JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain-Assisted Verifiable and Secure Remote Sensing Image Retrieval in Cloud Environment

Dr. C. DASTAGIRAIAH - Assistant Professor, Department of Computer Science, Anurag University,
SAI KETHAN BHARADWAJ KANITHI - Student, Department of Computer Science, Anurag University
DHAROOR VINAY KUMAR - Student, Department of Computer Science, Anurag University
M. SHREYA - Student, Department of Computer Science, Anurag University

Abstract

Secure retrieval of remote sensing images in an outsourced cloud environment garners considerable attention. Since the cloud service provider (CSP) is considered as a semi trusted third party that may return incorrect retrieval results to save computational resources or defraud retrieval fees for profit, it becomes a critical challenge to achieve secure and verifiable remote sensing image retrieval. This article presents a secure retrieval and blockchain-assisted verifiable scheme for encrypted remote sensing images in the cloud environment. In response to the characteristic that geographical objects in remote sensing images with clear category attributes, we design a remote sensing image retrieval method to facilitate secure and efficient retrieval. In addition, we propose a verifiable method combined with blockchain and Merkle trees for checking the integrity and correctness of the storage and retrieval services provided by CSP, which can replace the traditional third-party auditor. The security analysis and experimental evaluation demonstrate the security, verifiability, and feasibility of the proposed scheme, achieving secure remote sensing image retrieval while preventing malicious behavior of CSP.

1. INTRODUCTION

The number of remote sensing images has reached a petabyte level due to the growing volume and variety of satellites [1], placing a significant burden on users' storage and processing resources. At the same time, with the fast development of cloud computing, users with limited resources commonly employ cloud service providers (CSPs), which provide outsourced solutions and content-based remote sensing image retrieval [2], [3], [4].

However, as a semi trusted third party, CSP may illegally gather image information from users while providing retrieval services [5]. Because remote sensing images depict the distribution patterns and evolution patterns of morphological information, they expose highly sensitive data, such as resources and geographic locations. A data leak would cause various image security concerns and huge economic losses for users. For the sake of data protection, remote sensing images are encrypted before outsourcing to prevent CSP from gathering image information [6]. There are already some secure image retrieval schemes in the cloud environment, including randomized feature protection [7], homomorphic encryption [8], robust hash [9], bag-of-encrypted-words (BOEW) model [10], and secure multiparty computing [11], etc. Encryption makes a security paradigm available for outsourced data, but here is another fundamental challenge: How can we ensure that CSP can provide correct storage and retrieval services in the encrypted environment? The primary cause of such an issue is that image owner

and retrieval users will lose control of their data if images are outsourced to CSP, resulting in CSP returning incomplete or incorrect retrieval results to save computational resources or defraud retrieval fees for profit. CSP withholds technical proof from users, leaving users unable to verify whether CSP is truly providing services that meet their expectations [12].

In response to the drawbacks of semi trusted CSP, a traditional and straightforward option is to incorporate a third-party auditor (TPA) to verify that the CSP is providing services truthfully. For example, in the public auditable verification schemes [13], [14], it assumes that the TPA is unbiased and delegates it to evaluate the services of CSP. This may seem like an appropriate strategy, but only if the TPA is trusted without doubt. However, the truth is that TPA operates in a black box, with users not knowing its internal working procedures in reality [14],[15]. The TPA serves as a centralized third party, and its compromise may result in the termination of the entire verification service. Moreover, the TPA and CSP may collude to provide a mendacious verification report, i.e., regardless of the correctness of the services provided by the CSP, the TPA will report accurate verification results to the users.

Fortunately, blockchain technology provides a new perspective for the verification of data. As an excellent candidate for a trusted entity, the blockchain is a decentralized, nontempering, and traceable distributed ledger technology. In the blockchain, each participating full node saves replication to jointly maintain the integrity of the data, and the data structure of chained hashing and consensus algorithms ensures that data cannot be arbitrarily deleted or altered [16]. Therefore, blockchain technology ensures the integrity, reliability, and verifiability of the on-chain data, preventing the malicious behaviors of CSP or TPA mentioned above. However, the current technical architecture of the blockchain can hardly meet the existing verification methods [17]. Since each full node of the blockchain backs up the complete ledger, storing a large amount of verification data on the storage-constrained blocks will result in huge data size and high storage overhead. Furthermore, most of the verifiable schemes focus on data integrity, and several works focus on data integrity in cloud storage, such as the works of [3], [18], [19]. Moreover, the well-known distributed cloud storage commercial platforms such as Storj [20], Sia [21], and File coin [22], verify the integrity of stored data by filing metadata on blockchain. However, in a real-world image retrieval scenario, it is necessary to consider not only the integrity of the cloud-stored data, but also the correctness of the retrieved results and the correctness of the similarity ranking of the returned images. Therefore, we emphasize the integrity of data and the correctness of retrieval services.

1.2 Scope of the Project:

The project focuses on addressing the security and reliability challenges associated with remote sensing image retrieval in cloud environments. With the proliferation of satellite data leading to petabyte-level storage demands, users increasingly rely on cloud service providers (CSPs) for image storage and retrieval. However, concerns arise regarding the potential unauthorized access and manipulation of sensitive image data by semi trusted CSPs. To mitigate these risks, the project explores the integration of blockchain technology, leveraging its decentralized and tamper-resistant nature to ensure data integrity, reliability, and verifiability. By emphasizing the importance of both data integrity and the correctness of retrieval services, the project aims to develop a robust solution that enables secure and efficient remote sensing image retrieval while safeguarding against potential malicious behavior from CSPs and third-party auditors.

2. LITERATURE SURVEY

The literature survey encompasses the evolving landscape of remote sensing image retrieval within cloud environments, navigating the challenges of security and reliability. With satellite data reaching petabyte levels, users increasingly rely on Cloud Service Providers (CSPs) for outsourced solutions, including image retrieval. However, the semi-trusted nature of CSPs raises concerns regarding illicit data aggregation during retrieval services. Existing secure retrieval schemes, including encryption and third-party auditors, strive to address these challenges but face limitations in ensuring the accuracy of storage and retrieval services. Blockchain technology emerges as a transformative solution, offering decentralized and immutable data verification. While current blockchain architectures encounter scalability issues, leveraging blockchain for integrity verification presents opportunities to enhance data integrity and retrieval service correctness in cloud-

based image retrieval scenarios.

Tamiminia et al. [1] conducted a meta-analysis and systematic review on the utilization of Google Earth Engine for geo-big data applications, shedding light on its implications for remote sensing. Their study provides valuable insights into the potential of Google Earth Engine in handling large-scale geo-big data, which is particularly relevant for remote sensing applications where vast amounts of data need to be processed and analyzed efficiently.

Gao et al. [2] proposed a secure cloud-aided object recognition system for hyperspectral remote sensing images, with a focus on ensuring data security in cloud-assisted image processing. Their work addresses the critical need for secure and reliable processing of hyperspectral imagery, which is increasingly used in various remote sensing applications such as agriculture, environmental monitoring, and disaster management.

Zhao et al. [3] introduced a blockchain-based privacy-preserving scheme for remote data integrity checking in IoT information systems. By leveraging blockchain technology, their scheme aims to ensure data integrity in IoT environments, where data authenticity and trustworthiness are paramount. This research highlights the role of blockchain in enhancing data security and integrity in IoT applications.

Sukhia et al. [4] explored content-based remote sensing image retrieval using multi-scale local ternary patterns, contributing to the development of efficient retrieval techniques. Their work focuses on improving the accuracy and efficiency of image retrieval systems, which are essential for extracting relevant information from large repositories of remote sensing imagery.

Zhu et al. [5] addressed the challenge of generic, verifiable, and secure data search in cloud services, proposing mechanisms to ensure data integrity and security. Their research emphasizes the importance of verifiability and security in cloud-based data search systems, which are vulnerable to various security threats such as data breaches and unauthorized access.

Tong et al. [6] presented VFIRM, a verifiable fine-grained encrypted image retrieval scheme, enhancing the security of image retrieval in multi-owner multi-user settings. Their work focuses on addressing the security challenges associated with encrypted image retrieval, ensuring that sensitive image data remains protected even in shared storage environments.

Lu et al. [7] introduced a secure image retrieval method focusing on feature protection, aiming to safeguard image features during retrieval processes. Their research contributes to the development of secure image retrieval techniques, which are essential for protecting sensitive image data from unauthorized access and manipulation.

Zhang et al. [8] proposed a secure image retrieval approach based on homomorphic encryption, ensuring data confidentiality and privacy in cloud computing environments. Their work addresses the privacy concerns associated with cloud-based image retrieval systems, providing a secure solution for protecting sensitive image data from unauthorized access.

Weng et al. [9] developed a privacy-preserving framework for large-scale content-based information retrieval, emphasizing the importance of data privacy in retrieval systems. Their research highlights the need for privacy-enhancing techniques in information retrieval systems, which handle vast amounts of sensitive data that require protection from unauthorized access.

Xia et al. [10] proposed BOEW, a content-based image retrieval scheme utilizing bag-of-encrypted-words, contributing to secure retrieval in cloud environments. Their work focuses on enhancing the security of image retrieval systems, particularly in cloud-based environments where data confidentiality and privacy are critical considerations.

Shen et al. [11] addressed content-based multi-source encrypted image retrieval in clouds with privacy preservation, offering insights into privacy-enhanced retrieval mechanisms. Their research focuses on preserving the privacy of sensitive image data in cloud-based retrieval systems, ensuring that user data remains protected from unauthorized access and disclosure.

3. OVERVIEW OF THE SYSTEM

3.1 Existing System

In the existing system, secure content-based image retrieval (CBIR) frameworks typically consist of two main modules: feature protection and

feature similarity measurement. Feature protection involves extracting image features and encrypting them using encryption techniques to ensure that the encrypted feature descriptors can be utilized for retrieval calculations. Traditional hand-crafted features or deep learning network features are commonly used to represent the visual content of remote sensing images. Deep learning networks, in particular, have shown superior performance in recognizing essential image features, making them a feasible and advantageous choice for remote sensing image retrieval.

3.1.1 Disadvantages of Existing System

Computational Overhead: Homomorphic encryption typically involves complex mathematical operations, which can result in increased computational overhead compared to traditional encryption techniques. This may lead to higher processing times and resource utilization, potentially impacting system performance, especially in resource-constrained environments.

Implementation Complexity: Integrating homomorphic encryption into the image retrieval framework requires careful design and implementation, as well as expertise in cryptographic techniques. Developing and maintaining such a system may be challenging and require specialized knowledge, leading to higher development costs and complexity.

Potential Compatibility Issues: Homomorphic encryption may not be compatible with all existing systems or platforms, requiring modifications or upgrades to ensure seamless integration. This could introduce compatibility issues with legacy systems or third-party applications, necessitating additional effort for deployment and interoperability.

3.2 Proposed System

In the proposed system, a novel approach is introduced to address these limitations. Despite existing methods having low computational complexity, they may not adequately protect the original feature information, leading to insufficient retrieval performance. To mitigate these issues, a secure image retrieval method based on homomorphic encryption is proposed. Homomorphic encryption allows computation on encrypted data without decrypting it, enhancing both security and performance in retrieval tasks.

3.2.1 Advantages of Proposed System

Enhanced Security: By employing homomorphic encryption, the proposed system ensures that image features are securely encrypted, protecting sensitive information from unauthorized access or tampering. This enhances the overall security of the image retrieval process, reducing the risk of data breaches or privacy violations.

Improved Retrieval Performance: Homomorphic encryption allows for secure computation on encrypted data without the need for decryption, thereby preserving the confidentiality of image features while enabling efficient retrieval calculations. This can lead to improved retrieval performance compared to existing methods that may compromise feature information during encryption.

Versatility: Homomorphic encryption is a flexible cryptographic technique that supports various retrieval operations without compromising data privacy. The proposed system can accommodate different retrieval tasks and scenarios, making it suitable for a wide range of applications in remote sensing image retrieval.

3.3 Proposed System Design

In this project work, there are Five modules and each module has specific functions, they are:

1. User
2. Cloud Server
3. User
4. Key Management
5. Retravel User

3.3.1 USER

Using this module mobile user can register with application and login with valid username and password. User will get key from key management to login upload image and encrypt data and send to cloud server with block chain for attribute. User can view data and send to cloud.

3.3.2 CLOUD SERVER

Using this module cloud server will login view data uploaded by user and view requests from retravel user and respond to message by send request to block and verify block chain and then send decryption key to retravel user.

3.3.3 BLOCK CHAIN SERVER

Using this module block chain server can login view requests from cloud server verify block chain and send confirmation to retravel user.

3.3.4 KEY MANAGEMENT

Using this module key management will login and view users authorize and send security key for login.

3.3.5 RETRAVEL USER

Using this module retravel user will register get key to login view encrypted data and send request to cloud server who will verify block chain for attribute if successful user will download data with key sent by cloud server.

3.4 Architecture

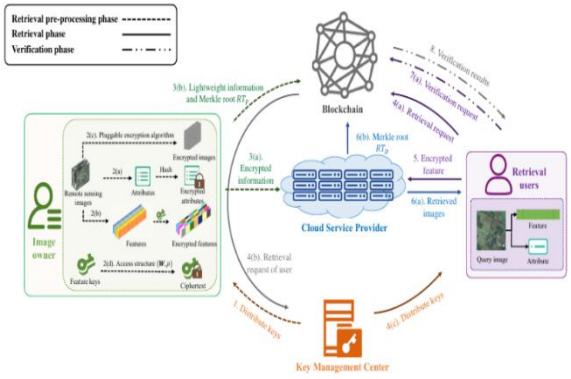
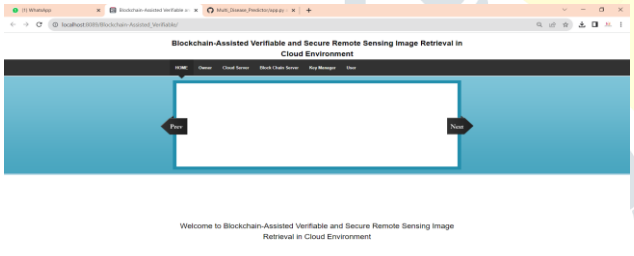
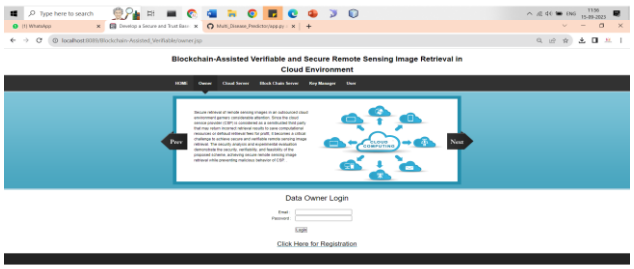
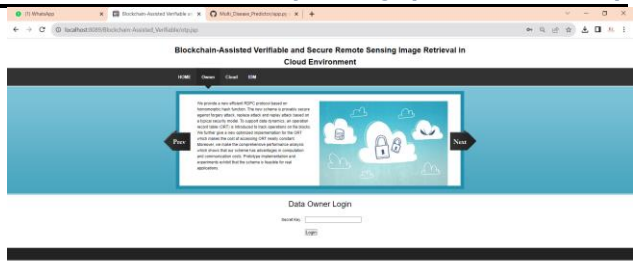


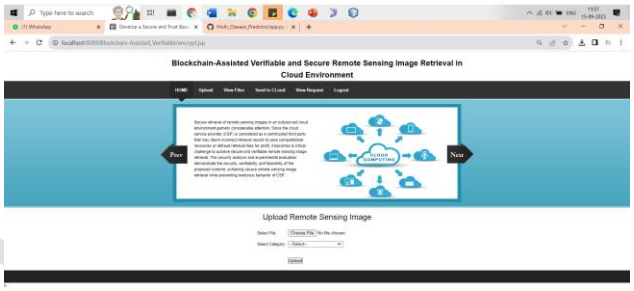
Fig 1: System Architecture

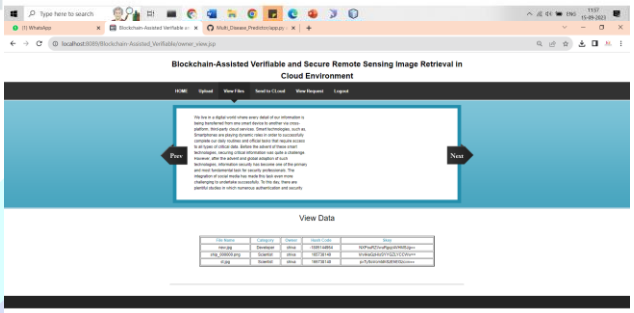
4. RESULT SCREEN SHOTS

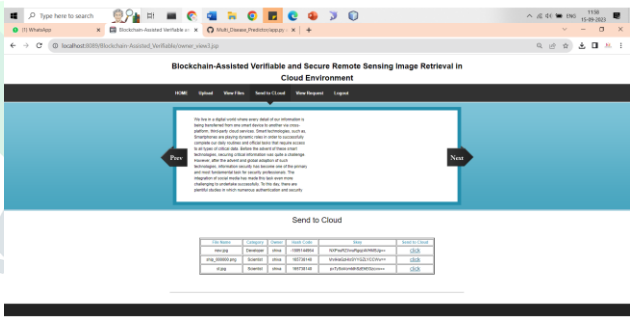


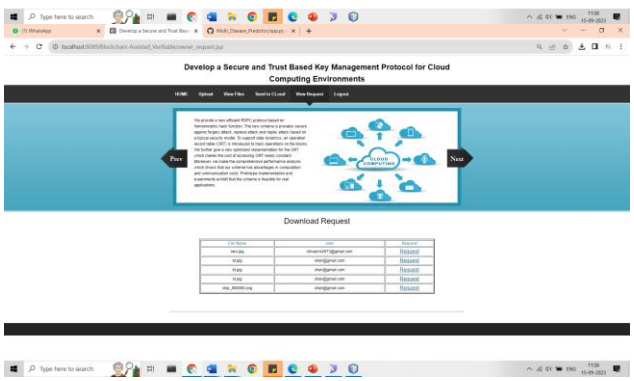


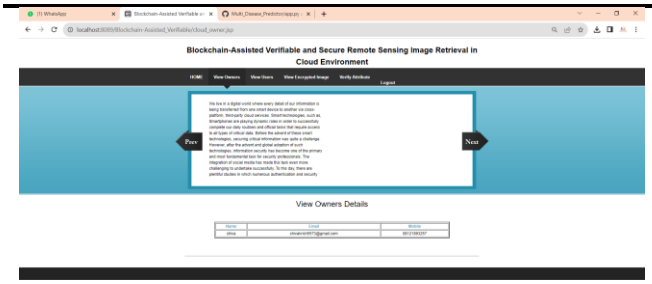


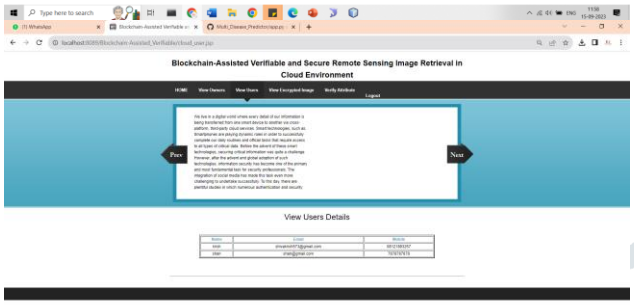


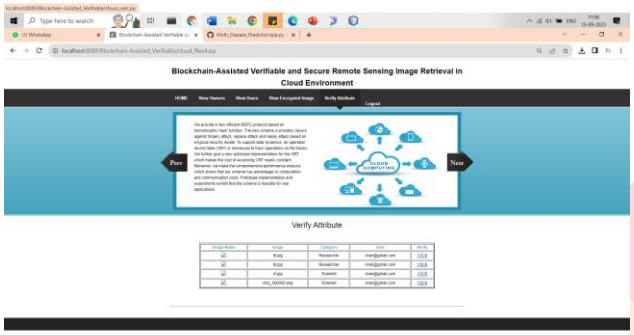


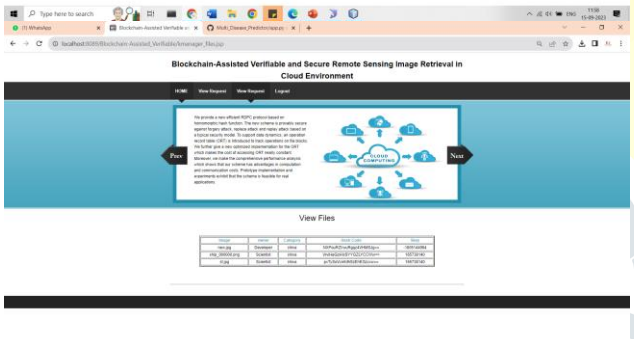


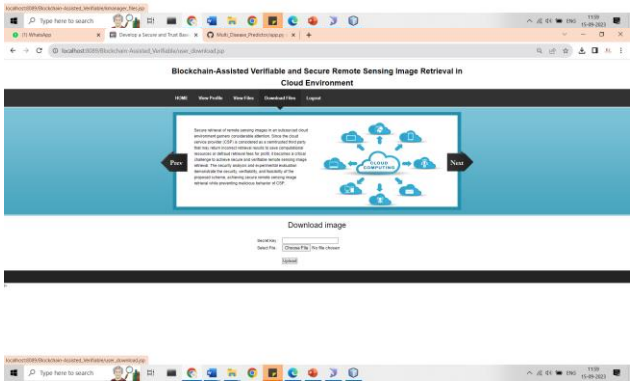












5. CONCLUSION

Your proposed blockchain-assisted verifiable and secure remote sensing image retrieval scheme in the cloud sounds intriguing! Leveraging blockchain technology to ensure the correctness and integrity of retrieval results is a novel approach, especially in the context of remote sensing images. Assigning geographical objects in remote sensing images as attributes and allowing the cloud service provider (CSP) to measure images with the same attributes as the query image can indeed enhance the efficiency of image retrieval. The incorporation of a blockchain-assisted verifiable method adds an extra layer of security and transparency, enabling users to verify the accuracy of retrieval results. Moreover, the ability to record any dishonest behavior by the CSP during retrieval services using the blockchain enhances accountability and trust in the system.

6. REFERENCES

[1] H. Tamiminia, B. Salehi, M. Mahdianpari, L. Quackenbush, S. Adeli, and B. Brisco, “Google earth engine for geo-big data applications: A metaanalysis and systematic review,” ISPRS J. Photogrammetry Remote Sens., vol. 164, pp. 152–170, 2020.

[2] P. Gao et al., “Secure cloud-aided object recognition on hyperspectral remote sensing images,” IEEE Internet Things J., vol. 8, no. 5, pp. 3287–3299, Mar. 2021.

[3] Q. Zhao, S. Chen, Z. Liu, T. Baker, and Y. Zhang, “Blockchain-based privacy-preserving remote data integrity checking scheme for iot information systems,” Inf. Process. Manage., vol. 57, no. 6, 2020, Art. no. 102355.

[4] K. N. Sukhia, M. M. Riaz, A. Ghafoor, and S. S. Ali, “Content-based remote sensing image retrieval using multi-scale local ternary pattern,” Digit. Signal Process., vol. 104, 2020, Art. no. 102765.

[5] J. Zhu, Q. Li, C. Wang, X. Yuan, Q. Wang, and K. Ren, “Enabling generic, verifiable, and secure data search in cloud services,” IEEE Trans. Parallel Distrib. Syst., vol. 29, no. 8, pp. 1721–1735, Aug. 2018.

[6] Q. Tong et al., “VFIRM: Verifiable fine-grained encrypted image retrieval in multi-owner multi-user settings,” IEEE Trans. Serv. Comput., vol. 15, no. 6, pp. 3606–3619, Nov./Dec. 2022.

[7] W. Lu, A. L. Varna, A. Swaminathan, and M. Wu, “Secure image retrieval through feature protection,” in Proc. IEEE Int. Conf. Acoust. Speech Signal Process., 2009, pp. 1533–1536.

[8] Y. Zhang, L. Zhuo, Y. Peng, and J. Zhang, “A secure image retrieval method based on homomorphic encryption for cloud computing,” in Proc. Int. Conf. Digit. Signal Process., 2014, pp. 269–274.

[9] L. Weng, L. Amsaleg, A. Morton, and S.

Marchand-Maillet, "A privacypreserving framework for large-scale content-based information retrieval," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 1, pp. 152–167, Jan. 2015.

[10] Z. Xia, L. Jiang, D. Liu, L. Lu, and B. Jeon, "BOEW: A content-based image retrieval scheme using bag-of-encrypted-words in cloud computing," IEEE Trans. Serv. Comput., vol. 15, no. 1, pp. 202–214, Jan./Feb. 2022.

[11] M. Shen, G. Cheng, L. Zhu, X. Du, and J. Hu, "Content-based multi-source encrypted image retrieval in clouds with privacy preservation," Future Gener. Comput. Syst., vol. 109, pp. 621–632, 2020.

[12] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, "The state of public infrastructure-as-a-service cloud security," ACM Comput. Surv., vol. 47, no. 4, pp. 1–31, 2015.

[13] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011.

[14] Y. Zhang, C. Xu, X. Lin, and X. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," IEEE Trans. Cloud Comput., vol. 9, no. 3, pp. 923–937, Sep. 2021.

[15] J. Li, J.Wu, G. Jiang, and T. Srikanthan, "Blockchain-based public auditing for Big Data in cloud storage," Inf. Process. Manage., vol. 57, no. 6, 2020, Art. no. 102382.

[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[17] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," IEEE Commun. Surv. Tut., vol. 21, no. 2, pp. 1508–1532, Secondquarter 2019.

[18] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in Proc. IEEE Int. Conf. Web Serv., 2017, pp. 468–475.

[19] T. Wu, G. Yang, Y. Mu, R. Chen, and S. Xu, "Privacy-enhanced remote data integrity checking with updatable timestamp," Inf. Sci., vol. 527, pp. 210–226, 2020.

[20] Storj Labs, "Storj: A decentralized cloud storage network framework," 2018. [Online]. Available: https://www.storj.io/storj.pdf

[21] D. Vorick and L. Champine, "Sia: Simple decentralized storage," 2014. [Online]. Available: https://sia.tech/sia.pdf

[22] Protocol Labs, "Filecoin: A decentralized storage network," 2017. [Online]. Available: https://filecoin.io/filecoin.pdf

[23] Z. Shao, W. Zhou, X. Deng, M. Zhang, and Q. Cheng, "Multilabel remote sensing image retrieval based on fully convolutional network," IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens., vol. 13, pp. 318–328, Jan. 2020.