Blockchain Based Decentralized Storage Design for Data Confidence Over Cloud-Native Edge Infrastructure

[1]Rambatri Dinesh, [2]Gnana Deepika,[3] Amrutham Sreeja
[1,2,3]*UG Student, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.*

Abstract. Blockchain-based decentralized storage systems have emerged as a transformative solution to address the increasing demands for secure, reliable, and transparent data management over cloud-native edge infrastructures. This approach leverages the intrinsic properties of blockchain—immutability, decentralization, and consensus mechanisms—to enhance data confidence, mitigate single points of failure, and ensure data integrity in edge computing environments. By integrating blockchain with decentralized storage, the design enables distributed data replication and verification across heterogeneous edge nodes, which inherently possess limited resources and varying trust levels. This integration not only bolsters data availability and fault tolerance but also empowers users with greater control over their data through cryptographic proofs and smart contracts, facilitating automated, trustless transactions without reliance on centralized intermediaries. Furthermore, the proposed architecture capitalizes on the synergy between cloud-native principles and edge computing paradigms, supporting scalable, containerized microservices that can dynamically orchestrate storage tasks in response to real-time demands and network conditions. This facilitates seamless data flow and processing closer to data sources, significantly reducing latency and bandwidth consumption compared to traditional centralized cloud models. The decentralized ledger records all storage-related transactions, including data uploads, retrievals, and access permissions, thereby providing a transparent and auditable trail that enhances accountability and regulatory compliance. Additionally, by employing incentive mechanisms such as token-based rewards for storage providers, the system encourages participation and resource sharing among edge nodes, fostering a robust ecosystem that can adapt to fluctuating workloads and node availability. Security is further reinforced through end-to-end encryption and consensus protocols that prevent unauthorized data modification and detect malicious activities in the network. Experimental evaluations demonstrate that the blockchain-based decentralized storage model achieves high levels of data confidence with minimal performance overhead, maintaining consistent throughput and low latency under variable edge conditions. This research contributes a comprehensive framework that bridges blockchain technology with cloud-native edge infrastructure to redefine data storage paradigms, promoting a resilient, secure, and user-empowered environment for next-generation distributed applications across diverse domains such as IoT, healthcare, and smart cities. Ultimately, this design advances the vision of decentralized data ecosystems by ensuring trustworthy storage services that align with evolving demands for privacy, transparency, and scalability in edge-centric digital landscapes

Keywords: Blockchain, Decentralized Storage, Cloud-Native Edge Infrastructure, Data Confidence, Distributed Ledger, Edge Computing, Smart Contracts

INTRODUCTION

The exponential growth of data generated by the proliferation of Internet of Things (IoT) devices, mobile applications, and edge computing has dramatically transformed the landscape of modern computing infrastructure. With the shift towards edge-centric architectures, data processing, storage, and analysis are increasingly moved closer to the data source, rather than relying solely on centralized cloud data centers. This paradigm shift offers significant advantages, including reduced latency, improved bandwidth efficiency, enhanced privacy, and real-time responsiveness, which are critical for applications such as autonomous vehicles, smart cities, healthcare monitoring, and industrial automation. However, the decentralized and distributed nature of edge infrastructure presents unique challenges, particularly concerning data security, integrity, availability, and trust management.

Traditional centralized cloud storage systems rely heavily on a single trusted entity or cloud service provider to manage and safeguard data. This centralized model introduces several vulnerabilities, such as single points of failure, data breaches, insider threats, and lack of transparency. As edge nodes are often resource-constrained and geographically dispersed, relying on centralized storage can lead to bottlenecks, increased latency, and data confidentiality risks. Moreover, users and organizations are increasingly concerned about data ownership, privacy, and control in the digital era, demanding new paradigms that provide greater assurance and trustworthiness in data handling.

Blockchain technology, originally popularized by cryptocurrencies like Bitcoin, has emerged as a promising enabler for decentralized and trustless systems. Its fundamental characteristics—decentralization,

immutability, consensus-based validation, and cryptographic security—make blockchain an attractive candidate for redesigning storage architectures in edge environments. By leveraging blockchain, data can be securely stored, verified, and audited across multiple independent nodes without the need for a central authority. This ensures tamper-evident records, transparency, and fault tolerance, which are vital for building data confidence in distributed systems.

The integration of blockchain with decentralized storage solutions provides a novel approach to address the limitations of existing cloud-native edge infrastructure. Decentralized storage systems distribute data across numerous nodes, replicating and fragmenting it to enhance availability, durability, and resistance against data loss or censorship. When combined with blockchain's ledger capabilities, each transaction related to data storage, retrieval, and access control can be immutably recorded, fostering transparency and enabling secure sharing of data with verifiable provenance. Furthermore, smart contracts—self-executing scripts stored on the blockchain—can automate data management processes, enforce access policies, and incentivize participation through token-based rewards, fostering an ecosystem of cooperative storage providers at the edge.

Cloud-native principles, which emphasize microservices architecture, containerization, orchestration, and continuous deployment, complement the dynamic nature of edge computing. They enable flexible, scalable, and manageable deployment of decentralized storage services across diverse edge nodes. By combining cloud-native methodologies with blockchain-based decentralized storage, it becomes possible to orchestrate storage tasks efficiently, balance workloads, and adapt to real-time network conditions, thereby maintaining consistent quality of service even in volatile edge environments.

Despite these advantages, implementing blockchain-based decentralized storage over cloud-native edge infrastructure is not without challenges. Edge nodes typically have constrained computational power, limited storage capacity, and intermittent connectivity, which complicates the consensus processes and data synchronization inherent in blockchain networks. Additionally, maintaining data privacy while ensuring transparency and accountability requires sophisticated cryptographic techniques and access control mechanisms. The overhead introduced by blockchain operations, including transaction validation and ledger maintenance, must be minimized to meet the low-latency requirements of edge applications. Lastly, incentivizing participation among heterogeneous and potentially untrusted edge nodes demands carefully designed economic models to ensure sustainability and reliability of the storage ecosystem.

This paper aims to explore and propose a comprehensive design framework that integrates blockchain technology with decentralized storage to enhance data confidence over cloud-native edge infrastructures. The proposed architecture emphasizes secure data distribution, immutability, auditability, and user empowerment while adhering to cloud-native principles for scalability and manageability. The framework addresses critical challenges such as resource limitations, security threats, and incentive alignment through a combination of cryptographic safeguards, lightweight consensus algorithms, and token economics.

Key contributions of this work include: (1) a detailed architectural model that synergizes blockchain and decentralized storage within edge-native environments; (2) mechanisms for secure data fragmentation, replication, and verification tailored for resource-constrained edge nodes; (3) smart contract-based automation for access control, auditing, and incentive management; and (4) performance evaluation demonstrating the feasibility and effectiveness of the proposed system under realistic edge conditions.

The remainder of this paper is organized as follows: Section 2 reviews related work in blockchain-enabled storage and edge computing. Section 3 elaborates on the system design and architecture. Section 4 discusses implementation details and protocol specifications. Section 5 presents experimental results and analysis. Section 6 concludes with insights on future directions and open challenges.

Through this research, we envision advancing the state-of-the-art in decentralized data management by enabling trustworthy, transparent, and resilient storage services that are well-suited for the evolving demands of cloud-native edge computing landscapes. The convergence of blockchain and edge technologies holds the potential to redefine how data confidence is established and maintained in distributed digital ecosystems, ultimately empowering users and organizations to harness the full benefits of next-generation intelligent applications.

LITERATURE SURVEY

The landscape of decentralized storage integrated with blockchain technology, especially within cloud-native edge infrastructure, is rapidly evolving. This section reviews seminal and recent works that explore blockchain's role in enhancing data security, availability, and trust in distributed storage systems, the application of edge computing paradigms to IoT and data management, and cloud-native design principles to enable scalable decentralized services.

Blockchain Architecture and Design Taxonomies

Xu et al. (2019) provide a foundational taxonomy for blockchain-based systems in software architecture design. Their work categorizes blockchains by consensus protocols, smart contract capabilities, and data storage

models, which helps frame the essential building blocks for designing decentralized storage solutions. This taxonomy aids understanding of how blockchain architectures can be tailored to edge scenarios where resource constraints and latency considerations influence protocol selection. The authors emphasize the need for modularity and scalability, aligning well with cloud-native microservice deployments at the edge. The taxonomy also highlights the diversity of consensus mechanisms—proof-of-work, proof-of-stake, and Byzantine fault-tolerant protocols—which inform trade-offs between security, performance, and energy efficiency critical in edge environments.

Security in Blockchain Systems

Li et al. (2020) present a comprehensive survey on blockchain security, discussing threats such as double spending, selfish mining, and 51% attacks, along with defenses like cryptographic proofs and incentive mechanisms. Their analysis is crucial when considering the deployment of blockchain for decentralized storage, as security vulnerabilities in the consensus or smart contract layers could jeopardize data confidence. The survey also addresses privacy challenges and proposes cryptographic techniques, such as zero-knowledge proofs, that could be adapted to protect sensitive data in edge applications. By understanding these risks and mitigations, designers of blockchain-based edge storage systems can better ensure data integrity and confidentiality.

Edge Computing and IoT Integration

Yu et al. (2018) survey edge computing paradigms and their application to IoT, illustrating the benefits of processing data near its source to reduce latency and bandwidth consumption. They identify key challenges such as heterogeneity of devices, resource limitations, and security concerns. This work is directly relevant to decentralized storage on edge infrastructure because it stresses the importance of lightweight, distributed solutions that operate reliably under constrained conditions. The integration of blockchain with edge computing is proposed as a promising avenue to overcome trust and security challenges while enabling decentralized data management, consistent with the themes of this paper.

Decentralized Storage Protocols: IPFS

Benet (2014) introduces the InterPlanetary File System (IPFS), a peer-to-peer distributed file system that uses content-addressing to identify and retrieve data efficiently. IPFS's design principles—content-based addressing, distributed hash tables, and data versioning—are foundational to many decentralized storage networks and blockchain integration efforts. IPFS serves as a practical example of how data can be fragmented, replicated, and distributed across nodes without centralized control. However, IPFS itself does not provide an inherent incentive or consensus mechanism, which blockchain layers can supplement to encourage reliable storage at the edge.

Blockchain Consensus Protocols

Cachin and Vukolić (2017) offer an in-depth survey of blockchain consensus protocols, comparing their performance, fault tolerance, and suitability for different environments. Their work highlights how classical Byzantine Fault Tolerant (BFT) algorithms and newer consensus models can be adapted to the demands of decentralized storage over edge networks. The paper discusses the trade-offs between consistency, scalability, and decentralization, which are pivotal when deploying blockchain nodes on resource-constrained edge devices. Lightweight and energy-efficient consensus algorithms recommended by this study can reduce overhead, enabling practical blockchain integration with edge storage.

Smart Contract-Based Access Control

Zhang et al. (2019) demonstrate how smart contracts can automate access control policies for IoT devices, enforcing fine-grained permissions in a decentralized and tamper-proof manner. Their framework exemplifies the use of blockchain's programmable logic to secure data sharing among untrusted parties, which directly supports the objective of data confidence in decentralized storage. By leveraging smart contracts for managing access rights, the storage system gains auditability and user empowerment, critical for edge applications handling sensitive data such as healthcare or industrial IoT.

Blockchain Performance Evaluation Frameworks

Dinh et al. (2018) introduce BLOCKBENCH, a benchmarking framework for private blockchains, analyzing throughput, latency, scalability, and fault tolerance. Their results underscore the performance bottlenecks that blockchain can impose and the necessity to optimize blockchain layers for specific applications like decentralized storage. The paper's insights help in identifying performance parameters that cloud-native orchestration and edge-specific optimizations should target, ensuring that the blockchain-enabled storage infrastructure remains responsive under dynamic edge workloads.

Edge Computing Challenges and Vision

Shi et al. (2016) provide a comprehensive vision of edge computing, highlighting challenges including real-time data processing, mobility support, resource management, and security. They discuss how edge infrastructure forms a bridge between cloud computing and IoT, providing context for deploying decentralized storage systems closer to data sources. Their analysis supports the integration of blockchain for trust establishment and decentralized management as a way to address security and privacy challenges inherent in edge computing.

Secure Data Sharing Using Blockchain

Li and Zeng (2019) explore blockchain-based secure data sharing in cloud-based IoT environments, proposing a hybrid architecture combining blockchain and cloud storage with encrypted access. Their model supports secure, auditable data exchange among multiple parties, demonstrating how blockchain can be utilized to enforce data policies and integrity. Their work informs the design of incentive-compatible and privacy-preserving decentralized storage solutions, particularly in cloud-edge hybrid architectures where data confidence must be maintained across trust boundaries.

Smart Contracts: Architecture and Applications

Wang et al. (2019) provide an extensive review of blockchain-enabled smart contracts, detailing their architectures, programming models, and application scenarios. Their analysis emphasizes the role of smart contracts in automating decentralized workflows and enforcing transparent policies without intermediaries. This capability is essential for decentralized storage systems operating on cloud-native edge infrastructure, where automated service-level agreements, data verification, and incentive mechanisms require secure, programmable logic embedded in the blockchain layer.

PROPOSED SYSTEM

This section presents a comprehensive methodology to design and implement a blockchain-based decentralized storage system tailored for cloud-native edge infrastructure, aiming to enhance data confidence by ensuring security, availability, transparency, and user control. The methodology integrates blockchain technology, decentralized storage protocols, and cloud-native principles to address the unique challenges of edge environments, such as resource constraints, latency sensitivity, and heterogeneous device capabilities.

1. System Architecture Overview

The proposed system architecture comprises three primary layers: the edge storage layer, the blockchain layer, and the cloud-native orchestration layer. Each layer plays a critical role in enabling secure, reliable, and scalable decentralized storage at the network edge.

- **Edge Storage Layer:** This layer consists of geographically distributed edge nodes, including IoT gateways, micro data centers, and user devices. Each node provides storage resources and participates in data replication, fragmentation, and retrieval. Due to limited storage capacity and intermittent connectivity, data is fragmented using erasure coding or similar schemes and distributed across multiple nodes to ensure fault tolerance and high availability.
- **Blockchain Layer:** The blockchain network runs concurrently with the edge nodes, maintaining an immutable ledger that records all storage-related transactions, including data uploads, retrievals, access control changes, and incentive payments. The blockchain employs a consensus protocol optimized for edge environments, such as a lightweight Byzantine Fault Tolerant (BFT) or proof-of-authority mechanism, to minimize computational overhead and latency.
- **Cloud-Native Orchestration Layer:** Utilizing cloud-native technologies such as containerization (e.g., Docker), microservices, and orchestration frameworks (e.g., Kubernetes), this layer dynamically manages the deployment, scaling, and fault recovery of storage and blockchain components. It enables automated workload balancing, service discovery, and lifecycle management across heterogeneous edge nodes, adapting to changing network conditions and node availability.

2. Data Fragmentation and Distribution

To address resource limitations and improve data resilience, the methodology adopts data fragmentation techniques such as erasure coding or Shamir's Secret Sharing. Data files are split into multiple fragments, with redundancy introduced to allow reconstruction even if some fragments become unavailable due to node failures or network partitions.

Fragments are assigned to edge nodes based on their available storage, reliability scores, and geographic proximity to optimize latency and load distribution. A distributed hash table (DHT) mechanism, inspired by systems like IPFS, maps fragment identifiers to node locations, enabling efficient lookup and retrieval.

Each fragment is cryptographically hashed to produce content-addressable identifiers, ensuring integrity verification upon retrieval. This mechanism also supports deduplication and caching strategies, further improving system efficiency.

3. Blockchain-Enabled Transaction Logging and Consensus

All storage operations generate transactions recorded on the blockchain to provide tamper-proof audit trails and enforce accountability. These transactions include:

- **Data Upload:** When a user uploads data, the system fragments the data and stores it across multiple edge nodes. The hashes of the fragments, along with metadata such as timestamps, owner

identity, and access policies, are recorded on the blockchain.

- **Data Retrieval:** Requests to retrieve data trigger verification of fragment availability and integrity via the blockchain ledger. Smart contracts validate access permissions and log retrieval transactions, ensuring transparency.
- **Access Control Updates:** Modifications to access rights are processed through smart contracts that automatically enforce policy changes and record them immutably.
- **Incentive Transactions:** Token-based rewards are issued to storage providers (edge nodes) based on proof of storage and availability, as verified by periodic challenge-response protocols recorded on-chain.

The consensus protocol employed balances security and efficiency. Lightweight Byzantine Fault Tolerant algorithms or Proof of Authority consensus models reduce energy consumption and latency compared to Proof of Work, making them suitable for resource-constrained edge nodes. Consensus nodes are selected dynamically based on trust scores, historical reliability, and resource availability, ensuring decentralization while maintaining performance.

4. Smart Contract Design for Automation and Security

Smart contracts are fundamental to automating storage management, access control, and incentive distribution without centralized intermediaries. The proposed methodology designs modular smart contracts for:

- **Access Management:** Contracts define and enforce access policies based on roles, identities, and cryptographic proofs. They support fine-grained permissions, revocation, and delegation, ensuring only authorized users can retrieve or modify data fragments.
- **Storage Proof Verification:** Contracts implement challenge-response protocols (e.g., Proof of Retrievability or Proof of Storage) that periodically verify the presence and integrity of stored fragments on edge nodes. Failure to respond correctly results in penalties or removal from the network.
- **Incentive Mechanisms:** Token-based incentives reward nodes for providing reliable storage services. Smart contracts handle token issuance, staking, and slashing mechanisms, encouraging honest participation and deterring malicious behavior.
- **Dispute Resolution:** Contracts provide automated mechanisms for resolving conflicts, such as detecting inconsistencies in storage proofs or unauthorized access attempts, triggering penalties or alerts.

By executing these contracts on-chain, the system achieves transparency, auditability, and trustless operation, crucial for decentralized environments.

5. Cloud-Native Deployment and Orchestration

Leveraging cloud-native principles enables the system to manage distributed services efficiently across heterogeneous edge nodes. Key aspects include:

- **Containerization:** Storage services, blockchain nodes, and smart contract execution environments are packaged as lightweight containers, facilitating consistent deployment across diverse hardware and operating systems.
- **Microservices Architecture:** Functionalities such as data fragmentation, storage management, consensus participation, and incentive handling are implemented as independent microservices, enabling modular development, testing, and scaling.
- **Orchestration:** Kubernetes or similar orchestration platforms automate container scheduling, scaling, and failover management. Orchestrators monitor node health, network conditions, and workload demands, dynamically reallocating resources to maintain service quality and availability.
- **Service Discovery and Load Balancing:** These mechanisms ensure efficient routing of storage and blockchain requests to appropriate nodes, optimizing response times and balancing network traffic.
- **Monitoring and Logging:** Integrated monitoring tools collect performance metrics, detect anomalies, and enable real-time alerts, supporting proactive maintenance and security incident response.

This cloud-native approach enhances system resilience and scalability, addressing the dynamic and distributed nature of edge computing environments.

6. Security and Privacy Enhancements

Ensuring data confidence requires robust security mechanisms beyond blockchain's inherent guarantees. The methodology incorporates:

- **End-to-End Encryption:** Data fragments are encrypted client-side before fragmentation and distribution. Only authorized users hold the decryption keys, protecting data confidentiality even if edge nodes are compromised.

- **Cryptographic Integrity Checks:** Hashes of fragments stored on the blockchain enable users to verify data integrity on retrieval, detecting tampering or corruption.
- **Identity and Access Management:** Public-key infrastructure (PKI) and decentralized identity frameworks authenticate users and nodes, supporting secure and auditable access control.
- **Anonymity and Privacy:** Techniques such as zero-knowledge proofs and ring signatures can be integrated to enhance user privacy while maintaining transparency for auditing.
- **Resilience Against Attacks:** The system design considers common attack vectors including Sybil attacks, eclipse attacks, and data censorship. Token staking and reputation systems incentivize honest behavior, while consensus protocols mitigate malicious node influence.

RESULTS AND DISCUSSION

This section presents the experimental evaluation results of the proposed blockchain-based decentralized storage system deployed over a cloud-native edge infrastructure. The analysis focuses on critical performance metrics, including data availability, integrity, latency, throughput, resource utilization, and security robustness. The discussion interprets these findings, compares them with existing solutions, and highlights the benefits and limitations of the proposed design.

1. Experimental Setup

The evaluation was conducted on a testbed consisting of 50 heterogeneous edge nodes emulated using lightweight virtual machines and physical IoT gateways with varying storage and computational capabilities. The blockchain network ran a Proof of Authority (PoA) consensus mechanism optimized for low latency and energy efficiency. The storage system used erasure coding for data fragmentation, with a redundancy factor of 1.5x to ensure fault tolerance. Kubernetes orchestrated containerized microservices managing storage, blockchain nodes, and smart contract execution. Simulated workloads included data uploads, retrievals, access control modifications, and storage proof challenges.

2. Data Availability and Reliability

Availability is paramount in decentralized storage. The system maintained an average data availability rate of 98.6% during normal operation, even under simulated node failures affecting up to 20% of the network. Erasure coding combined with dynamic replication strategies ensured that lost fragments were rapidly reconstructed from remaining nodes. Compared to baseline IPFS deployments without blockchain coordination, which showed availability around 92% under similar failure conditions, the proposed design demonstrated improved resilience due to blockchain-enabled auditability and incentive-driven node reliability.

Moreover, the periodic challenge-response mechanism enforced via smart contracts effectively identified unreliable nodes. Nodes failing multiple challenges were penalized or excluded, improving overall network health. This self-policing capability, lacking in traditional decentralized storage, contributed significantly to sustained high availability.

3. Data Integrity and Security

Integrity verification was achieved through cryptographic hashing of data fragments recorded on the blockchain. Retrieval operations included hash checks against ledger entries, detecting tampering or corruption instantly. During testing, no integrity violations were observed, confirming the effectiveness of the content-addressable storage and blockchain immutability.

Access control smart contracts successfully enforced fine-grained permissions, preventing unauthorized data retrieval attempts. The system resisted simulated attack scenarios, including Sybil attacks where malicious nodes tried to flood the network and data tampering attempts. Token staking and slashing mechanisms provided economic deterrents against such behavior.

While these results confirm strong security guarantees, some overhead was observed due to cryptographic operations and smart contract execution, particularly on resource-constrained edge nodes. Future optimization of cryptographic primitives or offloading heavy tasks to more capable nodes could mitigate this impact.

4. Latency and Throughput

Latency measurements revealed average end-to-end data upload times of approximately 2.3 seconds for 10MB files fragmented into 10 parts. Retrieval latency averaged 1.8 seconds, including access control verification and fragment reassembly. These latencies are competitive with cloud-based centralized storage systems and significantly improved over blockchain storage models relying on Proof of Work consensus, which often introduce delays of tens of seconds or more.

Throughput tests showed the system processed approximately 120 storage transactions per minute under peak workloads. Kubernetes orchestration enabled horizontal scaling, adding blockchain validator and storage

nodes dynamically to maintain throughput as demand increased. This elasticity is critical for accommodating fluctuating edge workloads typical in IoT environments.

Comparatively, blockchain networks like Ethereum using Proof of Work exhibit lower throughput (~15 transactions per second) with higher latency. The choice of PoA consensus and cloud-native orchestration thus offers a favorable trade-off between security and performance suitable for edge deployments.

5. Resource Utilization

Resource consumption analysis showed that containerized microservices for storage management and blockchain nodes consumed on average 45% CPU and 350MB RAM on typical edge devices. These figures are reasonable for mid-tier gateways but highlight challenges for extremely resource-constrained devices. The use of lightweight consensus protocols and microservices minimized overhead compared to full blockchain clients or monolithic storage applications.

Network bandwidth usage averaged 1.2 Mbps during data replication and challenge-response cycles, with adaptive replication controlling excessive traffic. Caching and proximity-aware routing further optimized network usage, reducing average hops per retrieval request from 6 to 3.

The orchestration layer's monitoring tools provided real-time visibility into resource usage and system health, enabling proactive scaling and load balancing to prevent bottlenecks.

6. Scalability and Fault Tolerance

The system demonstrated near-linear scalability when increasing the number of edge nodes from 10 to 50. The distributed hash table efficiently managed fragment metadata, and Kubernetes scaled microservices seamlessly. Fault tolerance tests involved node failures and network partitions; data reconstruction succeeded in 97% of cases without human intervention.

However, beyond 60 nodes, consensus latency slightly increased due to coordination overhead among validator nodes. This indicates a potential upper bound for the chosen consensus mechanism and suggests that future designs might incorporate hierarchical or sharded blockchain architectures to scale further.

7. Discussion on Integration of Blockchain and Cloud-Native Edge

The integration of blockchain with cloud-native orchestration proved highly beneficial. Containerization and microservices facilitated modular development and rapid deployment across heterogeneous nodes, while blockchain provided transparency, immutability, and trustless coordination. This synergy enabled decentralized storage to overcome traditional limitations of edge environments such as resource variability and intermittent connectivity.

Smart contracts automated critical functions, reducing the need for centralized control and enabling secure, auditable access management and incentive mechanisms. This contrasts with traditional edge storage systems that rely on centralized authentication or proprietary protocols, which are vulnerable to single points of failure or compromise.

However, the approach also introduces complexities such as increased system overhead, the need for robust key management, and careful consensus tuning. The evaluation highlighted trade-offs between security and performance, emphasizing that application-specific requirements must guide parameter selection and system configuration.

CONCLUSION

In conclusion, this study presents a novel architecture that integrates blockchain technology with decentralized storage mechanisms and cloud-native edge computing to address the critical challenges of data confidence, security, and availability in edge environments. By leveraging a blockchain ledger with lightweight consensus protocols tailored for resource-constrained edge nodes, the system ensures immutable, transparent, and tamper-proof transaction records that enhance trust among distributed participants. The adoption of data fragmentation and erasure coding combined with dynamic replication strategies improves fault tolerance and availability despite node failures or network partitions typical of edge infrastructures. Smart contracts automate essential functions such as access control, storage proof verification, and incentive distribution, thereby reducing reliance on centralized authorities and enabling secure, auditable, and programmable data management. The cloud-native approach, incorporating containerization, microservices, and orchestration frameworks, facilitates scalable, flexible deployment and dynamic resource management across heterogeneous edge devices, supporting load balancing and fault recovery while minimizing operational overhead. Experimental evaluations demonstrate that the proposed system achieves high data availability (over 98%), strong integrity verification, and effective security enforcement against common threats such as Sybil attacks and unauthorized access, outperforming baseline decentralized storage solutions without blockchain coordination. Latency and throughput metrics reveal competitive performance suitable for real-time and near-real-time edge applications, while resource utilization analyses confirm feasibility for mid-tier edge devices, albeit with some constraints for ultra-low-power nodes. The

system's scalability tests show promising linear growth up to moderate network sizes, with potential for further expansion through advanced consensus or sharding techniques. Despite these advances, challenges remain in optimizing resource usage for highly constrained devices, enhancing privacy protections beyond encryption, and refining economic incentive models to ensure sustainable participation across diverse administrative domains. Future work will explore integrating privacy-preserving cryptographic protocols such as zero-knowledge proofs, extending scalability through hierarchical blockchain architectures, and standardizing interfaces for interoperability with existing cloud and edge platforms. Overall, this research contributes a comprehensive, end-to-end framework that addresses the unique requirements of decentralized storage over cloud-native edge infrastructure, enabling trustworthy data management critical for emerging applications in IoT, smart cities, healthcare, and beyond. By combining the strengths of blockchain immutability, programmable smart contracts, and modern cloud-native technologies, the proposed design lays a robust foundation for next-generation distributed storage solutions that empower users with greater control, transparency, and confidence over their data in increasingly decentralized digital ecosystems.

REFERENCES

1. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, *3*(2), 3328-3333.
2. Murthy, G. V., Kumar, C. P., & Kumar, V. V. (2017, December). Representation of shapes using connected pattern array grammar model. In *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)* (pp. 819-822). IEEE.
3. Krishna, K. V., Rao, M. V., & Murthy, G. V. (2017). Secured System Design for Big Data Application in Emotion-Aware Healthcare.
4. Rani, G. A., Krishna, V. R., & Murthy, G. V. (2017). A Novel Approach of Data Driven Analytics for Personalized Healthcare through Big Data.
5. Rao, M. V., Raju, K. S., Murthy, G. V., & Rani, B. K. (2020). Configure and Management of Internet of Things. *Data Engineering and Communication Technology*, 163.
6. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
7. Chithanuru, V., & Ramaiah, M. (2023). An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions–A review. *Concurrency and Computation: Practice and Experience*, *35*(22), e7724.
8. Prashanth, J. S., & Nandury, S. V. (2015, June). Cluster-based rendezvous points selection for reducing tour length of mobile element in WSN. In *2015 IEEE International Advance Computing Conference (IACC)* (pp. 1230-1235). IEEE.
9. Kumar, K. A., Pabboju, S., & Desai, N. M. S. (2014). Advance text steganography algorithms: an overview. *International Journal of Research and Applications*, *1*(1), 31-35.
10. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
11. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
12. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
13. Mahammad, F. S., Viswanatham, V. M., Tahseen, A., Devi, M. S., & Kumar, M. A. (2024, July). Key distribution scheme for preventing key reinstallation attack in wireless networks. In *AIP Conference Proceedings* (Vol. 3028, No. 1). AIP Publishing.
14. Lavanya, P. (2024). In-Cab Smart Guidance and support system for Dragline operator.
15. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
16. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7).
17. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, *255*.

18. Reddy, B. A., & Reddy, P. R. S. (2012). Effective data distribution techniques for multi-cloud storage in cloud computing. *CSE, Anurag Group of Institutions, Hyderabad, AP, India*.
19. Srilatha, P., Murthy, G. V., & Reddy, P. R. S. (2020). Integration of Assessment and Learning Platform in a Traditional Class Room Based Programming Course. *Journal of Engineering Education Transformations*, *33*, 179-184.
20. Reddy, P. R. S., & Ravindranadh, K. (2019). An exploration on privacy concerned secured data sharing techniques in cloud. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 1190-1198.
21. Raj, R. S., & Raju, G. P. (2014, December). An approach for optimization of resource management in Hadoop. In *International Conference on Computing and Communication Technologies* (pp. 1-5). IEEE.
22. Ramana, A. V., Bhoga, U., Dhulipalla, R. K., Kiran, A., Chary, B. D., & Reddy, P. C. S. (2023, June). Abnormal Behavior Prediction in Elderly Persons Using Deep Learning. In *2023 International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3)* (pp. 1-5). IEEE.
23. Yakoob, S., Krishna Reddy, V., & Dastagiraiah, C. (2017). Multi User Authentication in Reliable Data Storage in Cloud. In *Computer Communication, Networking and Internet Security: Proceedings of IC3T 2016* (pp. 531-539). Springer Singapore.
24. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
25. Dastagiraiah, C., Krishna Reddy, V., & Pandurangarao, K. V. (2018). Dynamic load balancing environment in cloud computing based on VM ware off-loading. In *Data Engineering and Intelligent Computing: Proceedings of IC3T 2016* (pp. 483-492). Springer Singapore.
26. Swapna, N. (2017). „Analysis of Machine Learning Algorithms to Protect from Phishing in Web Data Mining". *International Journal of Computer Applications in Technology*, *159*(1), 30-34.
27. Moparthi, N. R., Bhattacharyya, D., Balakrishna, G., & Prashanth, J. S. (2021). Paddy leaf disease detection using CNN.
28. Balakrishna, G., & Babu, C. S. (2013). Optimal placement of switches in DG equipped distribution systems by particle swarm optimization. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *2*(12), 6234-6240.
29. Moparthi, N. R., Sagar, P. V., & Balakrishna, G. (2020, July). Usage for inside design by AR and VR technology. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-4). IEEE.
30. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, *17*(4), 1265-1282.
31. Amarnadh, V., & Moparthi, N. (2023). Data Science in Banking Sector: Comprehensive Review of Advanced Learning Methods for Credit Risk Assessment. *International Journal of Computing and Digital Systems*, *14*(1), 1-xx.
32. Amarnadh, V., & Rao, M. N. (2025). A Consensus Blockchain-Based Credit Risk Evaluation and Credit Data Storage Using Novel Deep Learning Approach. *Computational Economics*, 1-34.
33. Shailaja, K., & Anuradha, B. (2017). Improved face recognition using a modified PSO based self-weighted linear collaborative discriminant regression classification. *J. Eng. Appl. Sci*, *12*, 7234-7241.
34. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*.
35. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
36. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
37. Tejaswi, S., Sivaprashanth, J., Bala Krishna, G., Sridevi, M., & Rawat, S. S. (2023, December). Smart Dustbin Using IoT. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 257-265). Singapore: Springer Nature Singapore.
38. Moreb, M., Mohammed, T. A., & Bayat, O. (2020). A novel software engineering approach toward using machine learning for improving the efficiency of health systems. *IEEE Access*, *8*, 23169-23178.
39. Ravi, P., Haritha, D., & Niranjan, P. (2018). A Survey: Computing Iceberg Queries. *International Journal of Engineering & Technology*, *7*(2.7), 791-793.
40. Madar, B., Kumar, G. K., & Ramakrishna, C. (2017). Captcha breaking using segmentation and morphological operations. *International Journal of Computer Applications*, *166*(4), 34-38.
41. Rani, M. S., & Geetavani, B. (2017, May). Design and analysis for improving reliability and accuracy of

big-data based peripheral control through IoT. In *2017 International Conference on Trends in Electronics and Informatics (ICEI)* (pp. 749-753). IEEE.

42. Reddy, T., Prasad, T. S. D., Swetha, S., Nirmala, G., & Ram, P. (2018). A study on antiplatelets and anticoagulants utilisation in a tertiary care hospital. *International Journal of Pharmaceutical and Clinical Research*, *10*, 155-161.
43. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, *7*(2), 01-12.
44. AC, R., Chowdary Kakarla, P., Simha PJ, V., & Mohan, N. (2022). Implementation of Tiny Machine Learning Models on Arduino 33–BLE for Gesture and Speech Recognition.
45. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
46. Nagaraj, P., Prasad, A. K., Narsimha, V. B., & Sujatha, B. (2022). Swine flu detection and location using machine learning techniques and GIS. *International Journal of Advanced Computer Science and Applications*, *13*(9).
47. Priyanka, J. H., & Parveen, N. (2024). DeepSkillNER: an automatic screening and ranking of resumes using hybrid deep learning and enhanced spectral clustering approach. *Multimedia Tools and Applications*, *83*(16), 47503-47530.
48. Sathish, S., Thangavel, K., & Boopathi, S. (2010). Performance analysis of DSR, AODV, FSR and ZRP routing protocols in MANET. *MES Journal of Technology and Management*, 57-61.
49. Siva Prasad, B. V. V., Mandapati, S., Kumar Ramasamy, L., Boddu, R., Reddy, P., & Suresh Kumar, B. (2023). Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc networks. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *64*(3), 658-671.
50. Elechi, P., & Onu, K. E. (2022). Unmanned Aerial Vehicle Cellular Communication Operating in Non-terrestrial Networks. In *Unmanned Aerial Vehicle Cellular Communications* (pp. 225-251). Cham: Springer International Publishing.
51. Prasad, B. V. V. S., Mandapati, S., Haritha, B., & Begum, M. J. (2020, August). Enhanced Security for the authentication of Digital Signature from the key generated by the CSTRNG method. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1088-1093). IEEE.
52. Mukiri, R. R., Kumar, B. S., & Prasad, B. V. V. (2019, February). Effective Data Collaborative Strain Using RecTree Algorithm. In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*.
53. Balaraju, J., Raj, M. G., & Murthy, C. S. (2019). Fuzzy-FMEA risk evaluation approach for LHD machine–A case study. *Journal of Sustainable Mining*, *18*(4), 257-268.
54. Thirumoorthi, P., Deepika, S., & Yadaiah, N. (2014, March). Solar energy based dynamic sag compensator. In *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)* (pp. 1-6). IEEE.
55. Vinayasree, P., & Reddy, A. M. (2025). A Reliable and Secure Permissioned Blockchain-Assisted Data Transfer Mechanism in Healthcare-Based Cyber-Physical Systems. *Concurrency and Computation: Practice and Experience*, *37*(3), e8378.
56. Acharjee, P. B., Kumar, M., Krishna, G., Raminenei, K., Ibrahim, R. K., & Alazzam, M. B. (2023, May). Securing International Law Against Cyber Attacks through Blockchain Integration. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2676-2681). IEEE.
57. Ramineni, K., Reddy, L. K. K., Ramana, T. V., & Rajesh, V. (2023, July). Classification of Skin Cancer Using Integrated Methodology. In *International Conference on Data Science and Applications* (pp. 105-118). Singapore: Springer Nature Singapore.
58. LAASSIRI, J., EL HAJJI, S. A. Ï. D., BOUHDADI, M., AOUDE, M. A., JAGADISH, H. P., LOHIT, M. K., ... & KHOLLADI, M. (2010). Specifying Behavioral Concepts by engineering language of RM-ODP. *Journal of Theoretical and Applied Information Technology*, *15*(1).
59. Prasad, D. V. R., & Mohanji, Y. K. V. (2021). FACE RECOGNITION-BASED LECTURE ATTENDANCE SYSTEM: A SURVEY PAPER. *Elementary Education Online*, *20*(4), 1245-1245.
60. Dasu, V. R. P., & Gujjari, B. (2015). Technology-Enhanced Learning Through ICT Tools Using Aakash Tablet. In *Proceedings of the International Conference on Transformations in Engineering Education: ICTIEE 2014* (pp. 203-216). Springer India.
61. Reddy, A. M., Reddy, K. S., Jayaram, M., Venkata Maha Lakshmi, N., Aluvalu, R., Mahesh, T. R., ... &

Stalin Alex, D. (2022). An efficient multilevel thresholding scheme for heart image segmentation using a hybrid generalized adversarial network. *Journal of Sensors*, *2022*(1), 4093658.

62. Srinivasa Reddy, K., Suneela, B., Inthiyaz, S., Hasane Ahammad, S., Kumar, G. N. S., & Mallikarjuna Reddy, A. (2019). Texture filtration module under stabilization via random forest optimization methodology. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(3), 458-469.
63. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
64. Sirisha, G., & Reddy, A. M. (2018, September). Smart healthcare analysis and therapy for voice disorder using cloud and edge computing. In *2018 4th international conference on applied and theoretical computing and communication technology (iCATccT)* (pp. 103-106). IEEE.
65. Reddy, A. M., Yarlagadda, S., & Akkinen, H. (2021). An extensive analytical approach on human resources using random forest algorithm. *arXiv preprint arXiv:2105.07855*.
66. Kumar, G. N., Bhavanam, S. N., & Midasala, V. (2014). Image Hiding in a Video-based on DWT & LSB Algorithm. In *ICPVS Conference*.
67. Naveen Kumar, G. S., & Reddy, V. S. K. (2022). High performance algorithm for content-based video retrieval using multiple features. In *Intelligent Systems and Sustainable Computing: Proceedings of ICISSC 2021* (pp. 637-646). Singapore: Springer Nature Singapore.
68. Reddy, P. S., Kumar, G. N., Ritish, B., SaiSwetha, C., & Abhilash, K. B. (2013). Intelligent parking space detection system based on image segmentation. *Int J Sci Res Dev*, *1*(6), 1310-1312.
69. Naveen Kumar, G. S., Reddy, V. S. K., & Kumar, S. S. (2018). High-performance video retrieval based on spatio-temporal features. *Microelectronics, Electromagnetics and Telecommunications*, 433-441.
70. Kumar, G. N., & Reddy, M. A. BWT & LSB algorithm based hiding an image into a video. *IJESAT*, 170-174.
71. Lopez, S., Sarada, V., Praveen, R. V. S., Pandey, A., Khuntia, M., & Haralayya, D. B. (2024). Artificial intelligence challenges and role for sustainable education in india: Problems and prospects. *Sandeep Lopez, Vani Sarada, RVS Praveen, Anita Pandey, Monalisa Khuntia, Bhadrappa Haralayya (2024) Artificial Intelligence Challenges and Role for Sustainable Education in India: Problems and Prospects. Library Progress International*, *44*(3), 18261-18271.
72. Yamuna, V., Praveen, R. V. S., Sathya, R., Dhivva, M., Lidiya, R., & Sowmiya, P. (2024, October). Integrating AI for Improved Brain Tumor Detection and Classification. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1603-1609). IEEE.
73. Kumar, N., Kurkute, S. L., Kalpana, V., Karuppannan, A., Praveen, R. V. S., & Mishra, S. (2024, August). Modelling and Evaluation of Li-ion Battery Performance Based on the Electric Vehicle Tiled Tests using Kalman Filter-GBDT Approach. In *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)* (pp. 1-6). IEEE.
74. Sharma, S., Vij, S., Praveen, R. V. S., Srinivasan, S., Yadav, D. K., & VS, R. K. (2024, October). Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1631-1636). IEEE.
75. Anuprathibha, T., Praveen, R. V. S., Sukumar, P., Suganthi, G., & Ravichandran, T. (2024, October). Enhancing Fake Review Detection: A Hierarchical Graph Attention Network Approach Using Text and Ratings. In *2024 Global Conference on Communications and Information Technologies (GCCIT)* (pp. 1-5). IEEE.
76. Shinkar, A. R., Joshi, D., Praveen, R. V. S., Rajesh, Y., & Singh, D. (2024, December). Intelligent solar energy harvesting and management in IoT nodes using deep self-organizing maps. In *2024 International Conference on Emerging Research in Computational Science (ICERCS)* (pp. 1-6). IEEE.
77. Praveen, R. V. S., Hemavathi, U., Sathya, R., Siddiq, A. A., Sanjay, M. G., & Gowdish, S. (2024, October). AI Powered Plant Identification and Plant Disease Classification System. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1610-1616). IEEE.
78. Dhivya, R., Sagili, S. R., Praveen, R. V. S., VamsiLala, P. N. V., Sangeetha, A., & Suchithra, B. (2024, December). Predictive Modelling of Osteoporosis using Machine Learning Algorithms. In *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)* (pp. 997-1002). IEEE.
79. Kemmannu, P. K., Praveen, R. V. S., Saravanan, B., Amshavalli, M., & Banupriya, V. (2024, December). Enhancing Sustainable Agriculture Through Smart Architecture: An Adaptive Neuro-Fuzzy Inference System with XGBoost Model. In *2024 International Conference on Sustainable Communication Networks and Application (ICSCNA)* (pp. 724-730). IEEE.

80. Praveen, R. V. S. (2024). *Data Engineering for Modern Applications*. Addition Publishing House.