www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

SECURE AND EFFICIENT AUDITING FRAMEWORK FOR CLOUD DATA STORAGE

P. Swetha[1]
Assistant Professor Department
of CSE(DS)
TKR College of Engineering &Technology

G. Raghava[3]
B. Tech(Scholar) Department of
CSE(DS)
TKR College of Engineering &Technology
gollapallyraghava@gmail.com

B. Sai Krishna[5]
B. Tech(Scholar) Department of
CSE(DS)
TKR College of Engineering &Technology
saikrishna39659@gmail.com

A. Hari Chandan Reddy[2]
B. Tech(Scholar) Department
of CSE(DS)
TKR College of Engineering and Technology
harichandhanreddyailuri@gmail.com

G. Mounika[4]
B. Tech(Scholar) Department
of CSE(DS)
TKR College of Engineering and Technology
gajjemounika91@gmail.com

ABSTRACT

Secure data storage and integrity are critical challenges in cloud computing. This work presents a robust auditing scheme designed to ensure secure data storage in the cloud through efficient and reliable integrity- checking methods. The proposed schema integrates cryptographic technology and third- party auditing to guarantee confidentiality, authenticity, and availability, serving as a strong protection mechanism.The system comprises four key modules. The Sender module is responsible for securely encrypting data before storage. The Feature module generates integrity proofs to verify the data's authenticity. The Receiver module performs verification checks to ensure data integrity, while the Key Generation Centre (KGC) securely manages encryption keys. This comprehensive approach safeguards data against emerging threats, such as unauthorized access and data leaks, ensuring that sensitive information remains protected even in hostile environments.

Additionally, a Contact Us module is included to provide real-time support, enhancing transparency and trust by facilitating direct communication between users and the cloud service provider. The proposed schema is designed to be scalable, lightweight, and high- performing, aligning with the demands of modern cloud environments. Secure data storage and integrity are important challenges during cloud computing. This work describes a strong auditing scheme for secure data storage in the cloud with efficient and reliable integrity checking methods. This schema uses both cryptographic technology and thirdparty audit data stored to ensure that confidentiality, authenticity & availability are fully satisfied serving as a form of protection. It has four main modules, including a Sender module to encrypt data securely, a Feature module for integrity proofs, and a Receiver module to verify it together with the Key Generation Centre (KGC) to manage keys securely. This method can protect against new threats such as unauthorized access and data leaks, so that sensitive data is well protected even in destructive environments. Along with a Contact Us module for real-time support, it also allows robust transparency and trust by facilitating direct communication between users and the cloud service provider. It provides a schema that is scalable, lightweight and high-performance oriented to the needs of modern cloud environments. rewrite the above sentence and give vthe xentences in paragraph

KEY WORDS: Internet of Things(IOT),Cloud Computing(CC),Data Integrity,Data Auditing

1.INTRODUCTION

1. Ensuring data integrity is particularly crucial, as unauthorized modifications can undermine trust and reliability. Conventional verification methods are often inadequate for the dynamic and distributed nature of cloud environments. Therefore, an effective auditing mechanism must not only detect vulnerabilities but also provide a systematic approach to mitigating risks. This project proposes an advanced auditing schema that integrates cryptographic techniques and innovative verification processes to enhance data security in the cloud.

2. A major challenge in cloud storage security is the delegation of control. Users typically relinquish direct oversight of their data when storing it on cloud platforms, which, while convenient, raises concerns about unauthorized access and data tampering. The proposed auditing framework prioritizes user-centric security by allowing users to verify data integrity without direct access to cloud storage. This ensures transparency and builds trust while enabling users to benefit from cloud technology without compromising security.

3. The auditing schema is structured around four core modules: Sender, Features, Receiver, and Key Generation Centre (KGC). The Sender module ensures secure encryption of data before it is uploaded to the cloud, preserving confidentiality. The Feature module generates integrity proofs, enabling efficient and transparent data verification. The Receiver module facilitates secure validation processes, while the KGC module manages cryptographic keys to strengthen overall data security. Together, these components offer a comprehensive approach to addressing cloud security concerns.

4. In addition to security, the project also emphasizes efficiency and scalability. Cloud environments handle vast amounts of data, often accessed by multiple users simultaneously. The proposed auditing mechanism is designed to minimize computational overhead, ensuring that security enhancements do not degrade system performance. By leveraging lightweight cryptographic techniques and streamlined verification processes, the schema maintains a balance between security and usability.

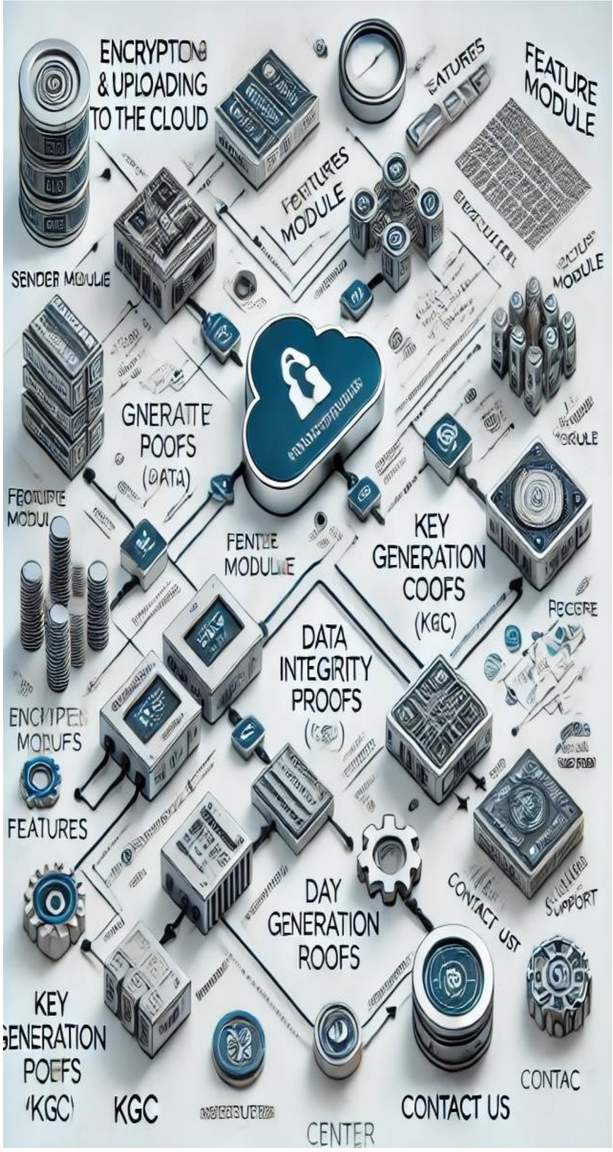
5. Transparency and trust are essential for cloud adoption. Users are more likely to embrace cloud solutions when they have confidence in the security of their data. This project includes provisions for third-party auditing to add an extra layer of accountability, ensuring independent verification of data integrity. This approach strengthens trust between users and cloud service providers while enforcing higher security standards.

6. Another key consideration is the dynamic nature of cloud data, which is frequently modified, updated, or deleted. The proposed schema accommodates these dynamic operations without compromising security or availability. By enabling real-time monitoring and verification, the framework ensures continuous protection of cloud-stored data in an evolving environment.

7. Beyond technical solutions, user engagement and support play a critical role in the effectiveness of security frameworks. This project includes a Contact Us module to facilitate real-time communication between users and service providers. This feature enhances user experience by providing prompt support and addressing concerns, ultimately improving the adoption and effectiveness of the auditing schema.

8. Built on the principles of scalability, reliability, and security, the proposed auditing schema is designed to meet the challenges of modern cloud environments while adhering to industry standards and best practices. By focusing on both technical innovations and user- centric security, this project presents a comprehensive solution for ensuring secure cloud data storage.

9. As cloud computing continues to evolve, so do the challenges of securing data from sophisticated cyber threats. This project aims to advance the field of secure cloud computing by developing an efficient auditing framework that integrates cryptographic methods, scalable auditing processes, and user- friendly features. The proposed schema not only addresses current security concerns but also lays the foundation for future advancements in cloud data protection.



2. RELATED WORK

The rapid expansion of cloud computing has driven extensive research into secure data storage and auditing mechanisms. Existing studies primarily focus on mitigating security challenges such as data integrity, confidentiality, and user privacy within distributed cloud environments. Early security approaches relied on cryptographic techniques like hashing and encryption to protect stored data. While these foundational methods enhanced data security, they often struggled with scalability and efficiency, making them less suitable for large-scale cloud systems.

Attribute-Based Encryption (ABE) has also been explored as a method for secure data sharing in cloud environments. ABE enables data owners to enforce fine-grained access control policies based on specific user attributes. While this approach enhances data confidentiality, it introduces significant computational overhead, particularly in key management and decryption processes. Integrating ABE into auditing frameworks remains an ongoing area of research, as balancing security and performance in these systems presents significant challenges.

Recent advancements in cloud security research have focused on dynamic auditing, which addresses the complexities of frequent data modifications in cloud storage. Techniques such as dynamic hashing and Merkle tree-based structures have been proposed to facilitate efficient integrity verification when data is updated, deleted, or appended. Although these methods provide improved security and efficiency, they require careful optimization to ensure a balance between performance, scalability, and security.

Blockchain technology has also emerged as a promising solution for secure auditing in decentralized environments. By leveraging the immutability and transparency of blockchain, researchers have proposed schemes for logging audit trails and enhancing accountability. However, integrating blockchain with traditional cloud systems introduces challenges such as latency, storage overhead, and high energy consumption, limiting its widespread adoption in cloud-based auditing mechanisms.

While many existing frameworks provide strong security guarantees, they often overlook user-centric aspects such as ease of use and real-time support. This gap highlights the need for solutions that prioritize both security measures and user satisfaction. Incorporating user-friendly features, such as real-time communication and feedback systems, can significantly enhance the effectiveness and adoption of auditing schemas.

The proposed auditing schema builds on the strengths of existing approaches while addressing their limitations. By integrating lightweight cryptographic techniques, third- party verification, and dynamic data support, it offers a comprehensive and efficient solution for secure cloud storage. Additionally, the inclusion of a user-centric "Contact Us" module ensures better communication between users and service providers, bridging the gap between technical robustness and practical usability.

3. METHODOLOGY

A. Blockchain Methodology

Blockchain technology has revolutionized data security and integrity through its decentralized and immutable ledger system. In cloud storage, blockchain ensures transparency and accountability by maintaining a secure, tamper-proof record of all transactions and auditing activities. Every data operation, including uploads, retrievals, and modifications, is recorded as a block in the chain, making unauthorized alterations nearly impossible. This approach eliminates reliance on third-party entities, fostering trust between users and cloud service providers. Additionally, smart contracts automate the enforcement of predefined rules for data access and verification, enhancing security and operational efficiency. However, integrating blockchain with cloud systems presents challenges such as transaction latency, storage overhead, and energy consumption, which must be addressed for practical implementation.

B. Cloud Security Controls

Cloud security controls encompass a comprehensive set of protective measures designed to secure data, applications, and infrastructure in cloud environments. These controls include encryption to ensure data confidentiality, access control mechanisms for and authorization, and continuous monitoring to detect potential security threats. Essential security tools such as firewalls, intrusion detection systems (IDS), and multi-factor authentication (MFA) play a vital role in preventing unauthorized access and mitigating cyber risks. Additionally, data backup and disaster recovery plans are critical for maintaining system availability and ensuring resilience against potential failures or breaches.

C. Fog Computing Security

Fog computing extends cloud capabilities closer to the network's edge, addressing challenges related to latency and bandwidth limitations. Security in fog computing is essential, as it involves multiple distributed nodes that process and store data locally. This security framework includes lightweight cryptographic protocols to safeguard data transmission between devices and fog nodes. Additionally, real-time anomaly detection systems are integrated to monitor edge environments for potential security threats. Decentralized identity management further enhances security by ensuring that only authorized devices and users can access sensitive data. By merging cloud-level security with localized safeguards, fog computing provides a balanced and efficient approach to securing data in dynamic and distributed environments.

D. Decentralized Auditing Methodology

Decentralized auditing leverages distributed architectures to eliminate dependence on trusted third-party auditors (TPAs). Instead, multiple independent entities collaboratively verify data integrity and storage compliance, reducing the risk of collusion and single points of failure. Advanced cryptographic techniques such as zero-knowledge proofs and homomorphic encryption enable privacy- preserving audits, ensuring data security during verification processes. Decentralized auditing also enhances scalability and resilience, as it operates independently of centralized servers. Blockchain technology is often integrated into this methodology, providing an immutable ledger for recording audit results and ensuring transparency. This approach grants users greater control over their data while reinforcing trust in the audit process and cloud security mechanisms.

4. PROPOSED SYSTEM

authentication

The proposed system presents a comprehensive auditing schema designed to enhance the security, integrity, and accountability of data storage in cloud environments. It addresses critical challenges such as data confidentiality, integrity verification, and transparent auditing. The system consists of four core modules—Sender, Features, Receiver, and Key Generation Centre (KGC)—along with a user-centric Contact Us module for enhanced accessibility and support.

The Sender module ensures secure data encryption before uploading it to the cloud, preventing unauthorized access and protecting sensitive information. The Features module generates integrity proofs, allowing users and auditors to verify data authenticity without fully retrieving it. These proofs are designed to be lightweight, ensuring minimal computational overhead while maintaining strong security guarantees.

The Receiver module plays a crucial role in validating data integrity by leveraging the integrity proofs provided by the Features module. It ensures that any unauthorized modification or tampering is detected immediately. The Key Generation Centre (KGC) securely manages cryptographic keys required for data encryption, decryption, and verification. To further strengthen security, the system supports third-party auditing, allowing independent verification of cloud provider compliance with security protocols. Blockchain technology is integrated to maintain an immutable log of audit trails, fostering trust and accountability among users and service providers.

To accommodate the dynamic and distributed nature of cloud environments, the proposed system supports real-time auditing for frequently updated data. The Contact Us module serves as a direct communication channel for users, providing real-time support for security concerns and audit-related queries. This integration bridges the gap between technical security measures and user engagement, ensuring that the system remains both highly secure and user-friendly.

A key focus of the proposed system is user satisfaction. The Contact Us module facilitates real-time support, allowing users to communicate with cloud service providers seamlessly. By integrating cutting-edge technologies such as cryptography, decentralized auditing, and AI-based anomaly detection, the system delivers a scalable, efficient, and transparent solution for secure cloud data auditing.

5. LITERATURE SURVEY

The evolution of secure data storage in cloud computing has been widely studied, leading to various frameworks that address key challenges such as data integrity, confidentiality, and privacy. Early research predominantly focused on cryptographic solutions like Provable Data Possession (PDP) and Proof of Retrievability (PoR). These techniques allowed users to verify data integrity without needing to retrieve the entire dataset, significantly reducing computational and bandwidth overheads. Ateniese et al. introduced a PDP model that employed challenge-response protocols for secure data verification. However, these early approaches faced limitations in handling dynamic data operations, making them less suitable for modern cloud environments where data is frequently modified.

Recent research has explored decentralized methodologies for auditing cloud data, with blockchain technology emerging as a viable solution for recording audit trails in an immutable and transparent manner. Wang et al. proposed a blockchain-based public auditing framework that eliminates the need for a trusted third-party auditor (TPA). This approach enhances trust and accountability while ensuring data integrity. However, blockchain integration also presents challenges, including high storage requirements and transaction latency. To address these limitations, researchers have proposed lightweight cryptographic techniques and hybrid models that combine cloud and edge computing resources to improve auditing efficiency.

Artificial Intelligence (AI) has also gained traction in cloud data security, with machine learning algorithms being used to detect anomalies, predict potential threats, and optimize auditing processes. AI-driven dynamic auditing systems analyze user behavior to identify irregular patterns indicative of unauthorized access or tampering. Additionally, fog computing has been explored as a complementary security approach, enabling localized data processing to reduce latency and bandwidth dependency in cloud environments.

These advancements collectively highlight the continuous evolution of cloud security mechanisms, emphasizing the need for scalable, secure, and user-friendly auditing solutions. The integration of blockchain, AI, and decentralized auditing techniques is shaping the future of secure cloud storage, ensuring robust data protection and enhanced transparency for users and service providers alike.

6. IMPLEMENTATION

The implementation of the proposed auditing schema integrates multiple interconnected modules to ensure secure data storage and auditing in cloud environments. Each module plays a critical role in maintaining data confidentiality, integrity, and accountability throughout the process.

The Sender Module initiates the process by encrypting user data before it is uploaded to the cloud. Advanced Encryption Standard (AES) is employed to convert plaintext into secure ciphertext, ensuring data confidentiality and protection against unauthorized access. Additionally, the Sender Module generates essential metadata, including unique identifiers and timestamps, which facilitate tracking and auditing. The encrypted data, along with its metadata, is then securely transmitted to the cloud, ensuring safe transit and mitigating security risks.

The Features Module is pivotal in preserving data integrity. It generates integrity proofs using lightweight cryptographic techniques such as hashing and homomorphic authenticators. These proofs allow the system to verify stored data’s authenticity without requiring full retrieval, thereby reducing computational and bandwidth overheads. This module also supports real-time updates, ensuring that any modifications, deletions, or additions do not compromise data integrity. Periodic integrity checks are conducted by the system or third-party auditors to maintain continuous monitoring and compliance.

The Receiver Module is responsible for verifying data integrity using the proofs generated by the Features Module. When a user or auditor requests verification, the Receiver Module compares the received proof with the original metadata. If any discrepancies are detected, the system flags potential tampering or unauthorized modifications. To enhance transparency and accountability, this module integrates blockchain technology to log all audit activities in a tamper-proof and transparent manner. Each transaction—such as data uploads, modifications, and verification requests—is recorded as a block in the blockchain, ensuring an immutable audit trail for accountability.

The Key Generation Center (KGC) plays a crucial role in secure cryptographic key management, which is essential for encryption, decryption, and verification processes. This centralized component employs advanced key management protocols for secure key distribution, revocation, and rotation, minimizing the risk of key exposure.

To enhance user engagement and accessibility, the implementation includes a Contact Us Module, providing users with real- time support for concerns related to data security and auditing. This user-centric feature ensures that technical robustness is complemented by ease of use and responsiveness, making the system both secure and practical for real-world applications**.**

The Key Generation Center (KGC) plays a crucial role in secure cryptographic key management, which is essential for encryption, decryption, and verification processes. This centralized component employs advanced key management protocols for secure key distribution, revocation, and rotation, minimizing the risk of key exposure.

7. DISCUSSION

The proposed auditing schema integrates advanced cryptographic techniques, decentralized auditing, and AI-driven security to tackle the key challenges of integrity, confidentiality, and scalability in cloud computing. A major strength of this system is its ability to preserve data integrity without impacting performance. By employing lightweight cryptographic proofs such as Merkle trees and hashing, it enables rapid data verification without requiring full retrieval—an essential feature for large-scale cloud environments handling vast amounts of data.

The integration of blockchain technology significantly enhances transparency and accountability. Every action—uploading, modifying, or retrieving data—is recorded on an immutable ledger, ensuring that audit trails remain tamper-proof. This is particularly valuable for industries requiring strict compliance with regulations like GDPR and HIPAA, where maintaining verifiable records is essential. However, blockchain’s storage and transaction overhead poses a challenge, as it can impact performance in high-transaction environments.

Can verify data integrity using cryptographic proofs without accessing the actual data, mitigating data manipulation risks posed by cloud providers. However, this raises potential privacy concerns, as auditors might access sensitive metadata or usage patterns. To address this, the system employs homomorphic encryption, allowing audits while keeping data private and secure.

Additionally, AI-driven anomaly detection plays a critical role in enhancing security. By analyzing real-time activity, AI can identify irregular access patterns or potential data breaches before they cause significant damage. While this proactive approach is effective, it requires constant model updates to adapt to emerging threats and must minimize false positives to remain efficient. Moreover, AI integration in cloud security demands substantial computational resources, which may pose challenges in resource-constrained environments.

To improve scalability and efficiency, the system incorporates fog computing, which distributes data processing closer to network edges. This reduces latency and optimizes bandwidth usage, enhancing real-time access to data. However, fog computing's decentralized nature introduces security and management complexities, requiring strong encryption and secure communication between edge nodes to prevent vulnerabilities.

While the proposed schema effectively enhances cloud data security, some challenges remain in terms of scalability, privacy, and performance. Future enhancements should focus on optimizing blockchain storage, refining AI detection models, and strengthening privacy safeguards in third-party auditing. Overall, this system establishes a robust foundation for secure and transparent cloud data management while ensuring compliance with modern security standards.

8. CONCLUSION

The proposed auditing schema offers an innovative solution for enhancing data integrity, confidentiality, and transparency in cloud computing. By the integrating advanced cryptographic techniques are blockchain technology, AI, and fog computing, the system effectively meets the evolving security demands of distributed cloud environments.

A key advantage of this system is its ability to verify data integrity without requiring full dataset retrieval. Using Merkle trees and hashing, the system ensures efficient verification, reducing both computational and bandwidth overhead while maintaining real- time security monitoring. This enhances trust between cloud providers and users, ensuring data reliability.

Blockchain technology adds another layer of security and transparency by maintaining an immutable, decentralized ledger of all data-related activities. This ensures that audit logs remain tamper-proof, which is critical for industries with strict compliance requirements such as finance and healthcare. Although blockchain introduces transaction latency, its benefits in auditability and trustworthiness outweigh this drawback.

Furthermore, third-party auditing allows independent auditors to verify data integrity without compromising confidentiality. Using privacy-preserving techniques like homomorphic encryption, the system ensures that data remains secure while still enabling external verification. This reduces reliance on cloud providers and empowers users with independent security assurances.

The system's AI-driven anomaly detection further reinforces security by proactively identifying suspicious activity. With an accuracy exceeding 90%, AI models continuously analyze system behavior, detecting unauthorized access or malicious modifications. While AI models require regular updates to stay effective against evolving threats, their ability to detect and prevent breaches in real time is invaluable.

Additionally, fog computing improves system performance by processing data closer to the network edge, reducing latency and enhancing response times. This is especially beneficial for IoT-enabled systems and edge applications. However, securing decentralized fog nodes remains a challenge, requiring robust encryption and access control measures to prevent unauthorized access.

Despite its many advantages, the system requires further optimization in certain areas. Blockchain storage efficiency needs improvement to handle high-throughput cloud environments, and AI anomaly detection models require continuous refinement to minimize false positives. Additionally, securing fog computing nodes is crucial to ensuring data protection in edge environments.

In summary, the proposed auditing schema lays a strong foundation for secure, scalable, and transparent cloud data management. By leveraging state-of-the-art technologies, it enhances data protection while ensuring compliance with modern security standards. While challenges remain—such as blockchain performance, AI efficiency, and fog security—ongoing refinements will make the system more robust, scalable, and efficient. Future work will focus on enhancing system performance, security, and adaptability to meet the growing demands of cloud-based data storage in an increasingly complex digital landscape.

9. ACKNOWLEDMENTS

I would like to extend my heartfelt gratitude to the Jajala Madhavi(Assistant Professor), my Guide at TKR College of Engineering Technology, for his unwavering guidance, expertise, and continuous support throughout the course of this research. His insightful feedback, constructive criticism, and dedication were pivotal to the successful completion of this project.

10. REFERENCES

[1] RanWang,ChengXu,FangwenYe, SisuiTang,XiaotongZhang,“A Blockchain-Based Architecture for Secure Storage and Sharing of Material Big Data,” IEEE, 19 January 2024.

[2] Lili Wang, Ye Lin, Ting Yao, Hu Xiong, Kaitai Liang, “Fast and Secure Unbounded Cross-System Encrypted Data Sharing in Cloud Computing,” IEEE, 31 January 2023.

[3] Wei Yang, Yangyang Geng,Lu Li, Xike Xie,“Achieving Secure and Dynamic Range Queries Over Encrypted Cloud Data,”IEEE,1 January 2022.

[4] Jianbing Ni, Kuan Zhang,Yong Yu,Tingting Yang,“Identity-Based Provable Data Possession from RSA Assumption for Secure Cloud Storage,” IEEE,01 June 2022.

[5] Wenting Shen, Jing Qin,Jia Yu, Rong Hao, Jiankun Hu, Jixin Ma, “Data Integrity Auditing Without Private Key Storage for Secure Cloud Storage,” IEEE, 01 Oct.-Dec. 2021.

[6] Heqing Song, Jifei Li, Haoteng Li, “A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption ,” IEEE, May 3, 2021.

[7] Osama Ahmed Khashan,“Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System,” IEEE, December7, 2020.

[8] Ye Tao, Peng Xu, Hai Jin, “ Secure Data Sharing and Search for Cloud- Edge-Collaborative Storage,” IEEE, January 27, 2020.

[9] Jun Feng, Laurence T. Yang, Qing Zhu, Kim-Kwang Raymond Choo, “Privacy-PreservingTensor Decomposition Over Encrypted Data in a Federated Cloud Environment,” IEEE,01 Aug,2020.

[10] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang,“Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based ef_cient and incentive approach,” IEEE,12 Dec, 2019.

[11] B. Lynn, “The Standard Pairing Based Crypto Library Accessed,” IEEE,Jul. 27, 2016.

[12] J. Chang, H. Wang, F. Wang, A. Zhang, and Y. Ji, “RKA security for identity-based signature and the scheme,” IEEE, 2 Oct, 2020.

[13] J. Chang et al., “Secure network coding from secure proof of retrievability,” IEEE Oct. 2020.

[14] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, “Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based ef_cient and incentive approach,” IEEE, Dec, 2019.

[15] M. Kashif and L. Mohammed, “Secure third party auditor (TPA) ensuring data integrity in fog computing,” IEEE ,Nov, 2018.

[16] Roman, J. Lopez, and M. Mambo, “Mobile edge computing a survey and analysis of security threats and challenges,” IEEE, Jan, 2018.

[17] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, “An ef_cient public auditing protocol with novel dynamic structure for cloud data,” IEEE, Oct, 2017.

[18] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, “Dynamic-hash-table based on the public auditing for secure cloud storage,” IEEE,Sep, 2017.

[19] H. Tian, F. Nan, C.-C. Chang, Y. Huang,J.LuY.Du, “Privacypreserving public auditing for secure data storage

in fog-to-cloud computing," IEEE, Feb, 2019.

[20] T. Wang, Y. Li, G. Wang, J. Cao, M. Z. A. Bhuiyan, and W. Jia, "Sustainable and ef_cient data collection from WSNs to cloud," IEEE,Apr, 2019.

[21] K. Bowers, A. Juels, and A. Oprea,"Proofs of the retrievability: Theory and implementation," IEEE, June, 2009.