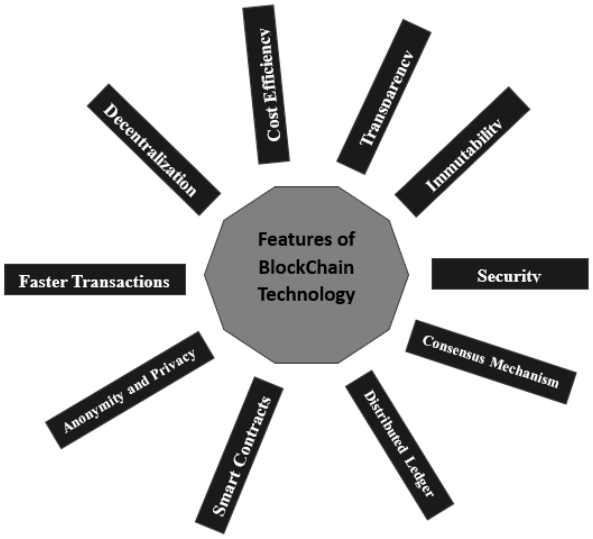

Figure 5. Features of Blockchain Techno

- **Decentralization:** Unlike traditional systems that rely on a central authority, blockchain operates on a decentralized network of computers (nodes). Each node has a copy of the entire blockchain, reducing dependency on a single point of control or failure.

- **Transparency:** All participants in the blockchain network have access to the same data, ensuring full transparency. Every transaction is recorded on the ledger and can be viewed by anyone with access to the network, although the identities of participants can remain anonymous.
- **Immutability:** Once a transaction is recorded on the blockchain, it cannot be modified or removed, which guarantees the integrity of the data. Blockchain operates using a consensus mechanism to validate transactions.
- **Security:** Blockchain employs cryptographic algorithms to safeguard transactions and maintain data integrity. Its decentralized structure...
- **Consensus Mechanism:** Transactions on the blockchain are validated through a consensus mechanism. Popular methods include Proof of Work (PoW) and Proof of Stake (PoS), where multiple nodes in the network agree on the validity of transactions before they are added to the ledger.

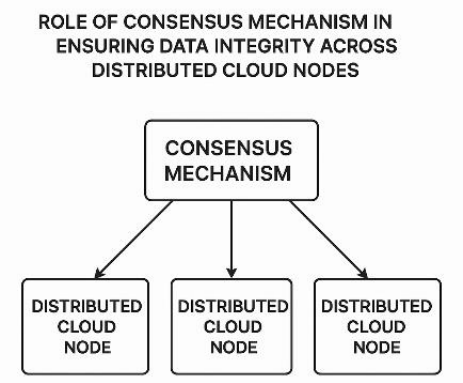

Figure 6. Role of Consensus Mechanism

Figure 6. illustrates how a blockchain-based system maintains data consistency and trust across a decentralized cloud environment. At the center of the diagram is the Consensus Mechanism, which acts as the coordinating entity responsible for validating transactions and updates before they are accepted into the shared ledger. This mechanism—whether it is Proof of Work (PoW), Proof of Stake (PoS), or any other consensus protocol—ensures that all participating nodes in the network agree on the current state of the data. Connected to the consensus mechanism are multiple Distributed Cloud Nodes, each representing an independent storage or compute unit in the cloud

infrastructure. Arrows from the consensus mechanism to each cloud node signify that data is only synchronized or updated across the nodes after achieving consensus, preventing conflicts, unauthorized tampering, and inconsistencies. This approach guarantees that all nodes reflect the same verified state of data, thereby reinforcing trust, fault tolerance, and security in distributed cloud storage environments powered by blockchain technology.

- **Distributed Ledger:** Blockchain is a type of distributed ledger where all participants hold a synchronized copy of the data eliminating the need for intermediaries and ensures consistency across all copies of the ledger.
- **Smart Contracts:** Blockchain supports programmable contracts, known as smart contracts, which automatically execute predefined actions when certain conditions are met. This feature allows for automation in processes like payments, transfers, and legal agreements.
- **Anonymity and Privacy:** While blockchain offers transparency, it also guarantees privacy. Participants can operate under pseudonyms or public keys, maintaining a certain level of anonymity while still ensuring the integrity of the transaction process.
- **Faster Transactions:** Compared to the traditional financial systems, blockchain technology can facilitate faster transactions by removing intermediaries, paper work, and operating 24/7. This can reduce the time for cross-border payments or business agreements.
- **Cost Efficiency:** By eliminating intermediaries and central authorities, blockchain can reduce transaction fees and operational costs, making processes more efficient for business operations.

3. Cloud Computing Meets Blockchain Mechnology

The combination of blockchain technology and cloud computing offers a promising way to improve the functionality, reliability, and security of cloud services. By using blockchain's decentralized, transparent, and tamper-proof structure, this approach aims to tackle some long-standing issues in cloud environments, especially concerning data security, privacy, and operational efficiency. Traditional cloud computing models depend heavily on centralized systems, which, while effective, create vulnerabilities like single points of failure, possible data breaches, and limited user control over data. In contrast, blockchain provides a distributed ledger system where data is stored in unchangeable blocks. This means that once information is saved, it cannot be altered or deleted without agreement from the network participants. This feature greatly improves data integrity and trust. Additionally, smart contracts—self-executing contracts with the terms written directly in code—add a level of automation and enforceability to cloud operations. Smart contracts can manage access controls, automate service-level

agreements (SLAs), and allow secure transactions between users and service providers without needing middlemen. Overall, merging blockchain and cloud computing could reshape cloud infrastructure by making it more secure, transparent, and focused on users, while also enhancing efficiency and resilience in service delivery.

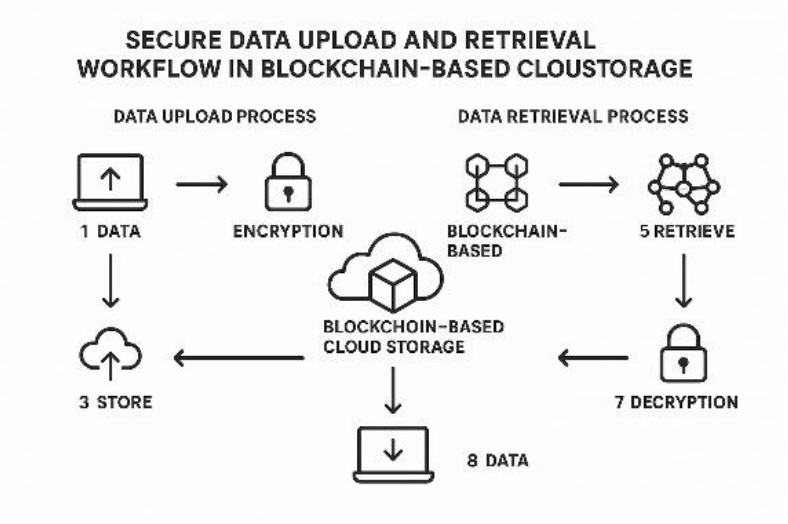

Figure 7. Secure Data Upload and Retrieval Workflow in Blockchain-Based Cloud Storage

Figure 7. illustrates the step-by-step process of securely managing data using blockchain-integrated cloud services. The Data Upload Process starts with the user uploading data, which is then encrypted to ensure confidentiality. The encrypted data is stored in a Blockchain-Based Cloud Storage system, ensuring tamper-proof logging and integrity. In the Data Retrieval Process, a blockchain-based mechanism verifies the request, and the encrypted data is retrieved securely. The data is then decrypted and delivered back to the user. This workflow ensures both security and trust through encryption and blockchain-backed storage and access control.

3.1. Data Security and Privacy

It enhances data integrity by ensuring cloud data storage into a secured, tamper-proof and immutable ledger, making it more difficult for hackers to manipulate or steal data stored in the cloud. Additionally, cloud platforms integrated with blockchain can utilize smart contracts can program to enforce access control policies, allowing for more granular control over who can access specific data.

3.2. Decentralized Cloud Data

It can enable decentralized cloud storage systems through distributed file systems, where data is stored across multiple nodes. This reduces the user's reliance on centralized servers, enhancing both security and availability. Additionally, by leveraging a peer-to-peer storage network, the costs typically associated with traditional cloud storage may be lowered.

3.3. Supply Chain Management

Cloud platforms integrated with blockchain can facilitate real-time data sharing across the supply chain, ensuring transparency and traceability of products from production to delivery. Additionally, blockchain's immutable ledgers improve tracking and auditing of assets within the supply chain, reducing fraud and enhancing trust among stakeholders.

3.4. Smart Contracts

It can automate service-level agreements (SLAs) between cloud providers and clients, ensuring that if the conditions are fulfilled, the services can be delivered as agreed and then only the payments are processed. Additionally, cloud services integrated with blockchain can streamline business process automation by handling tasks such as invoicing, payments, and service delivery across various domains.

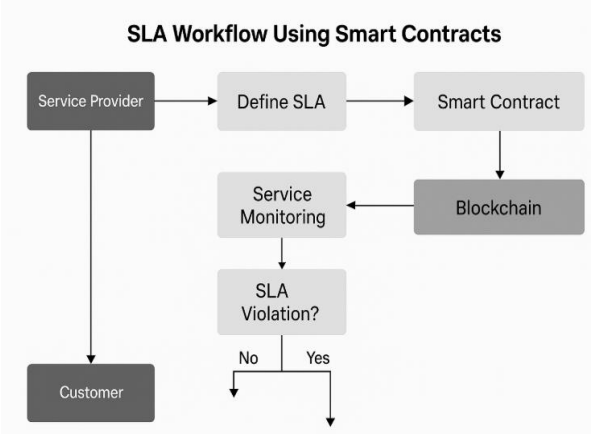

Figure 8. SLA Workflow diagram for Smart Contract

Figure 8. visually represents the process of enforcing a Service Level Agreement through blockchain technology. It begins with the Service Provider defining the SLA terms, which are codified into a Smart Contract and recorded immutably on the

Blockchain. The workflow then incorporates Service Monitoring, continuously checking compliance with the SLA. If a violation is detected, the system triggers predefined actions as per the smart contract, ensuring transparency, automation, and trust between the Service Provider and the Customer, eliminating the need for manual intervention or intermediaries.

3.5. Healthcare

This service ensures the secure sharing of sensitive patient data across healthcare providers, maintaining privacy and compliance with regulations. Moreover, healthcare records stored on blockchain-enabled cloud platforms become tamper-proof, guaranteeing that medical histories remain accurate and unchangeable. They also can speed up the insurance process as the patient history can be taken from the blockchain ledger.

3.6. Government and Public Services

Blockchain-based identity management systems hosted in the cloud can provide secure and verifiable identity services for government use cases such as voting, tax filing, and social services. Additionally, governments can utilize blockchain to store public records in a transparent and immutable way, enhancing trust and reducing corruption.

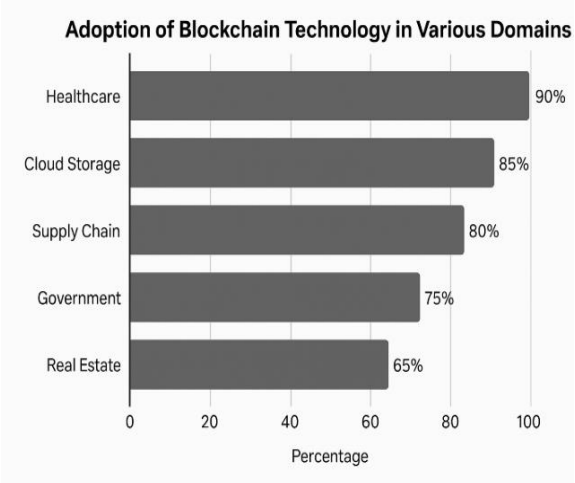

Figure 9. Adoption of Blockchain Technology in various Domains

Figure 9. shows highest blockchain adoption in Healthcare (90%), followed by Cloud Storage (85%) and Supply Chain (80%). Real Estate has the lowest adoption at 65%, indicating room for further growth in this sector.

4. Challenges In Blockchain Technology

4.1. Low Scalability and Performance

Because of the inherently decentralized nature of the blockchain, it is not capable of handling as large a load of concurrent transactions compared to traditional databases. One challenge is low throughput in transactions: blockchains like Bitcoin and Ethereum process fewer transactions per second compared to centralized systems. There is also high energy consumption due to consensus mechanisms like Proof of Work. Solutions being explored including Layer 2 technologies, such as the Lightning Network, sharding, and alternative consensus mechanisms like Proof of Stake.

4.2. Security Vulnerabilities

Although blockchain is often seen as a secure and reliable technology because of its use of strong cryptographic methods and decentralized structure, it still has security vulnerabilities. Several well-known threats reveal the limits and risks linked to blockchain systems.

One major threat is the 51% attack. In this scenario, a single person or a group of miners takes control of more than half of the network's computing power. With this power, the attacker can change the blockchain, reverse transactions, stop new transactions from being confirmed, and possibly double-spend digital assets; this undermines the trust and integrity of the system.

Another serious threat is the Sybil attack. Here, an attacker creates multiple fake identities or nodes to gain excessive influence over the network. This can disrupt consensus processes, manipulate voting systems, and even cause denial-of-service (DoS) attacks in peer-to-peer networks.

Additionally, smart contracts provide automation and transparency but also bring unique security risks. Badly written or unverified smart contracts can have bugs and vulnerabilities that malicious actors can exploit. A well-known example is the DAO hack on the Ethereum network. Flaws in the contract's code were taken advantage of, resulting in a loss of about $60 million worth of Ether. This incident showed that, even with

blockchain's security features, weaknesses in application-layer code can lead to serious issues. [14].

4.3. Regulatory and Legal Challenges

Blockchain faces challenges because its decentralized nature doesn't fit well with traditional regulations. There's often confusion about how cryptocurrencies, ICOs, and other blockchain applications should be regulated legally. Different countries have their own rules, making it hard for businesses to know which laws to follow and hence lack standardization.

Table 1. Key Challenges in Blockchain–Cloud Integration and Mitigation Strategies

Challenge	Mitigation Strategy
Scalability	Layer 2, PoS, Sharding
Security	Formal Verification, PBFT
Legal/Regulatory	ZKP, GDPR-compatible Solutions
Interoperability	Cross-chain bridges, Polkadot, Cosmos
User Adoption	UI simplification, Education Campaigns

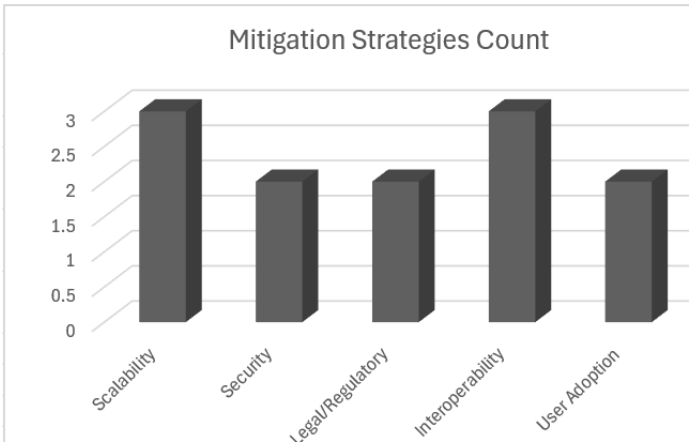

Figure 10. Key Challenges in Blockchain –Cloud Integration and Mitigation Strategies

Figure 10. highlights the major challenges encountered when integrating blockchain technology with cloud computing environments and outlines corresponding strategies to mitigate each challenge. It addresses technical, regulatory, and user-experience aspects to ensure scalable, secure, compliant, and user-friendly deployment of blockchain-cloud solutions[15].

5. Strategies For Addressing Blockchain Challenges

5.1. Scalability and Performance Issues

Blockchain struggles with processing large numbers of transactions quickly. To overcome this, solutions like Layer 2 networks (e.g., Lightning Network for Bitcoin) process transactions off-chain, reducing congestion. Sharding splits the network into smaller parts to handle transactions in parallel will also help[16]. Additionally, moving from Proof of Work (PoW) to Proof of Stake (PoS) as in Ethereum 2.0, can improve transaction speeds since it consumes less energy.

5.2. Security Vulnerabilities

Blockchain systems face risks like 51% attacks and bugs in smart contracts. To improve security, developers are working on quantum-resistant cryptography to prevent future threats and using zero-knowledge proofs to enhance privacy. Verifying smart contracts with formal methods ensures they behave correctly, reducing the risk of bugs. New consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT) also make networks more resilient to attacks.

5.3. Regulatory and Legal Challenges

Blockchain technology often operates outside of clear legal frameworks, making it hard to comply with regulations. To solve this, there needs to be international standards and clear rules for blockchain implementation. Self-regulation by industry groups can also help to set best practices. Technologies like zero-knowledge proofs can protect user privacy while complying with laws like GDPR and on-chain governance allows blockchain networks to adapt to changing regulations.

5.4 . Interoperability between Blockchains

Different blockchains cannot easily communicate with each other, limiting their use. Cross-chain bridges allow assets and data to move between blockchains. New platforms like Polkadot and Cosmos are being developed to support seamless interaction between networks. By creating standardized protocols, blockchains can easily work together, making the entire system more flexible and useful[17].

5.5. User Adoption and understanding

Blockchain is still considered as complex and difficult technique for the users to understand. To encourage adoption, more user-friendly interfaces are being created, and the onboarding process is being simplified by developers. Awareness about how blockchain works and its benefits can be spread through educational campaigns. Real-world applications, like supply chain tracking and decentralized finance (DeFi), are also

making blockchain technology more practical and accessible. By focusing on these strategies, businesses can address the major challenges of integrating blockchain with cloud computing more effectively[18].

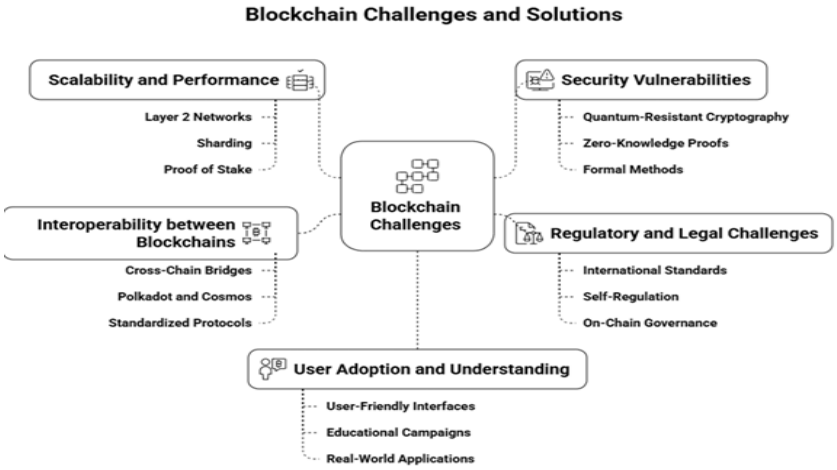

Figure 11. Blockchain Challenges and Solutions

Figure 11. highlights key blockchain challenges and their solutions across five areas. Scalability is improved through Layer 2 networks, sharding, and Proof of Stake, while security is enhanced using quantum-resistant cryptography and zero-knowledge proofs. Interoperability is addressed via cross-chain bridges and standardized protocols, and regulatory issues are tackled with international standards and on-chain governance. Finally, user adoption is boosted through user-friendly interfaces, education, and real-world applications.

6. Case Studies

Blockchain in cloud computing provides many transformative use cases across various industries. In supply chain management, blockchain offers transparency and traceability. Companies like IBM Food Trust use blockchain integrated with cloud solutions to track products from origin to consumer, reducing fraud and ensuring product authenticity. In healthcare, blockchain provides securely manage sensitive patient data, enabling decentralized storage and tamper-proof medical records. Cloud-hosted blockchain platforms like MedRec allow authorized parties such as doctors or patients to securely access and manage medical records while maintaining privacy[19].

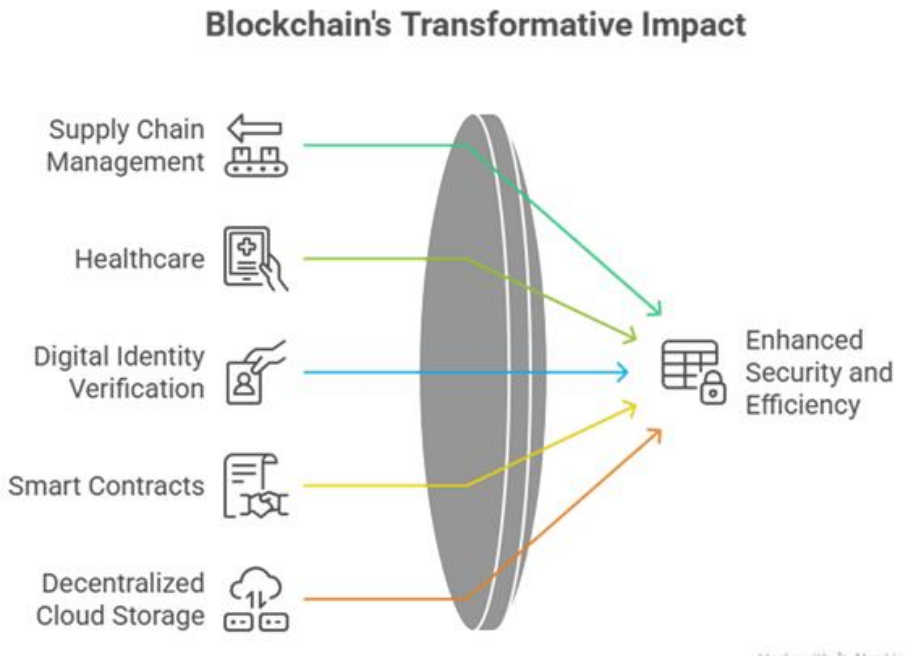

Figure 12. Blockchain Transformative Impact

Figure 12. shows how blockchain transforms various sectors—like supply chain management, healthcare, digital identity verification, smart contracts, and decentralized cloud storage—by delivering enhanced security and efficiency. Each use case benefits from blockchain's transparency, immutability, and decentralized structure. In digital identity verification, where cloud-based blockchain systems, such as uPort, allow individuals to control their own digital identities without relying on centralized authorities with improved security, privacy, and prevents identity theft. Smart contracts are revolutionizing industries like real estate, where cloud-based blockchain networks automatically enforce agreements, such as property transfers, once predefined conditions are met, reducing the need for intermediaries. At last, decentralized cloud storage is gaining popularity. Platforms like Storj use blockchain to decentralize cloud storage, allowing users to store data securely and more cost-effectively. This approach leverages blockchain's immutability and decentralization, ensuring that data stored in the cloud remains secure, private, and easily accessible without relying on traditional, centralized cloud storage providers These use cases demonstrate how blockchain in cloud computing can drive innovation, enhance security, and improve efficiency across various domains.

7. Proposed Blockchain-Cloud Security Framework

To address the limitations of traditional cloud security, we propose a new blockchain-integrated cloud framework that improves data integrity, confidentiality, and trust in cloud environments. This framework uses consensus mechanisms and cryptographic techniques to create a secure, scalable, and transparent infrastructure. The main components of the proposed framework include: Distributed Blockchain Ledger: A tamper-proof, decentralized ledger maintained across cloud nodes to ensure data records remain intact and unchangeable. This removes single points of failure and builds trust among stakeholders. Smart Contracts: Self-executing code embedded in the blockchain that automates Service-Level Agreements (SLAs), enforces access control policies, and manages resource allocation transparently and without human involvement. Consensus Algorithms: RAFT is used in private cloud environments and provides a lightweight, efficient consensus mechanism. It works well in systems with trusted nodes, ensuring high availability and easy implementation. Practical Byzantine Fault Tolerance (PBFT) is used in public or consortium cloud environments. It offers strong protection against malicious actors and Byzantine faults. It allows secure consensus even with untrusted or potentially compromised nodes. Both RAFT and PBFT are energy-efficient alternatives to Proof of Work (PoW), lowering computational demands and enhancing performance. Encrypted Cloud Storage: All data stored in the cloud is encrypted to maintain confidentiality, while the blockchain layer ensures data integrity and traceability. This dual-layer approach boosts protection against unauthorized access and tampering.Together, these elements create a unified structure that combines the transparency and security of blockchain with the scalability and flexibility of cloud computing. This provides a modern solution for secure and trustworthy cloud services. [20].

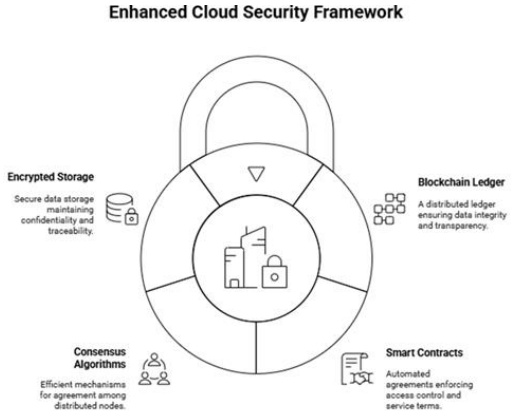

Figure 13. Enhanced Cloud Security Framework

Figure 13. illustrates an enhanced cloud security framework using blockchain. It includes encrypted storage for confidential data, a blockchain ledger for integrity and transparency, consensus algorithms for agreement across nodes, and smart contracts to automate access control and service terms. Together, these elements strengthen cloud data protection.

8. Results And Discussion

Table 2. Comparative Analysis of Cloud and Blockchain–Cloud Architectures

Attribute	Cloud	Blockchain-Cloud
Data Integrity	Moderate	High
Transparency	Low	High
Centralization	Centralized	Decentralized
Resistance to Tampering	Moderate	Very High
Auditability	Limited	Full

Table 2. compares traditional cloud computing with blockchain-integrated cloud architectures across key attributes such as data integrity, transparency, centralization, tamper resistance, and auditability. It highlights the enhanced security, decentralization, and trust features introduced by blockchain integration.

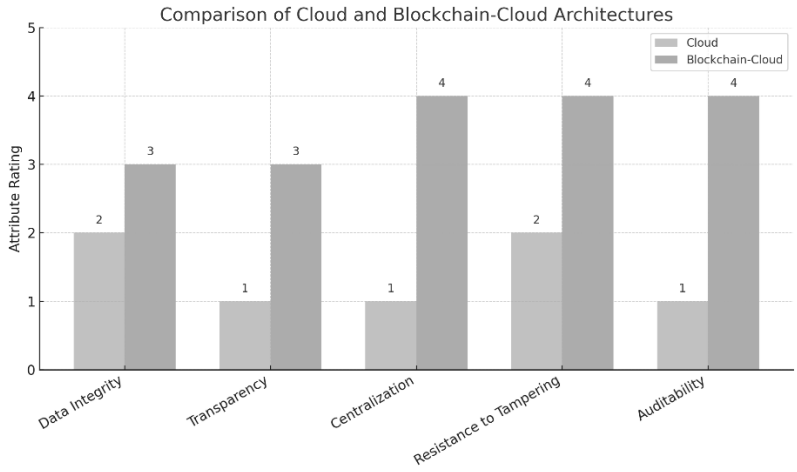

Figure 14. Comparison of Cloud and Blockchain-Cloud Architectures

Figure 14. compares Cloud and Blockchain-Cloud architectures across key attributes. Blockchain-Cloud scores higher in data integrity, transparency, decentralization, tamper resistance, and auditability, indicating stronger performance in security and trust. Traditional cloud systems lag behind, especially in transparency and auditability.

Table 3. Comparison Between Traditional Cloud and Blockchain-Enabled Cloud

Metric	Traditional Cloud	Blockchain-Enabled Cloud
Data Tampering Incidents	5 per month	0 per month
Average Access Time (ms)	120	150
Data Recovery Time (mins)	20	5
Transparency Level	Low	High
User Trust Index (out of 10)	6.5	9.2

Table 3. compares key performance metrics of Traditional Cloud and Blockchain-Enabled Cloud systems. The blockchain-based cloud shows superior security and transparency with zero tampering incidents and high user trust. However, it has slightly slower access time (150 ms vs. 120 ms). Data recovery is significantly faster in the blockchain cloud, highlighting its efficiency in disaster recovery.

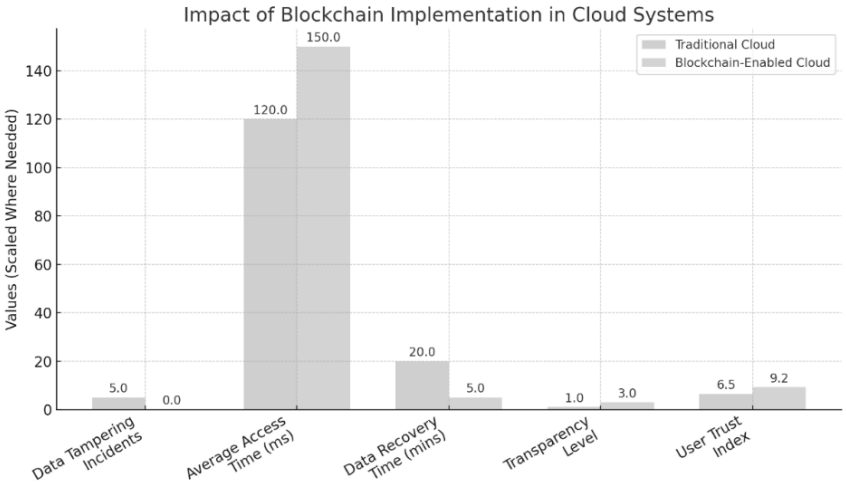

Figure 15. Impact of Blockchain Implementation in Cloud Systems

Figure 15. is a graph showing the impact of adding blockchain to a cloud system. It clearly highlights improvements in data tampering, recovery time, transparency, and user trust, though access time slightly increases due to blockchain overhead[15].

9. Conclusion

In this paper, a systematic survey of blockchain technology integrated with cloud computing to secure cloud data has been assessed. When blockchain technology is combined with cloud computing, usability, trust, security, scalability, and data management will contribute towards significant improvement in cloud performance. Additionally, this paper presents a comprehensive overview of few applications directions of blockchain: cryptocurrencies, supply chains, and healthcare security.[20] It explains the significant advantages that blockchain offers in these areas and provides a certain degree of outlook for future improvement in adoption of cloud technology. As a future direction, we propose a blockchain-cloud security framework that leverages smart contracts, encrypted storage, and advanced consensus algorithms like RAFT and PBFT to enhance trust and resilience. This framework aims to overcome current limitations of cloud security by ensuring tamper-proof data, automated policy enforcement, and efficient fault-tolerant operations.

References

[1] Rodrigues, Rodrigo Craveiro, Pedro Miguel Calhau Mateus, and Valderi Reis Quietinho Leithardt. "Prichain II: CloudGuardian Cloud Security Proposal with Blockchain." arXiv preprint arXiv:2407.19961, 2024.

[2] Habib, Gousia, Sparsh Sharma, Sara Ibrahim, Imtiaz Ahmad, Shaima Qureshi, and Malik Ishfaq. "Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing." Future Internet 14, no. 11 , 2022.

[3] Fadhil, Jawaher, and Subhi RM Zeebaree. "Blockchain for Distributed Systems Security in Cloud Computing: A Review of Applications and Challenges." Indonesian Journal of Computer Science 13, no. 2 , 2024.

[4] Kishor, Kaushal. "Cloud computing in blockchain." In Cloud-based Intelligent Informative Engineering for Society 5.0, pp. 79-105. Chapman and Hall/CRC, 2023.

[5] Sharma, Pratima, Rajni Jindal, and Malaya Dutta Borah. "Blockchain technology for cloud storage: A systematic literature review." ACM Computing Surveys (CSUR) 53, no. 4 2020, pp.1-32.

[6] Wang, Mu, Changqiao Xu, Xingyan Chen, Lujie Zhong, Zhonghui Wu, and Dapeng Oliver Wu. "BC-mobile device cloud: A blockchain-based decentralized truthful framework for

mobile device cloud." IEEE Transactions on Industrial Informatics 17, no. 2, 2020. pp. 1208-1219.

[7] Farah, Mohamed Ben, Yussuf Ahmed, Haithem Mahmoud, Syed Attique Shah, M. Omar Al-Kadri, Sandy Taramonli, Xavier Bellekens, Raouf Abozariba, Moad Idrissi, and Adel Aneiba. "A survey on blockchain technology in the maritime industry: challenges and future perspectives." Future Generation Computer Systems ,2024.

[8] Liu, Jiajun, and Junhao Wu. "A Comprehensive Survey on Blockchain Technology and Its Applications." Highlights in Science, Engineering and Technology 85, 2024, pp. 128-138.

[9] Dong, Shi, Khushnood Abbas, Meixi Li, and Joarder Kamruzzaman. "Blockchain technology and application: an overview." PeerJ Computer Science 9 , 2023.

[10] Musa, Hussam Saeed, Moez Krichen, Adem Alpaslan Altun, and Meryem Ammi. "Survey on blockchain-based data storage security for android mobile applications." Sensors 23, no. 21, 2023.

[11] Khanna, Abhirup, Anushree Sah, Vadim Bolshev, Alessandro Burgio, Vladimir Panchenko, and Marek Jasiński. "Blockchain–cloud integration: a survey." Sensors 22, no. 14, 2022.

[12] Sarmah, Simanta Shekhar. "Application of blockchain in cloud computing." International Journal of Innovative Technology and Exploring Engineering (IJITEE) 8, no. 12, 2019, pp.4698-4704.

[13] Habib, Gousia, Sparsh Sharma, Sara Ibrahim, Imtiaz Ahmad, Shaima Qureshi, and Malik Ishfaq. "Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing." Future Internet 14, no. 11, 2022.

[14] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." International journal of web and grid services 14, no. 4, 2018, pp. 352-375.

[15] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, 14(11), 341. 2022.

[16] Sharma, P., Jindal, R., & Borah, M. D. Blockchain technology for cloud storage: A systematic literature review. ACM Computing Surveys (CSUR), 53(4), 1-32. 2020.

[17] Khanna, A., Sah, A., Bolshev, V., Burgio, A., Panchenko, V., & Jasiński, M. Blockchain–cloud integration: A survey. Sensors, 22(14), 5238. 2022.

[18] Sarmah, S. S. (2019). Application of blockchain in cloud computing. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(12), pp. 4698-4704.

[19] Rodrigues, R. C., Mateus, P. M. C., & Leithardt, V. R. Q, Prichain II: CloudGuardian Cloud Security Proposal with Blockchain. arXiv preprint arXiv:2407.19961. 2024.

[20] Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. Blockchain technology and application: an overview. PeerJ Computer Science, 9, e1705. 2023.