e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:02/February-2022 Impact Factor- 6.752 www.irjmets.com

PRIVACY-PRESERVING MEDIA SHARING WITH SCALABLE ACCESS CONTROL AND SECURE DEDUPLICATION IN CLOUD COMPUTING

Meet Bhanushali*1, Mahesh Kalkute*2, Krushna Channe*3

*1,2,3Computer Engineering, SKNSITS, Lonavala, Maharashtra, India.

ABSTRACT

With the aim to save cloud storage space, safe deduplication algorithms have been developed. We will begin with AES encryption algorithm; it encrypts the messages using a message-derived key. In the result, we found out that identical plaintexts generate similar ciphertexts. AES encryption algorithm encompasses convergent encryption and provides precise security definitions, was proposed. Cloud computing is the advancement of sharing very large amounts of data via network. There are multiple approaches available for providing data security in the cloud storage space. Whereas present approaches are more closely tied to the ciphertext. So, we are suggesting a cloud-based data collection, sharing, and restricted dissemination plan that will preserve multi-owner privacy, in this paper. In this, the database owner will be able to securely share confidential data with a group of clients through the cloud.

I. INTRODUCTION

It is a network-based computer system with a very large storage space where only authorized users will be able to access the platform from anywhere and at any time using a good internet or network connection. Secure deduplication solutions have been proposed to preserve cloud storage space because of increasing development of media content.

In the beginning, the AES encryption algorithm was established, which uses a message-derived key, for message encryption. In the result, we found out that identical plaintexts generate similar ciphertexts. AES encryption algorithm encompasses convergent encryption and provides thorough security, was proposed. It is the advancement of sharing huge amounts of data via network. There are multiple methods for delivering data security in the cloud. Whereas present approaches are more closely tied to the ciphertext. As a result, we propose that data should be gathered, shared, and distributed in a controlled environment. We need to create a plan that can protect the privacy of several owners, in the cloud. The owner of the data will be able to share this data here and store the data securely.

II. LITERATURE SURVEY

Qinlong Huang, Member, Zhicheng Zhang, and Yixian Yang," Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing." [1]

A large number of media assets, such as videos, are shared in mobile networks thanks to cloud computing and mobile devices. Although scalable video coding can help with adaptability, the cloud poses a severe danger to media privacy. We offer a privacy-preserving method in this research. In mobile cloud computing, SMACD is a multi-dimensional media sharing mechanism. To begin, each media layer is encrypted with an access policy based on attribute-based encryption, which ensures media confidentiality and fine-grained access control. control of access Then we show how to build a multi-level access policy with secrets. scheme of sharing It ensures that mobile users who obtain a media layer do it in a safe and secure manner. The access trees of its child layers at the lower access level must be satisfied by a higher access level, which is compatible with the characteristics of multi-dimensional media. It also makes access policies less complicated. We also propose decentralized key servers to achieve both of these goals.

Di Zhang, Junqing Le, Nankun Mu, Jiahui Wu, Xiaofeng Liao," Secure and Efficient Data Deduplication in JointCloud Storage." [2]

Data deduplication can effectively remove data redundancies in cloud storage while also lowering users' bandwidth requirements. However, most previous systems that rely on the assistance of a trustworthy key server (KS) are vulnerable and limited due to information leakage, low attack resistance, high computational cost, and other issues. When the trustworthy KS fails, the entire system fails, resulting in single-point-of-failure. We propose a Secure and Efficient data Deduplication strategy (called SED) in a Joint Cloud storage system that provides worldwide services through collaboration with various clouds in this study. SED can also update and share dynamic data without relying on the trusted KS. Furthermore, SED can avoid the single-point-of-failure problem that plagues traditional cloud storage systems. According to theoretical assessments, our SED ensures semantic security in the random oracle model and has significant anti-attack capabilities, such as brute-force attack resistance and a strong anti-hacking capability. resistance to collusion attacks Furthermore, with low computing complexity, connectivity, and storage overhead, SED can effectively eliminate data redundancies. Client-side usability is improved by SED's efficiency and functionality. Finally, the comparison findings reveal that our strategy outperforms the competition.

Zahra Pooranian; Mohammad Shojafar; Sahil Garg; Rahim Taheri; Rahim Tafazolli," Secure Deduplicated Cloud Storage with Encrypted Two-Party Interactions in Cyber--Physical Systems" [3]

In cloud computing, cloud envisioned cyber-physical systems (CCPS) is a practical technology that relies on the interaction of cyber elements such as mobile users to transport data. Cloud storage uses data deduplication techniques to save space and bandwidth for real-time services in CCPS. Data deduplication is used in this architecture to reduce duplicate data and improve the speed of the CCPS application. It does, however, pose security and privacy problems. For example, data deduplication is incompatible with encryption from several users using separate keys. Several types of research have been conducted in this area. Despite this, they are lacking in terms of security, performance, and adaptability. To reconcile the encryption and data deduplication, we propose a message lock encryption with never-decrypt homomorphic encryption (LEVER) protocol between the uploading CCPS user and cloud storage in this paper. LEVER is the first encrypted deduplication system that is resistant to brute-force attacks.

Xue Yang, Rongxing Lu, Jun Shao, Xiaohu Tang, "Achieving Efficient Secure Deduplication with User-Defined Access Control in Cloud "[4]

One of the most important services of cloud computing is cloud storage, which allows cloud users to outsource their data to the cloud for storage and sharing with authorized users. Secure deduplication has been actively researched in cloud storage because it may minimize redundancy over encrypted data, reducing storage space and communication overhead. Many existing secure deduplication systems aim to achieve the following features in terms of security and privacy: data secrecy, tag consistency, access control, and resistance to brute-force attacks. However, none of them, as far as we know, can meet all four requirements at the same time. To address this limitation, we present an efficient safe deduplication approach with user-defined access control in this paper. Specifically, by permitting only the cloud service provider to authorize data access on behalf of data owners, our system may reduce duplicates to the greatest extent possible without jeopardizing cloud users' security and privacy.

Haoran Yuan, Xiaofeng Chen, "Secure Cloud Data Deduplication with Efficient Re-encryption" [5]

Commercial cloud storage providers have widely implemented data deduplication techniques, which is both significant and required in dealing with the increasing expansion of data. Many secure data deduplication algorithms have been created and implemented in various contexts to further protect the security of users' sensitive data in the outsourced storage mode. Numerous scholars have focused on secure and efficient re-encryption for encrypted data deduplication, and many methods have been developed to facilitate dynamic ownership management. We focus on the re-encryption deduplication storage system in this research, and we show that the recently designed lightweight rekeying-aware encrypted deduplication scheme (REED) is vulnerable to a stub-reserved Attack.

Gulsayyar Ali Dr. Mian Ilyas Ahmad," Secure Block-level Data Deduplication approach for Cloud Data Centers "[6]

The continued growth of the information and technology sector has resulted in an unprecedented surge in storage requirements in cloud data centers. According to the EMC Digital Universe study 2012 [1], global storage has surpassed 2.8 trillion GB and will reach 5247GB per user by 2020. Because clients upload data without knowing what content is available on the server, data redundancy is one of the primary causes of storage scarcity. 18Centers Outages were discovered by the Ponemon Institute" [15]. The concept of data deduplication is utilized to tackle this problem, with each file having a unique hash identifier that changes with the content of the file. When a client wants to save a duplicate of an existing file, he or she is given a pointer to the existing file's location. Data deduplication aids in storage reduction and the identification of redundant duplicates of the same files stored in data centers in this fashion.

Shunrong Jiang†, Tao Jiang and Liangmin Wang," Secure and Efficient Cloud Data Deduplication with Ownership Management "[7]

Data deduplication is a technique for reducing storage space and communication overhead in cloud storage by removing redundant data and storing only one duplicate of it. The convergent encryption system and many of its variants are offered for secure data deduplication. However, most of these solutions ignore or are unable to solve both dynamic ownership changes and secure Proof-of-Ownership (PoW) at the same time. In this paper, we offer a safe data deduplication strategy for dynamic ownership management that uses an efficient PoW process. Our approach, in particular, provides data deduplication at the file and block level for both cross-user and intra-user users. We create a novel PoW scheme during file-level deduplication to ensure tag consistency and achieve mutual ownership verification. Furthermore, in order to accomplish efficient ownership management, we devise a lazy updating technique.

Yuan Zhang, Yunlong Mao," Towards Thwarting Template Side-channel Attacks in Secure Cloud Deduplications "[8]

Deduplication is one of a few essential cloud storage technologies that helps cloud servers to reduce storage space by eliminating redundant file copies. It does, however, frequently leak side channel information about whether or not an uploading file is deduplicated. Adversaries can easily launch a template side-channel attack using this information, substantially harming cloud customers' privacy. We use the k-anonymity privacy principle to create secure threshold deduplication techniques to counter this type of attack. We developed a new cryptographic primitive termed "dispersed convergent encryption" (DCE) scheme and suggested two distinct implementations.

Jianbing Ni, Student Member, Kuan Zhang," Providing Task Allocation and Secure Deduplication for Mobile Crowdsensing via Fog Computing "[9]

Mobile crowdsensing allows a group of people to collect data for a specific consumer using their mobile devices in a cooperative manner. The success of mobile crowdsensing is largely determined by the number of people who participate. The more people who participate, the more sensor data is acquired; nevertheless, the more replication data is generated, which adds extra communication overhead. As a result, data deduplication, also known as data elimination, is crucial for improving communication efficiency. Unfortunately, sensing data is frequently encrypted, making deduplication difficult. In this paper, we present a fog-assisted mobile crowdsensing framework for enhancing task assignment accuracy by allowing fog nodes to allocate tasks depending on user mobility.

SHUGUANG ZHANG," Secure Encrypted Data Deduplication with Dynamic Ownership Updating" [10]

Deduplication eliminates duplicate data copies and lowers cloud service provider storage costs. Deduplication of encrypted data, on the other hand, is challenging. Current systems rely significantly on trustworthy third parties and fail to account for data's popularity, resulting in insufficient security and efficiency. A data deduplication system based on data popularity that is secure and encrypted is proposed. To determine whether different encrypted data originate from the same plaintext, check tags are calculated using bilinear mapping. To safeguard the tags, ciphertext policy attribute-based encryption is used.

III. PROPOSED SYSTEM

We are going to use the AES encryption algorithm for encryption and decryption in the suggested system, as well as data security and secure access management. The MD 5 algorithm will be used for avoid data duplication.

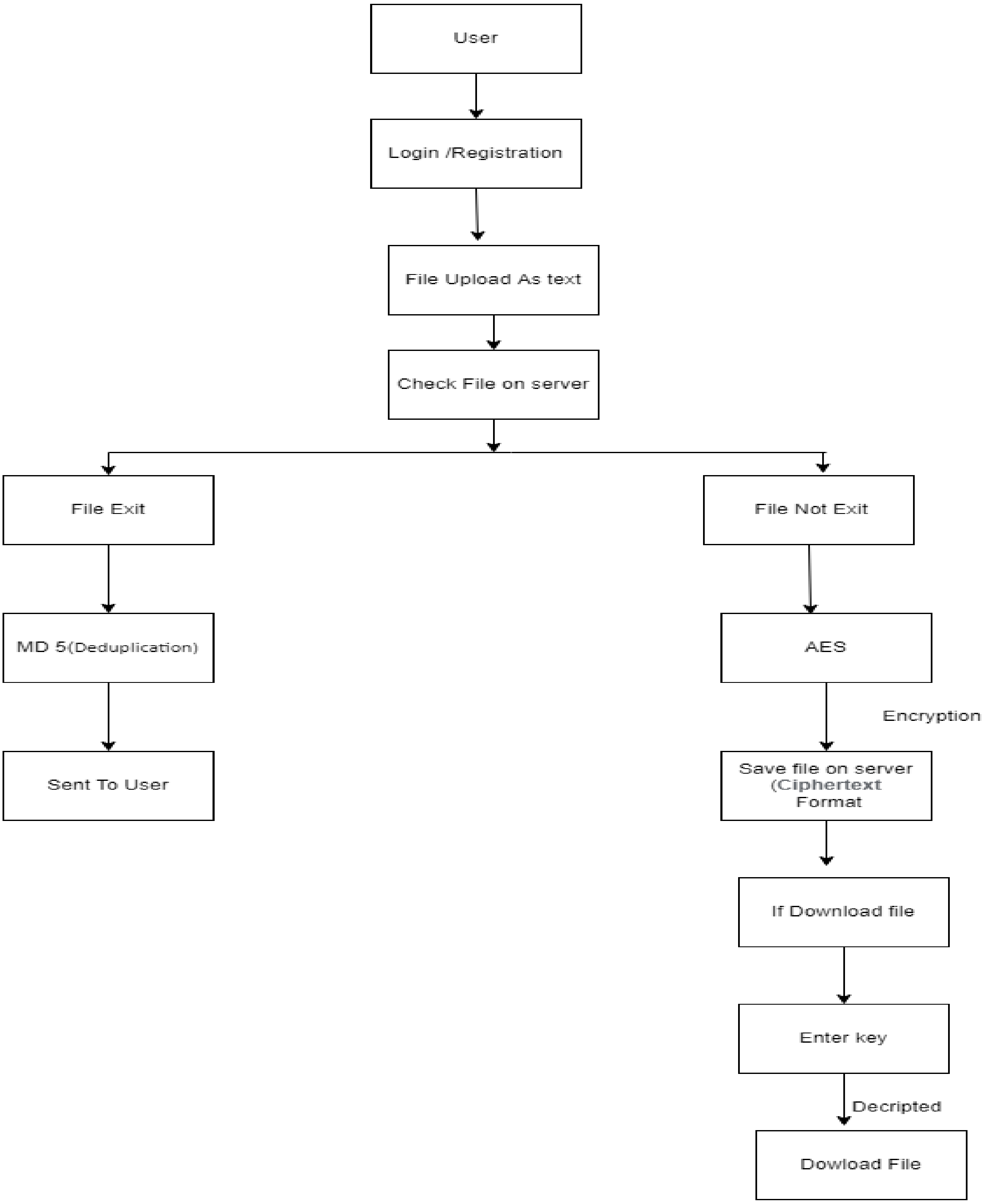

Figure 1: The System Architecture.

IV. ALGORITHM

AES algorithm is a symmetrical block cypher method which accepts plain text in format of 128-bit blocks and converts it into ciphertext using keys of 128, 192, and 256 bits. The AES algorithm is a worldwide standard because it is considered one of the most secure algorithms. The Advanced Encryption Standard (AES) algorithm is a symmetric block cypher that the United States government has chosen with aim to safeguard confidential data. AES algorithm is used to encrypt sensitive data in software and hardware all over the planet. It is very critical for government computer security, cybersecurity, and data security.

MD5: The MD5 message-digest technique produces a 128-bit hash value and it is cryptographically broken but still used frequently. Even though MD5 was created with the aim of being used as a cryptographic hash function, it has been discovered to have multiple flaws. Java is an object-oriented programming language with a high level of abstraction and as few implementation dependencies as possible. Java applications are normally compiled to bytecode, which can execute on any Java virtual machine, regardless of the computer architecture.

V. CONCLUSION

We will avoid deduplication and save files securely in our project. Deduplication is a useful approach for saving cloud storage space and network traffic by removing redundant data. And, for encryption and decryption, we will use the AES algorithm.

VI. REFERENCES

[1] Q. Li, J. Ma, R. Li, X. Liu, J. Xiong, and D. Chen, “Secure, efficient and revocable multi-authority access control system in cloud storage,” Computers Security, vol. 59, pp. 45–59, 2016.

[2] J. Li, H. Yan, and Y. Zhang, “Certificateless public integrity checking of group shared data on cloud storage,” IEEE Transactions on Services Computing, pp. 1–12, 2018.

[3] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, “Flexible and fine-grained attribute-based data storage in cloud computing,” IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 785–796, Sept 2017.

[4] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, “User collision avoidance cp-abe with efficient attribute revocation for cloud storage,” IEEE Systems Journal, pp. 1–11, 2017.

[5] H. Wang, Z. Zheng, L. Wu, and P. Li, “New directly revocable attribute-based encryption scheme and its application in cloud storage environment,” Cluster Computing, vol. 20, no. 3, pp. 2385–2392, Sep 2017. [Online].

[6] T. Taleb, A. Ksentini, M. Chen, and R. Jantti, “Coping with Emerging Mobile Social Media Applications Through Dynamic Service Function Chaining,” IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 2859–2871, Apr. 2016.

[7] K. Yang, Z. Liu, X. Jia, and X. S. Shen, “Time-Domain Attribute Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach,” College Short Form Name, Department of Computer Engineering 2021 44 IEEE Transactions on Multimedia, vol. 18, no. 5, pp. 940–950, May 2016

[8] M. J. Atallah, K. B. Frikken, and M. Blanton, “Dynamic and Efficient Key Management for Access Hierarchies,” in Proceedings of the 12th ACM Conference on Computer and Communications Security, 2005, pp. 190–202.

[9] C. Ma, Z. Yan, and C. W. Chen, “Scalable Access Control for Privacy-Aware Media Sharing,” IEEE Transactions on Multimedia, vol. 21, no. 1, pp. 173–183, Jan. 2019.

[10] H. Cui, R. H. Deng, Y. Li, and G. Wu, “Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud Transactions on Big Data, pp. 1–1, 2019.