IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304020 |

Strengthened File Auditing Framework for Cloud Servers with Secure Download Key Notifications

Ajinthan S[1], Arun Bharathi N[2], Vel Kumar K[3], Dr.S. Subha Shree[4]

U.G. Student, Department of Computer Science and Engineering, E.G.S.Pillay Engineering College, Nagapattinam, TamilNadu, India[1,2,3].

Assistant Professor, Department of Computer Science and Engineering, E.G.S.Pillay Engineering College, Nagapattinam, Tamilnadu, India[4].

ABSTRACT: Securing sensitive files stored on cloud servers presents a paramount challenge in today's digital landscape, demanding a robust file auditing mechanism that transcends traditional methods. This paper introduces an innovative approach to file auditing in cloud environments, distinguished by the integration of secure download key notifications with login processes. Unlike conventional file auditing techniques that primarily focus on monitoring file activities, this proposed solution recognizes the critical need for securely tracking file downloads. To address this gap, we present a sophisticated system that not only comprehensively audits file activities but also seamlessly integrates with login processes to provide secure download key notifications. By bridging the gap between file auditing and user authentication, our solution enhances the security posture of cloud-based file storage systems, empowering organizations to safeguard their sensitive data effectively. Through detailed analysis and evaluation, we demonstrate the efficacy and practicality of our approach in enhancing the security and integrity of sensitive files stored on cloud servers.

KEYWORDS: Cloud Server, Auditing, Data Effectively

I.INTRODUCTION

Cloud computing has revolutionized the way organizations store, manage, and access their data, offering unparalleled flexibility, scalability, and cost-effectiveness. With the increasing adoption of cloud-based services, the volume of data stored in the cloud continues to soar, encompassing a wide range of sensitive information, including proprietary business data, financial records, and personal information. However, alongside the benefits of cloud storage come significant security challenges, particularly concerning the protection of sensitive files from unauthorized access, manipulation, or theft. As organizations entrust their valuable data to third-party cloud service providers, ensuring robust security measures becomes imperative to mitigate risks and safeguard sensitive information.

File auditing emerges as a critical component of cloud security strategies, enabling organizations to monitor and track file activities to detect unauthorized access, unauthorized modifications, or other suspicious behaviors. Traditionally, file auditing has been conducted within on-premises IT environments, where organizations maintain full control over their infrastructure and security policies. However, the transition to cloud-based storage introduces new

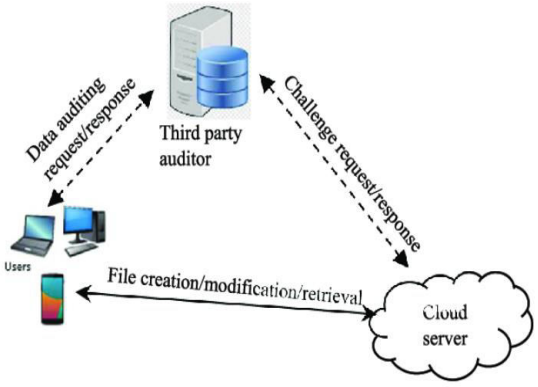
| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304020 |

complexities and considerations for file auditing, necessitating the development of innovative approaches and technologies to address emerging challenges.

The advent of cloud computing has revolutionized the way organizations manage and store their digital assets, offering unprecedented scalability, flexibility, and accessibility compared to traditional on-premises solutions. Cloud-based storage services, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, have become indispensable tools for businesses of all sizes, enabling them to store, share, and access vast amounts of data from anywhere, at any time. This shift towards cloud storage has been driven by a myriad of factors, including the exponential growth of data, the need for cost-efficient storage solutions, and the rise of remote work environments.



II. RELATED WORK

Liping Qiao; Yanping Li, Cloud storage has benefited millions of users with its remarkable advantages of economy and flexibility. Since a single cloud service provider is not always reliable and prone to a single point of failure, multi-cloud storage is proposed to enhance data availability. However, cross multiple clouds (cross-cloud) auditing to provide users with the integrity verification of outsourced data also faces many challenges, such as the fact that a large quantity of existing schemes rely heavily on the trusted third-party. Therefore, we propose a decentralized data storage and integrity auditing scheme for multi-cloud scenarios to eliminate the dependence on the third-party, namely BDDR, and an improved version iBDDR with stronger security. First, both BDDR and iBDDR adopt multi-cloud data storage and support batch auditing to greatly save computation costs. Second, our schemes not only get rid of a third-party, but also do not require a dispute arbitration since the outsourced data can be verified by cloud server providers via the homomorphic verifiable tags published on the blockchain. Third, locating the corrupted cloud server providers and accurately recovering the corrupted data at a lower communication and computation costs are supported. Finally, security and performance analyses demonstrate the security and effectiveness of our schemes.

Yanan Tian; Shichong Tan, With the prevalence of distributed network storage services, the security and dynamicity of cloud storage data have become essential focuses of attention. Meanwhile, research on secure deduplication, integrity audit, and dynamic operations has been extensively conducted. However, in existing research, many data deduplication schemes supporting auditing focus on static file storage. This paper proposes a blockchain-based dynamic data deduplication scheme that supports public auditing, enabling data's dynamic operations. In addition, the existing proof of ownership is designed only to meet the needs of the server. Therefore, we adopt BLS short signature to design a secure and efficient bidirectional proof of ownership mechanism, supporting the server and client to prove they have the same data. Based on this, we design a multi-server storage mechanism under the supervision of blockchain, which achieves public auditing without a trusted third party and supports block-level deduplication within a server and file-level deduplication across servers. Finally, we demonstrate the feasibility and performance of the proposed scheme through experimental analysis.

Shanshan Li; Chunxiang Xu, In this paper, we introduce a concept of transparent integrity auditing and propose a concrete scheme based on the blockchain, which goes one step beyond existing public auditing schemes, since the

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304020 |

auditing does not rely on third-party auditors while freeing users from heavy communication costs on auditing the data integrity. Then we construct a secure transparent deduplication scheme based on the blockchain that supports deduplication over encrypted data and enables users to attest the deduplication pattern on the cloud server. Such a scheme allows users to directly benefit from data deduplication and protects data content against anyone who does not own the data. Finally, we integrate the proposed transparent integrity auditing scheme and transparent deduplication scheme into one system, dubbed BLIND. We evaluate BLIND from security and efficiency, which demonstrates that BLIND achieves a strong security guarantee with high efficiency.

Ying Xie; Ke Huang; Sheng Yuan Internet of Things (IoT) revolutionizes data collection, especially in e-healthcare, where patients data from wearables and sensors improves medical services. However, IoT's limitations in computing and storage require cloud outsourcing. Combining IoT with the cloud has potential but raises concerns about data security. Leveraging cloud storage presents an attractive solution for accommodating the substantial volume of data outsourced by IoT devices. As the outsourcing of real-time data to cloud storage becomes commonplace, the adoption of data auditing schemes emerges as a means to ensure data integrity. To curtail operational expenses, various deduplication techniques are commonly employed on outsourced data, effectively sidestepping redundant data and resulting in storage and bandwidth efficiencies. Although real-time data typically remains distinct due to its diverse origins, scenarios, such as data sharing or trading in data-driven services and datamarkets, can lead to data redundancy. Moreover, in order to fortify against any potential information leakage, encryption is implemented prior to deduplication. Convergent encryption (CE) stands as a prominent exemplar of this approach. Effectively integrating data auditing, deduplication, and encryption for wireless sensor devices is no trivial task. To efficiently and securely accommodate data while authenticating them through a heterogeneous framework, we present a novel remote data checking scheme, denoted as the VRDC scheme. This scheme empowers IoT data to be encrypted, updated, deduplicated, and audited, aligning with the imperatives of security, privacy, and efficiency. Through comprehensive security analysis, we establish that our VRDC scheme is fortified against potential threats. Our experimental findings highlight the efficiency of our approach in the realms of auditing, deduplication, and updates. Furthermore, the evidence highlights the potential for optimization within our scheme when compared to related works. This is achieved through the careful management of dynamic update scales within a file.

Suresh Chavhan Owing to the increased worldwide awareness regarding pollution caused by the consumption of fossil fuels, Battery-powered vehicles are bound to take over the conventional Internal Combustion Engine. Keeping the difficulties faced by the economy of the city and the populace of adapting to an entirely grid-run charging infrastructure in mind, a framework incorporating electric vehicles to everything (EV2X) communication and Charge Slot booking based on data got from a survey conducted has been developed in this literature. The conclusions drawn from the survey develop key insights into developing statisticorating the use of LTE to support the conventional OCPP and promote user controlal models that are further explored in this context. Algorithms and strategies to implement next-generation efficient EV2X communications have been implemented and developed for the city. Further, we have established a priority order for slot booking and incorp over charge-cycles. Introducing IPMUs using an LTE connection to act as a supplement to the conventional OCPP is explored in this context. Besides that, we have built the M/M/m queuing model of EVs in the charging station and its optimisation. We have done the exhaustive evaluation of the robustness of the proposed system in a fairly large-scale network in a discrete-time event simulator. The proposed system's results (simulation, analytical, and comparison) show the reduction of waiting time, good accuracy, and saving of charging time and costs. These performances measures improve shows the real-time applicability of the proposed system.

III. EXISTING METHODOLOGY

This introduction sets the stage for a comprehensive exploration of cloud file auditing, delving into its significance, challenges, and potential solutions. The following sections will examine the evolving landscape of cloud storage, the importance of file auditing in ensuring data security and compliance, the unique challenges posed by cloud

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

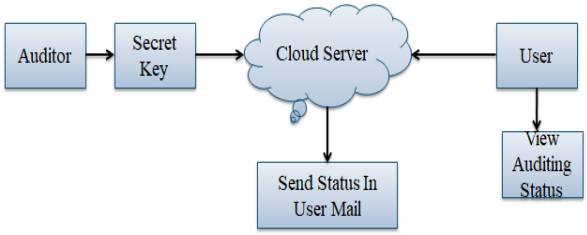
|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304020 |

environments, and the current state-of-the-art techniques and technologies for auditing files stored in the cloud. Additionally, this paper will propose novel approaches and strategies to enhance cloud file auditing, leveraging emerging technologies such as machine learning, blockchain, and secure authentication mechanisms to strengthen data protection and mitigate security risks in cloud-based storage environments. Through in-depth analysis and discussion, this paper aims to provide valuable insights and practical recommendations for organizations seeking to enhance the security of their sensitive files in the cloud.

IV. PROPOSED METHODOLOGY

The proposed method for securing sensitive files stored on cloud servers offers a novel solution to address the shortcomings of conventional file auditing methods. By integrating secure download key notifications with login processes, our approach enhances the security of file downloads in cloud environments. Unlike traditional auditing systems that often overlook the critical aspect of monitoring file downloads securely, our solution ensures comprehensive auditing of file activities while seamlessly integrating with login processes. This innovative feature provides organizations with enhanced control over file access and facilitates secure sharing of sensitive information in cloud environments. Our method employs advanced encryption techniques to generate unique download keys for authorized users, which are securely transmitted upon successful login authentication. These download keys serve as access tokens, enabling users to securely retrieve and download sensitive files from the cloud server. Meanwhile, our auditing system meticulously tracks and logs all file download activities, including the user identity, timestamp, and accessed file details, providing organizations with detailed visibility into file access events. Additionally, our solution incorporates proactive measures to mitigate potential security risks, such as unauthorized downloads or access attempts, by issuing real-time notifications and alerts to administrators. By adopting our proposed method, organizations can bolster their data security posture, ensuring the confidentiality, integrity, and availability of sensitive files stored on cloud servers. Through rigorous testing and validation, we demonstrate the effectiveness and practicality of our approach in safeguarding sensitive data and mitigating security threats in cloud environments.



System Architecture

IV. RESULT AND DISCUSSION

- **Secure Download Key Generation Module**

This module plays a crucial role in ensuring the security of file downloads by generating unique secure download keys for each download request. These keys serve as access tokens, functioning as a secure mechanism to verify the authenticity and authorization of users requesting file downloads. By generating unique keys for each download request, the module enhances security measures, effectively preventing unauthorized access to sensitive files stored on cloud servers. This ensures that only authorized users with valid download keys can access and download the requested files, thereby safeguarding the confidentiality and integrity of sensitive data.

- **Login Integration Module**

This module seamlessly integrates with the login processes of the cloud server, ensuring a smooth and intuitive user experience. Upon successful authentication, it automatically initiates the generation and sending of secure download key notifications to the designated email addresses linked to the respective user accounts. This proactive

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304020 |

approach enhances the security of file downloads by providing users with unique access tokens that authenticate their identity and authorize access to sensitive files stored on the cloud server. By integrating seamlessly with the login processes, this module streamlines the workflow for users while bolstering the overall security posture of the cloud storage system.

- **Auditing Module**

This module serves as a vital component in ensuring the thorough auditing of file activities within a system. It tracks various actions including downloads, uploads, modifications, and deletions, capturing essential metadata such as user identity, file name, timestamp, and the associated secure download key for each action. By meticulously logging these details, the module provides comprehensive visibility into file-related activities, enabling organizations to monitor and analyze user interactions with sensitive data effectively. This helps enhance security measures, detect unauthorized access or modifications, and maintain compliance with regulatory requirements.

- **Access Control Module**

This module implements access controls by verifying the validity of secure download keys generated for file access. Users must provide these keys to gain access to requested files, ensuring that only authorized individuals can securely and controllably access sensitive information. By enforcing this mechanism, the module guarantees secure and controlled access to files, enhancing data security and minimizing unauthorized access risks.

- **Notification Sending Module**

Once a user logs in and requests to download a file, this module automatically generates a notification containing essential details such as file name, timestamp, user identity, and the secure download key. It then sends this notification to the designated email address. This process ensures that users receive timely and relevant information regarding their file downloads, enhancing transparency and security in the download process. Additionally, by providing users with detailed notifications, organizations can maintain accountability and oversight over file access activities, facilitating compliance with security policies and regulations.

VI.CONCLUSION

The proposed method for securing sensitive files stored on cloud servers represents a significant advancement in addressing the limitations of conventional file auditing methods. By integrating secure download key notifications with login processes, our approach offers a comprehensive solution to enhance the security of file downloads in cloud environments. Unlike traditional auditing systems that may overlook the critical aspect of securely monitoring file downloads, our solution ensures thorough auditing of file activities while seamlessly integrating with login processes. This innovative feature not only provides organizations with enhanced control over file access but also facilitates secure sharing of sensitive information in cloud environments. Through the implementation of advanced encryption techniques and real-time monitoring capabilities, our solution empowers organizations to safeguard their sensitive data effectively and mitigate potential security risks. Furthermore, by leveraging the flexibility and scalability of cloud technology, our approach enables organizations to adapt and scale their security measures according to evolving needs and requirements. Overall, the proposed method offers a reliable and efficient solution to bolster the security of sensitive files stored on cloud servers, thereby enhancing data protection and promoting secure collaboration in modern computing environments.

REFERENCES

1. Haoran Yuan, Xiaofeng Chen, Jianfeng Wang, Jiaming Yuan, Hongyang Yan and Willy Susilo, "Blockchain-based public auditing and secure deduplication with fair arbitration", *Inf. Sci.*, vol. 541, pp. 409-425, 2020.
2. Yuefeng Du, Huayi Duan, Anxin Zhou, Cong Wang, Man Ho Au and Qian Wang, "Towards privacy-assured and lightweight on-chain auditing of decentralized storage", *40th IEEE International Conference on Distributed Computing Systems ICDCS 2020 Singapore November 29 - December 1 2020*, pp. 201-211, 2020.
3. Yuefeng Du, Huayi Duan, Anxin Zhou, Cong Wang, Man Ho Au and Qian Wang, "Enabling secure and efficient decentralized storage auditing with blockchain", *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 5, pp. 3038-3054, 2022.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304020 |

4. Zhonghao Yuan, Jiaojiao Wu, Jianpeng Gong, Yao Liu, Guohua Tian, Jianfeng Wang, et al., Blockchain-based self-auditing scheme with batch verification for decentralized storage, vol. 20, pp. 1-13, jan 2022.
5. Hao Jin, Hong Jiang and Ke Zhou, "Dynamic and public auditing with fair arbitration for cloud data", *IEEE Trans. Cloud Comput.*, vol. 6, no. 3, pp. 680-693, 2018.
6. Ruonan Chen, Yannan Li, Yong Yu, Huilin Li, Xiaofeng Chen and Willy Susilo, "Blockchain-based dynamic provable data possession for smart cities", *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4143-4154, 2020.
7. Taek-Young Youn and Ku-Young Chang, "Bi-directional and concurrent proof of ownership for stronger storage services with de-duplication", *Sci. China Inf. Sci.*, vol. 61, no. 3, pp. 032107:1-11, 2018.
8. Xiang Gao, Jia Yu, Wenting Shen, Yan Chang, Shibin Zhang, Ming Yang, et al., "Achieving low-entropy secure cloud data auditing with file and authenticator deduplication", *Inf. Sci.*, vol. 546, pp. 177-191, 2021.
9. Yang Xu, Cheng Zhang, Guojun Wang, Zheng Qin and Quanrun Zeng, "A blockchain-enabled deduplicatable data auditing mechanism for network storage services", *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 3, pp. 1421-1432, 2021.
10. Guohua Tian, Yunhan Hu, Jianghong Wei, Zheli Liu, Xinyi Huang, Xiaofeng Chen, et al., "Blockchain-based secure deduplication and shared auditing in decentralized storage", *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 6, pp. 3941-3954, 2022.
11. Lu Rao, Hua Zhang and Tengfei Tu, "Dynamic outsourced auditing services for cloud storage based on batch-leaves-authenticated merkle hash tree", *IEEE Trans. Serv. Comput.*, vol. 13, no. 3, pp. 451-463, 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details