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

Meet Bhanushali, Mahesh Kalkute, Krushna Channe

Computer Engineering
SKNSITS, Lonavala, 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.

INTRODUCTION

It is a network-based computer system with very large storage space where only authorized users can access the platform from anywhere and anytime with a good internet or network connection. With the increasing development of media content, secure deduplication solutions have been proposed to save cloud storage space. In the beginning, the AES encryption algorithm was developed, which uses a message-derived key to encrypt messages. As a result, we found that identical plaintexts produce similar ciphertexts. The AES encryption algorithm includes convergent encryption and offers comprehensive security, it has been proposed. It is the advancement of sharing huge amounts of data over the network. There are several methods of providing data security in the cloud. While current approaches are more tightly bound to the ciphertext. Therefore, we propose that data should be collected, shared and distributed in a controlled environment. We need to create a plan that can protect the privacy of multiple owners in the cloud. The owner of the data can share this data here and store the data securely.

LITERATURE SURVEY

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

Thanks to cloud computing and mobile devices, a variety of media content such as videos is being shared on mobile networks. Although scalable video encoding can help with adaptability, the cloud poses a serious

threat to media privacy. We offer a privacy-friendly methodology in this investigation. In mobile cloud computing, SMACD is a multidimensional media sharing mechanism. First, each media layer is encrypted with an access policy based on attribute-based encryption that ensures media confidentiality and fine-grained access control. Access Control Then we show how to create a multi-level access policy with secrets. It sharing scheme ensures that mobile users receiving a media layer do so in a safe and secure manner. The access trees of their sublayers at the lower access level must be satisfied by a higher access level that is compatible with the properties of multidimensional media. It also makes access policies less complicated. We also proposed decentralized key servers to achieve both of these goals.

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

Data deduplication can effectively remove data redundancies in cloud storage while reducing users' bandwidth requirements. However, most previous systems that depend on the support of a trusted key server (KS) are vulnerable and limited due to information leakage, low attack resistance, high computational cost and other issues. If the trusted KS fails, the entire system fails, resulting in a single point of failure. We propose in this study a secure and efficient data deduplication strategy (called SED) in a shared cloud storage system that provides worldwide services by collaborating with different clouds. SED can also update and share dynamic data without relying on the trusted KS. In addition, 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 strong anti-hacking ability. Resistance to collusion attacks In addition, with low computational complexity, connectivity and storage overhead, SED can effectively eliminate data redundancies. Client-side usability is enhanced by the efficiency and functionality of SEDs. Finally, the comparative results show that our strategy outperforms the competition.

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

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 CCPS application speed. However, it poses security and privacy issues. For example, data deduplication is not compatible with encryption by multiple users using separate keys. Various types of investigations have been made in this field. Despite this, they lack security, performance, and customizability. To balance encryption and data deduplication, in this document we propose message lock encryption using Never-Decrypt Homomorphic Encryption (LEVER) protocol between the uploading CCPS user and the cloud storage. LEVER is the first encrypted deduplication system resistant to brute force attacks.

D. Xue Yang, Rongxing Lu, Jun Shao, Xiaohu Tang, "Achieving Efficient Secure Deduplication with UserDefined Access Control in Cloud "

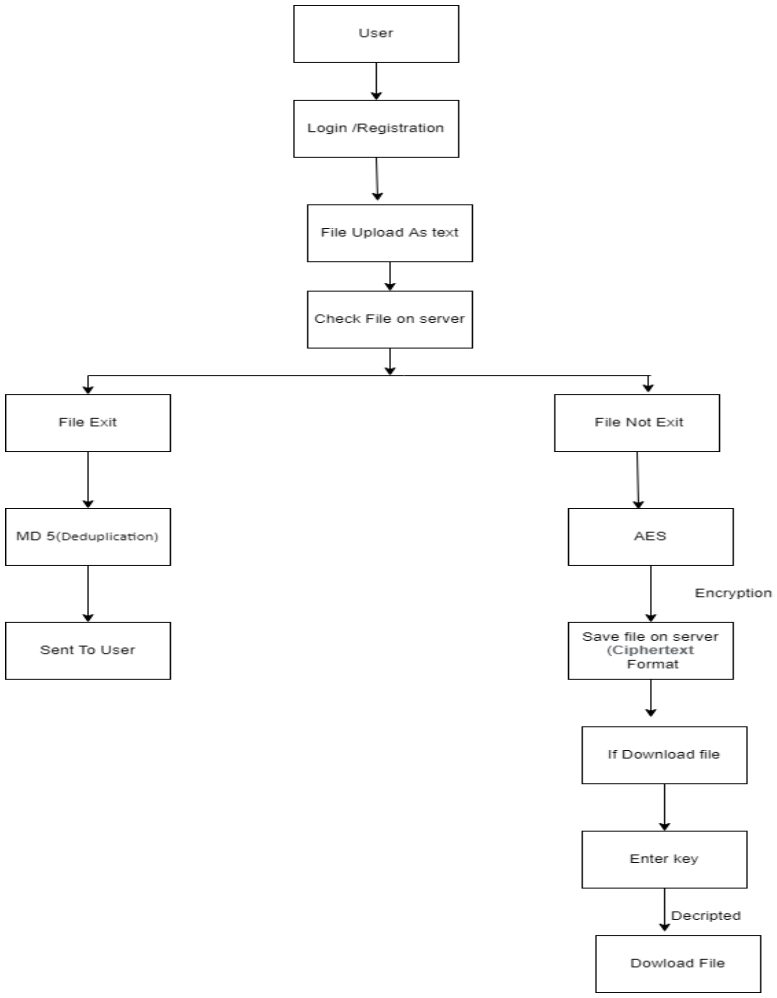
One of the most important services of cloud computing is cloud storage, which allows cloud users to offload their data to the cloud for storage and sharing with authorized users. Secure deduplication has been actively researched in cloud storage as it can minimize redundancy in encrypted data and reduce storage space and communication overhead. Many existing secure deduplication systems aim to achieve the following security and data protection characteristics: data privacy, tag consistency, access control, and resilience to brute force attacks. However, none of them, as far as we know, can fulfill all four requirements at the same time. To address this limitation, in this white paper we present an efficient secure deduplication approach with custom access control. In particular, by allowing only the cloud service provider to authorize data access on behalf of the data owners, our system can reduce duplicates as much as possible without compromising the security and privacy of cloud users.

E. Haoran Yuan, Xiaofeng Chen, "Secure Cloud Data Deduplication with Efficient Re-encryption"

Commercial cloud storage providers have widely implemented data deduplication techniques, which is both important and necessary to cope with increasing data sprawl. Many secure data deduplication algorithms have been created and implemented in various contexts to further protect the security of sensitive user data in paged storage mode. Numerous researchers have focused on secure and efficient re-encryption for deduplication of encrypted data, and many methods have been developed to facilitate dynamic ownership management. We focus on the re-encryption deduplication storage system in this investigation and show that the recently designed lightweight rekey-aware encrypted deduplication (REED) scheme is vulnerable to a stub-reserved attack.

PROPOSED SYSTEM

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



The System Architecture.

ALGORITHM

The AES algorithm is a symmetric block cipher that accepts plaintext in the form of 128-bit blocks and converts it to ciphertext using keys of 128, 192, and 256 bits. The AES algorithm is a worldwide standard as it is considered to be one of the most secure algorithms. The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher chosen by the United States government to protect sensitive data. The AES algorithm is used to encrypt sensitive data in software and hardware around the world. It is very important for government computer, cyber and data security. MD5: The MD5 message digest technique produces a 128-bit hash value and is cryptographically broken, but is still commonly used. Although MD5 was developed with the aim of being used as a cryptographic hash function, several bugs were discovered. Java is an object-oriented programming language with a high degree of abstraction and as few implementation dependencies as possible. Java applications are typically compiled into bytecode that can run on any Java virtual machine, regardless of computer architecture.

CONCLUSION

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

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].