ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 1, 2025

"Secure and Scalable Media Sharing with Privacy Protection and De duplication in Cloud Computing"

*J Sudheer Kumar[1], S Veeresh Kumar[2], T Bhargavi[3], A Sravani[4]

[1] Assistant Professor, Department of CSE, TKR Engineering College –Hyderabad

[2, 3, 4] Assistant Professor, St. Martin's Engineering College, Secunderabad, Telangana – 500100

*Corresponding Author

Email: jsudheer559@gmail.com

ABSTRACT

With the aim to save cloud storage space, safe de duplication 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 cipher texts. 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 cipher text. 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 anytime using a good internet or network connection. Secure de duplication 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 cipher texts. 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 aremultiplemethodsfordeliveringdatasecurityinthecloud.Whereaspresentapproachesaremore closely tied to the cipher text. 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 sever almoners, in the cloud. The owner of the data will be able to share this data here and store the data securely.

II. LITERATURESURVEY

Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing. 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.

Data de duplication 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 De duplication 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-failureproblemthatplaguestraditionalcloudstoragesystems.Accordingtotheoreticalassessments, 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.

Secure De duplicated Cloud Storage with Encrypted Two-Party Interactions in Cyber--Physical Systems.

In cloud computing, clouded versioned 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 de duplication techniques to save space and bandwidth for real-time services in CCPS. Data de duplication 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 de duplication 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 de duplication, we propose a message lock encryption with never-decrypt homomorphism encryption (LEVER) protocol between the uploading CCPS user and cloud storage in this paper. LEVER is the first encrypted de duplication system that is resistant to brute-force attacks.

Achieving Efficient Secure De duplication with User- Defined Access Control in Cloud.

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 de duplication has been actively researched in cloud storage because it may minimize redundancy over encrypted data, reducing storage space and communication overhead. Many existing secure deduplicationsystemsaimtoachievethefollowingfeaturesintermsofsecurityandprivacy: data

Secrecy, tag consistency, access control, and resistance to brute- force attacks. However, none of them, as far as we know, can meet all of our requirements at the same time. To address this limitation, we present an efficient safe de duplication 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 re duce duplicates to the greatest extent possible without jeo pardizing cloud users' security and privacy.

Secure Cloud Data De duplication with Efficient Re- encryption

Commercial cloud storage providers have widely implemented data de duplication techniques, which is both significant and required in dealing with the increasing expansion of data. Many secure data de duplication

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 de duplication, and many methods have been developed to facilitate dynamic ownership management. We focus on the re-encryption de duplication storage system in this research, and we show that the recently designed lightweight rekeying-aware encrypted reduplication scheme (REED) is vulnerable to a stub-reserved Attack.

Secure Block-level Data De duplication approach for Cloud Data Centers.

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, 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 storagescarcity.18Centers Outages were discovered by the Ponemon Institute". The concept of data de duplication is utilized to tackle this problem, witheachfilehavingauniquehashidentifierthatchangeswiththecontentofthefile.Whenaclient wants to save a duplicate of an existing file, and he or she is given a pointer to the existing file's location. Data de duplication aids in storage reduction and the identification of redundant duplicates of the same files stored in data centers in this fashion.

Secure and Efficient Cloud Data De duplication with Ownership Management.

Data de duplication is a technique for reducing storage space and communication over head 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 de duplication. 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 de duplication strategy for dynamic ownership management that uses an efficient PoW process. Our approach, in particular, provides data de duplication at the file and block level for both cross-user and intra-user users. We create a novel PoW scheme during file-level de duplication to ensure tag consistency and achieve mutual ownership verification. Furthermore, in order to accomplish efficient ownership management, we devise a lazy updating technique.

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

Towards Thwarting Template Side-channel Attacks in Secure Cloud De duplications.

De duplication is one of a few essential cloud storage technologies that help cloud server store duce storage space by eliminating redundant file copies. It does, however, frequently leak side channel information about whether or not an uploading file is de duplicated. 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 de duplication techniques to counter this type of attack. We developed a new cryptographic primitive termed "dispersed convergent encryption" (DCE) scheme and suggested two distinct implementations.

Providing Task Allocation and Secure De duplication for Mobile Crowd sensing via Fog Computing.

Mobile crowd sensing allows a group of people to collect data for a specific consumer using their mobiledevicesinacooperativemanner.Thesuccessofmobilecrowdsensingislargelydetermined 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 de duplication, also known as data elimination, is crucial for improving communication efficiency. Unfortunately, sensing data is frequently encrypted, making de duplication difficult. In this paper, we present a fog-assisted mobile crowd sensing frame work for enhancing task assignment accuracy by allowing fog nodes to allocate tasks depending on user mobility.

Secure Encrypted Data De duplication with Dynamic Ownership Updating.

De duplication eliminates duplicate data copies and lowers cloud service provider storage costs. De duplication of encrypted data, on the other hand, is challenging. Current systems rely significantly on trust worthy third Parties and fail to account for data's popularity, resulting in insufficient security and efficiency. A data De duplication 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, cipher text policy attribute-based encryption is used.

III. PROPOSEDSYSTEM

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.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

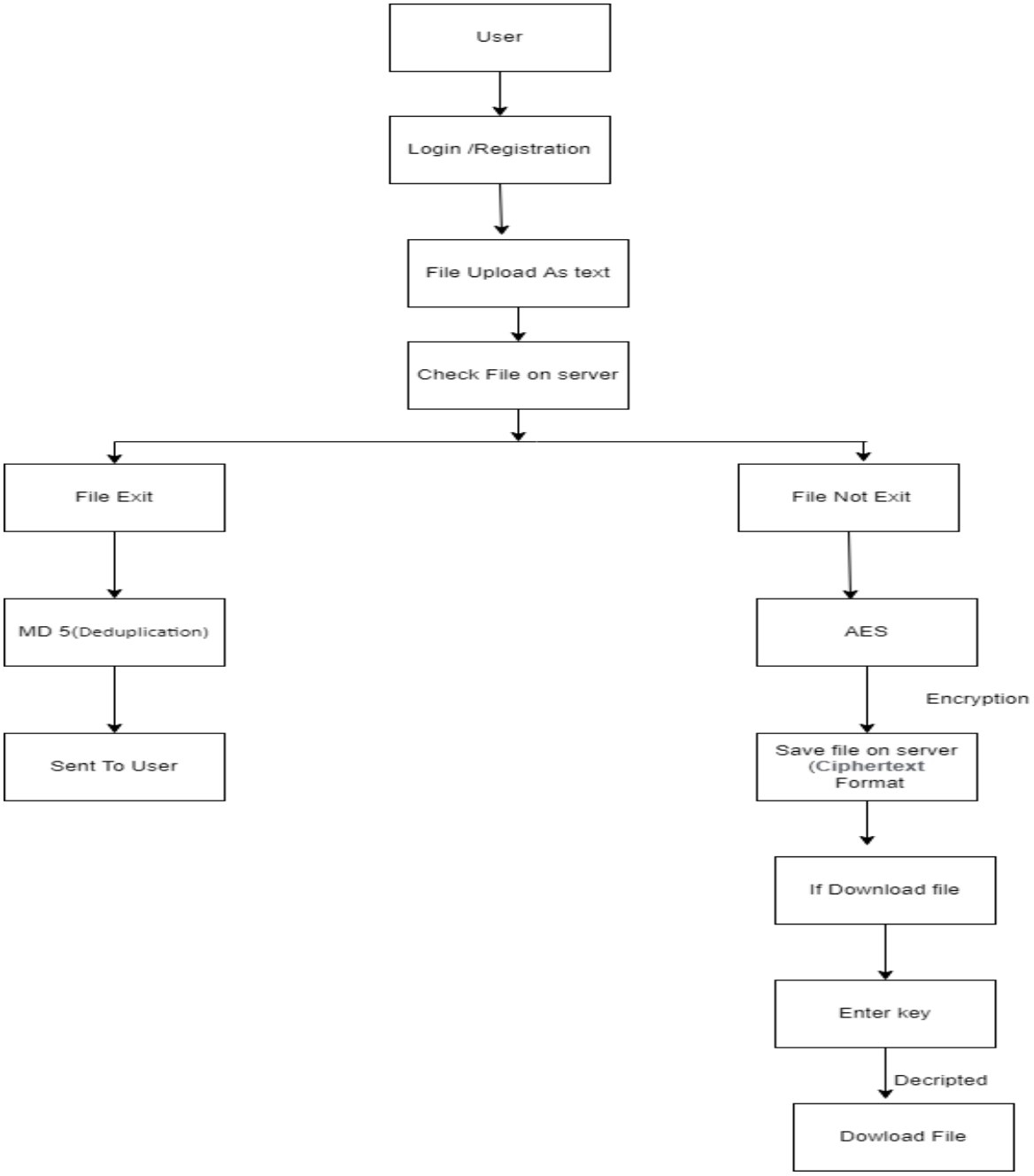

Figure1: The System Architecture.

IV. ALGORITHM

AES algorithm is asymmetrical block cipher method which accepts plain text in format of128-bit blocks and converts it into cipher text 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 cipher 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, cyber security, and data security.

MD5:TheMD5message-digesttechniqueproducesa128-bithashvalueanditiscryptographically 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 byte code, which can execute on any Java virtual machine, regardless of the computer architecture.

V. CONCLUSION

We will avoid de duplication and save files securely in our project. De duplication 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 integritychecking 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,andJ.Han,"Flexibleandfine-grainedattribute-baseddata 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,andJ.Shen,"Usercollisionavoidancecp-abewithefficient 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,andR.Jantti,"CopingwithEmergingMobileSocialMedia ApplicationsThroughDynamicServiceFunctionChaining,"IEEETransactionsonWireless Communications, vol. 15, no. 4, pp. 2859–2871, Apr. 2016.

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

[8] M.J.Atallah,K.B.Frikken,andM.Blanton,"DynamicandEfficientKeyManagementfor 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 Transactionson Big Data, pp. 1–1, 2019.