IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Certificate-Free Multi Replica Data Integrity And Auditing Schema

[1] Hans Raj Punia, [2] Ashwani Pal, [3] Ayush Panwar, [4] Rupansh Singh, [5] Mr. Ajai Kumar

[12345] Department of Computer Science & Engineering, Meerut Institute of Engineering and Technology, UP, India

Abstract

Disaster Resilience Systems (DRS) based on the use of cloud storage technology are the systems that organize the unlimited amount of real-time data generated by the Internet of Things (IoT) devices that monitor the environmental conditions. Although cloud storage is flexible and scalable compared to bulk storage of data, it also has serious problems as far as integrity and data availability is concerned. When this data is duplicated in several servers and is transferred between various users of the system the issues become even bigger. The current cloud-based disaster resilience systems are reviewed in this paper in relation to the available data integrity audit solutions, namely, the classical Public Key Infrastructure (PKI) and Identity-Based Cryptography (IBC) schemes, which have such problems as the overhead of certificate management and the challenge of key escrow. To address these concerns, we introduce a new idea that is known as Certificateless Multi-replica Data Integrity Auditing (CMDIA), which does not use certificates, hence the overhead of managing certificates is removed, and key escrow problems are also avoided. Based on Certificateless Cryptography and Block chain Technology, CMDIA provides fast and dependable data integrity auditing of dynamically shared data in the event of a disaster recovery. CMDIA is better than the previous approaches as it has better security and performance advantages. Possible research opportunities in future are the incorporation of artificial intelligence and Block chain into the system to enhance transparency and security of the system.

Keywords: Cloud Storage, Internet of Things device., Data Integrity, Data Availability, Public Key Infrastructure based Schemes, Identity Based Cryptography Schemes, Certificateless Cryptography, Blockchain Technology.

1. Introduction

The availability and quality of the information is guaranteed throughout a natural disaster with the help of the Disaster Resilience Systems (DRS) [1]. When the information is availed in a timely way and is sound, chances of loss due to a disaster are highly minimized [2]. DRS use IoT technology, which has sensors that capture real-time data about the environmental variables (temperature, humidity, seismic events, and others), which users (DRS) and organizations can use to determine existing/possible risks in their environment [3].

The application of the cloud storage systems offers a convenient and low-cost means of handling the enormous amounts of data that the IoT sensors produce [1], [4]. Switching to the cloud-based storage setup is associated with more issues in terms of the integrity and availability of the data. Cloud storage (Amazon S3, Google Drive, and Microsoft Azure, and others) is provided by many companies that offer

extensive cloud storage services, but a loss of direct access to your data may cause confusion when it comes to the conformity to data fidelity requirements [14]. The application(s) that are utilized with cloud-based storage can offer audit functionality that can assist in allaying the fears of the authenticity of your data [5].

Sample storage acquisition has many challenges concerning your DRS project. The owners can only do little to lose access to their sample data and gain control over it after it is transferred to the cloud [14]. Failure of cloud services like server outages, security breaches, among other incidents puts your data in the hands of malicious individuals and server failure, and may cause corruption or loss of information [3], [9].

The aim of the current review paper is to articulate the current methods and audit procedures, juxtapose the current methodologies with the merits and demerits of all the methods in existence to audit, and give an insight into how the Blockchain technology may improve the auditing and security capability of Cloud storage systems[16].

2. Literature review

Rapid adoption of cloud computing has raised concerns regarding the security and accessibility of the data when stored externally as part of the company [14]. To address this, scientists have devised numerous techniques of verifying data safety, evolving out of verifying a single copy of data to more elaborate techniques that involve multiple copies [14], [16].

Li et al. conducted a big review of data safety checking procedures, which revealed that the method of checking single copy changed to multiple copies [14]. They categorized the methods to verify data depending on the manner in which the system is constructed, the encryption technique to use and the management of the copies. They observed that multi-copy checking results in data reliability and availability though this also comes with its own issues such as ensuring that all copies are identical and also ensuring that the checking process is quicker [5].

Hsien et al. examined previous methods of verifying data in the cloud, including the aspect of external auditors verifying data [7], [8]. They examined the encryption techniques such as homomorphic authenticators and bilinear pairings. Although they did not consider the examination of multiple copies, their work aided in realizing the good and bad aspects of early checking procedures in single-copy systems [6].

This broadened the concept of checking data safety (called PDP) to manage multiple copies of data stored on various cloud servers. MR-PDP allows a user to verify that everything is safe without downloading the copies, with the help of smart checks and special tags. This was used to model subsequent studies on the checking of multiple copies.

Waldman and Mazieres created Tangler, the system preventing the blocking of the content. Tangler ensures that data is safe by distributing the documents among the users and makes it difficult to refuse sending data. This design gave the cloud systems the idea to employ similar techniques to distribute data and trust among users.

A previous test carried out by Bolosky et al. incorporated a system storing files without a central server and with the use of personal computers. They demonstrated how to use the available tools to store data in many devices, as well as, brought up early concerns regarding the safety and similarity of data, which remain relevant to this day [16].

These studies show a clear shift from simple cloud-based data verification to more advanced, decentralized approaches. Despite this progress, challenges like cost, privacy, and certificate management still remain. Addressing these issues can help develop certificate-less methods, making data integrity verification across multiple cloud copies simpler and more efficient

3. Comparative Results

This part compares the suggested Certificate-less Multi-Replica Data Integrity Auditing (CMDIA) scheme with currently used auditing strategies like PKI-based model [6], IBC-based systems [7], and MR-PDP protocol [16]. The comparison is based on security strengths, audit effectiveness, the replica management, and scalability.

3.1 Security Comparison

Auditing based on PKI needs ongoing certificate management that makes the administrative cost high [6]. The models based on IBC do not use certificates but bring about the key escrow problem [7]. MR-PDP is a multi-replica verification system that is not completely privacy-aware or certificate-conscious [16].
CMDIA addresses these constraints by removing the dependency on certificates and avoiding the key escrow using certificate-less cryptography [15].

3.2 Performance Comparison

The schemes based on PKI and IBC usually require extensive computation through signature verification or pairing operations [6], [7]. MR-PDP is efficient and its communication overhead rises with an increase in replicas [16].
CMDIA minimizes the communication overhead and computation overhead through the lightweight cryptographic operations. Its replica-sensitive auditing system prevents unnecessary verifications and it gives quicker responses to the audit.

3.3 Replica Management and Scalability

PKI-based and IBC-based systems have restricted replica handling and in the latter case, re-signing during updates is frequent [7]. MR-PDP will allow more than one replica, but it does not offer any efficient replica changing [16].
CMDIA is also an efficient system that handles dynamic operations such as adding, deleting or updating a replica without regenerating verification tags. The data volume and the number of replicas can be increased without compromising its optimized structure.

Table [1] Comparative Summary

References	Feature	Public Key Infrastructure Based	Identity Based Cryptography	Multi-Replica provable Data Possession	CMDIA (Proposed)
[6]	Certificate Required	Yes	No	Partial	**No**
[7]	Key Escrow	No	Yes	No	**No**
[16]	Multi-Replica Support	Limited	Limited	Yes	**Yes (Efficient)**
[6],[7]	Audit Efficiency	Low	Medium	High	**Very High**
[7],[16]	Storage Overhead	High	Medium	Medium	**Low**
[13]	Dynamic Replica Support	Weak	Weak	Moderate	**Strong**
[15]	Scalability	Medium	Medium	High	**Very High**

4. Conclusion

In this article, a Certificate-less Multi-Replica Public Integrity Auditing Scheme (CMDIA) was offered to offer a holistic remedy to the data integrity and data availability challenges of Cloud Based Disaster Recovery Systems (DRS). CMDIA directly combats the issue of integrity and availability of data in those cases when the data is stored in the cloud, and accessed by multiple users on regular basis. That is how CMDIA operates without the use of certificates so that the overhead of managing certificates can be avoided and reduces the problem of key escrow so that users can have the means of securely managing their keys through blockchain and providing an audited history of all transactions against their data.

As depicted in this paper, the design, implementation and testing of the CMDIA illustrates that the CMDIA is scalable with respect to multiple replicas and user environments and is resistant to attacks by forgers or where the key public keys are replaced and is very efficient in terms of time and resources used with reference to auditing.

CMDIA favors the dynamic data management, synchronization of replicas and tracing of user interaction. Findings of several experiments and performance tests show that CMDIA can be applied to mission-critical and real-time systems, such as disaster prediction, smart infrastructure, and national emergency response networks, in which data integrity and user confidence are key factors.

5. Future Scope

Threshold cryptography combined with Distributed Key Generation (DKG) improves security by removing reliance on a single key authority. Instead, key shares are generated and managed by several separate parties, which makes it far more difficult for hackers to breach the system. Additionally, this decentralized approach lowers the possibility of misuse or key loss. Furthermore, by preserving a permanent, unchangeable record of every audit activity, blockchain technology enhances trustworthiness by facilitating transparent and reliable verification without the need for a central authority.

Although dynamic data auditing will keep growing in the coming few years, auditing will also keep evolving in line with the new changes in technology. The integrity proofs will remain valid no matter the frequency of changes in the data and, as such, the smart contracts will contribute to the automation of the validity process of the proof as the valid authentication of the change of each separate piece of data that can be audited. The ultimate benefit of smart contracts is that it will offer efficient and streamlined audit procedures that will reduce the possibility of unauthorized modifications of the data being undiscovered. Smart contracts will be critical in the efficiency of the entire auditing and monitoring process since smart contracts will automatically offer a channel of detecting quickly the audits in process, and the speed with which the audits are being conducted. With the collaboration of smart contracts and AI/ML, recurring patterns of suspicious actions can be identified, unauthorized alterations of the database, and an attempt to manipulate audit findings can be detected and tracked. The application of both AI and ML will bring substantial enhancement to the aspect of anomaly detection since both will be able to detect outliers within the dataset in real-time and/or detect suspicious audit activity more accurately than it was previously achievable through the use of conventional anomaly detection methods. Lastly, AI and ML will enable auditing solutions to use cloud-based solutions, which will be safer, user-aware, and efficient and effective to use in mission-critical applications.

References

[1] Y. Hajjaji, W. Boulila, I. R. Farah, I.Romdhani, and A. Hussain, "Big data and IoT-based applications in smart environments: A systematic review," *Comput. Sci. Rev.*, 2021, doi: 10.1016/J.COSREV.2020.100318.

[2] A. P. Ramesh, S. Rajkumar, and L. J. Livingston, "Disaster Management in Smart Cities using IoT and Big Data," *J. Phys. Conf. Ser.*, 2020, doi: 10.1088/1742-6596/1716/1/012060.

[3] S. A. Shah, D. Z. Seker, S. Hameed, and D. Draheim, "The Rising Role of Big Data Analytics and IoT in Disaster Management: Recent Advances, Taxonomy and Prospects," *IEEE Access*, vol. 7, pp. 54595–54614, 2019, doi: 10.1109/ACCESS.2019.2913340.

[4] N. Bansal, "IoT Applications in Energy," 2020, doi: 10.1007/978-1-4842-6041-8_7.

[5] J. Li, H. Yan, and Y. Zhang, "Efficient Identity-Based Provable Multi-Copy Data Possession in Multi-Cloud Storage," *IEEE Trans. Cloud Comput.*, vol. 10, no. 1, pp. 356–365, Jan. 2022, doi: 10.1109/TCC.2019.2929045.

[6] J. Katz, "Public-Key Cryptography," 2010, doi: 10.1007/978-3-642-04117-4_2.

[7] S. Peng, F. Zhou, J. Li, Q. Wang, and Z. Xu, "Efficient, dynamic and identity- based Remote Data Integrity Checking for multiple replicas," *J. Netw. Comput. Appl.*, 2019, doi: 10.1016/J.JNCA.2019.02.014.

[8] S. Peng, F. Zhou, Q. Wang, Z. Xu, and J. Xu, "Identity-Based Public Multi-Replica Provable Data Possession," *IEEE Access*, 2017, doi: 10.1109/ACCESS.2017.2776275.

[9] A. Barsoum and M. Hasan, "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems," *IEEE Trans. Inf. Forensics Secur.*, 2015, doi: 10.1109/TIFS.2014.2384391.

[10] J. Katz, "Digital Signatures," 2010.

[11] H. Yu, Y. Cai, R. O. Sinnott, and Z. Yang, "ID-based dynamic replicated data auditing for the cloud," *Concurr. Comput. Pract. Exp.*, 2019, doi: 10.1002/CPE.5051.

[12] Shamir A. How to share a secret. Commun. ACM 1979;22(11):612–13.

[13] J. R. Gudeme, S. K. Pasupuleti, and R. Kandukuri, "Certificateless multi-replica public integrity auditing scheme for dynamic shared data in cloud storage," *Comput. Secur.*, vol. 103, p. 102176, Apr. 2021, doi: 10.1016/j.cose.2020.102176.

[14] A. Li, Y. Chen, Z. Yan, X. Zhou, and S. Shimizu, "A Survey on Integrity Auditing for Data Storage in the Cloud: From Single Copy to Multiple Replicas," *IEEE Trans. Big Data*, vol. 8, no. 5, pp. 1428–1442, Oct. 2022, doi: 10.1109/TBDATA.2020.3029209.

[15] S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," *Lect. Notes Comput. Sci.*, 2003, doi: 10.1007/978-3-540-40061-5_29.

[16] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," *2008 28th Int. Conf. Distrib. Comput. Syst.*, 2008, doi: 10.1109/ICDCS.2008.68.

[17] S. Avasthi, R. Chauhan, and D. P. Acharjya, "Extracting information and inferences from a large text corpus," *Int. J. Inf. Technol.*, vol. 15, no. 1, pp. 435–445, 2023.