iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50400

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Secure Data Sharing and Search for Cloud Edge Collaborative

Hitesh Munot[1], Ashwin Bettawar[2], Dipen Saka[3], Nikhil Langewar[4]
Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune

Abstract: ***The cloud-edge-collaborative storage (CECS) model is a promising one for handling internet of things data (IoT). It enables edge servers to instantly process IoT data and store it on a cloud server. However, CECS faces the possibility of data leaking as a result of the weakness of edge and cloud servers. Only if all edge servers are trusted are the current secure CECS schemes secure. In other words, all cloud data (produced by IoT devices) will be exposed if any edge server is attacked.It first gives users the ability to create a public-private key pair and take control of their own private keys. The current approach, however, calls for edge servers to control users' private keys. Second, it employs searchable public key encryption to make data searches more safe, effective, and adaptable. In terms of security, our plan guarantees the privacy of cloud data, secure data sharing, secure data searching, and prevents a single point of breach. In particular, when compared to the current secure CECS system, our scheme requires less computing and communication overhead to generate a search trapdoor.***
Keywords: CECS, edge servers, public and private keys, fog computing, aes encryption.

I. INTRODUCTION

The existing method, on the other hand, demands the usage of edge servers to control users' private keys. In order to enhance the security, effectiveness, and adaptability of data searches, it also uses searchable public-key encryption.
Our approach guarantees the anonymity of cloud data, safe data sharing and searching, and the removal of a single point of failure in terms of security. Cloud- Secure Data deduplication Based a promising framework to process data of the internet of things (IoT). It enables real-time IoT data processing on servers and cloud server storage. As a result, it can quickly respond to requests from IoT devices, offer a sizable amount of cloud storage for IoT data, and make it simple for users to share IoT data. However, it faces the risk of data leaking because of the weakness of edge and cloud servers. The security of current Secure Data deduplication in Cloud Storage techniques depends on the trustworthiness of all edge servers. In other words, all cloud data will leak if any edge server is compromised. To address the above problems, we propose a new secure data search and sharing scheme.

II. MOTIVATION

This work showed that it was possible to share and search outsourced data in the cloud-edge collaborative paradigm while maintaining privacy by implementing searchable encryption along with another AES technique.The work would allow IOT devices from different domains to work together without compromising the security of the user or data. The low computing required for the encryption is the most suitable for such devices and also proves efficient in low cost computing which is environment friendly.

III. OBJECTIVE

To make sharing and transfer of data more secure and to deduce a solution which requires low computational power thus helping IOT devices to use it efficientely.

IV. LITERATURE SURVEY

1) *Paper Name: Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing.*

Author: Qinlong Huang, Member, IEEE, Zhicheng Zhang, and YixianYang
Abstract:- Benefiting from cloud computing and mobile devices, a huge number of media contents, such as videos are shared in mobile networks. Although scalable video coding can be utilized to provide flexible adaptation, the cloud poses a serious threat to media privacy. In this paper, we propose a privacy-preserving multi-dimensional media sharing scheme named SMACD in mobile cloud computing. First, each media layer is encrypted with an access policy based on attribute-based encryption, which guarantees media confidentiality as well as fine-grained access control.

Then, we present a multi-level access policy construction with a secret sharing scheme. It ensures that the mobile consumers who obtain a media layer at a higher access level must satisfy the access trees of its child layers at the lower access level, which is compatible with the characteristics of multi-dimensional media and also reduces the complexity of access policies. Moreover, we introduce decentralized key servers to achieve both intra-server and inter-server deduplication by associating different access policies into the same encrypted media. Finally, we conduct experimental evaluation on mobile devices and cloud platforms with real-world datasets. The results indicate that SMACD protects media privacy against cloud media centers and unauthorized parties, while incurring less computational and storage cost.

2) Paper Name: 1.A Data Integrity Verification Scheme of Deduplication for Cloud Ciphertexts

Author: K. Spandana,2Dharani Dadamoni,3Shreya Maramreddy

Abstract::- This paper proposes a data integrity verification scheme of DE dupli- cation for cloud ciphertexts, including cloud cipher text DE duplication and cloud data integrity verification. In the data integrity verification, the proxy re-signature method is adopted.The deduplication technique is used to manage data duplication in clouds. Although there are some deduplication approaches used to avoid data redundancy, still they have a lack of efficiency. The main aim of this paper is to obtain sufficient knowledge and a good idea about deduplication techniques by surveying existing approaches and this work may help the researcher and practitioner for their future research in developing efficient cloud storage management techniques.

3) Paper Name: Image And Text Encrypted Data With Authorized Deduplication In Cloud

Author: S.Uthayashankar J.Abinaya V.Harshini R.Jayavardhani

Abstract : The role re-encryption is used to avoid the privacy data leakage and also to avoid the deduplication in a secure role re-encryption system.Role re-encryption method is to share the access key for the corresponding authorized user for access- ing the particular file without the leakage of privacy data. In this paper, the role re-encryption is used to avoid the privacy data leakage and also to avoid the dedupli- cation in a secure role re-encryption system(SRRS). And also it checks for the proof of ownership to identify whether the user is an authorized user or not. This is for efficiency. Role re-encryption method is to share the access key for the corresponding authorized user for accessing the particular file without the leakage of privacy data. In our project we are using both the avoidance of text and digital images.

4) Paper Name: Analysis on data deduplication techniques of storage of big data in cloud

Author: K.Vijayalakshmi Dr.V.Jayalakshmi

Abstract : Cloud computing is the optimal technology that provides many comput- ing resources, especially storage for Big data. Cloud offers the best storage man- agement to back up the big data from IoT, business, enterprise, or government.As nowadays, many devices are connected to the internet (Thing continuum), and many businesses deal with a huge amount of data, digital data growth is exponentially in- creased. Cloud computing is the optimal technology that provides many computing resources, especially storage for Big data. Cloud offers the best storage management to up the big data from IoT, business, enterprise, or government.

5) Paper Name: Secure Data deduplication Based on Threshold Blind Signature and Bloom Filter in Internet of Things

Author: BO MI 1, YANG LI1, HUANG DARONG 1

Abstract: Within the cloud environment, the availability of storage, as well as band- width, can be effectively preserved in virtue of data deduplication. However, re- fraining redundancy from additional storage or communication is not trivial due to security concerns. Though intensive researches have been addressed on a conver- gent crypto system for secure data deduplication, the conflicts amongst functional- ity, confidentiality, and authority remain unbalanced. Moreconcretely, although data are obfuscated under convergent encryption, a violent dictionary attack is still effi- cacious since the whole process relies heavily on plain texts.As for data ownership the download privilege, which depends on hash value, may also be infringed due to the same reason.

6) Paper Name: A Data Integrity Verification Scheme of Deduplication for Cloud Ciphertexts

Author: Qingyun Hu

Abstract: Cloud data deduplication can save cloud storage resources and network communication bandwidth, and improve cloud storage efficiency. A series of dedu- plication technologies are proposed to achieve cloud data deduplication. However, the traditional deduplication schememainly implements data deduplication with- out providing data integrity verification, so it cannot beverified whether the CSP correctly stores user data.

This paper proposes a data integrity verificationscheme of deduplication for cloud ciphertexts, including cloud ciphertext deduplication and cloud data integrity verification. In the data integrity verification, the proxy re-signature method is adopted. In addition, our scheme realizes user revocation, ensures the privacy of cloud data, and satisfies unforgeability of tags. Performance analysis results show that it has higher efficiency than similar schemes.

7) Paper Name: Secure Cloud Data Deduplication with Efficient Re-encryption

Author: Haoran Yuan, Xiaofeng Chen, Senior Member

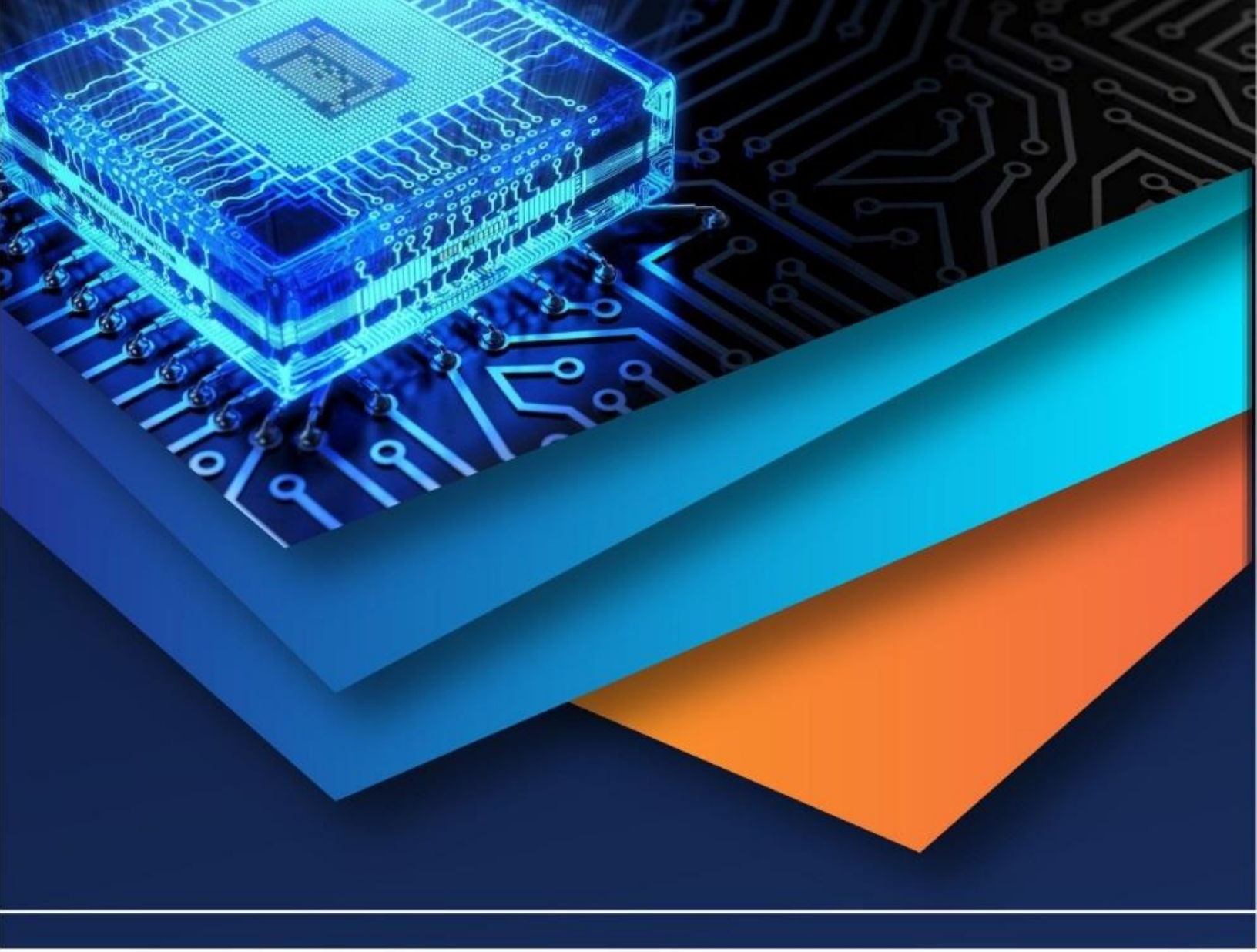
Abstract:- Data deduplication technique has been widely adopted by commercial cloud storage providers, which is both important and necessary in coping with the explosive growth of data. To further protect the security of users' sensitive data in the outsourced storage mode, many secure data deduplication schemes have been de- signed and applied in various scenarios. Among these schemes,secure and efficient re-encryption for encrypted data deduplication attracted the attention of many schol- ars,and many solutions have been designed to support dynamic ownership man- agement. In this paper, we focus on the re-encryption deduplication storage system and show that the recently designed lightweight rekeying-aware encrypted dedu- plication scheme (REED) is vulnerable to an attack which we call it stub-reserved attack. Furthermore, we propose a secure data deduplication scheme with efficient re-encryption based on the convergent all-or-nothing transform (CAONT) and ran- domly sampled bits from the Bloom filter. Due to the intrinsic property of one-way hash function, our scheme can resist the stub-reserved attack and guarantee the data privacy of data owners' sensitive data.

VI. CONCLUSION

By reading from various research papers and books we have gathered the information about how data deduplication vendors are adding capabilities to their products to help increase its adoption rate and to fight off challenges from alternatives like the cloud, tape and even regular disk in a server. By using the AES algorithm, they are evolving from just disk storage systems with deduplication software to truly complete data protection devices that can be integrated into applications and backup software for improved efficiency and management .

REFERENCES

[1] Qinlong Huang, Member, IEEE, Zhicheng Zhang, and Yixian Yang,"Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing," IEEE Transactions on Mobile Computing vol.20, pp. 1951-1964, 2021.
[2] A Data Integrity Verification Scheme of Deduplication for Cloud Ciphertexts K. Spandana,Dharani Dadamoni,3Shreya Maramreddy
[3] Paper Name: Image And Text Encrypted Data With Authorized Deduplication In Cloud Author:S.Uthayashankar J.Abinaya V.Harshini R.Jayavardhani
[4] Paper Name:Image And Text Encrypted Data With Authorized Deduplication In Cloud Author:S.Uthayashankar J.Abinaya V.Harshini R.Jayavardhani
[5] Paper Name: Secure Data deduplication Based on Threshold Blind Signature and Bloom Filter in Internet of Things Author: BO MI 1, YANG LI1, HUANG DARONG
[6] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Transactions on Wire- less Communications, vol. 10, no. 7, pp. 2372–2379, 2018
[7] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large databases with incremental updates," IEEE Trans.Computers, vol. 65, no. 10, pp. 3184–3195, 2019
[8] X. Chen, B. Lee, and K. Kim, "Receipt-free electronic auction schemes us- ing homomorphic encryption," Information Security and Cryptology - ICISC 2003, 6th International Conference, Seoul, Korea, November 27-28, 2019, Re- vised Papers, pp. 259–273, 2019
[9] T. Jiang, X. Chen, Q. Wu, J. Ma, W. Susilo, and W. Lou, "Secure and efficient cloud data deduplication with randomized tag," IEEE Trans. Information Forensics and Security, vol. 12, no. 3, pp. 532–543, 2019.
[10] J. Li, C. Qin, P. P. C. Lee, and J. Li, "Rekeying for encrypted deduplication storage," in 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2016, pp. 618–629.
[11] GFG - AES algorithm explained- https://www.geeksforgeeks.org/advanced-encryption-standard-aes



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY