Image And Text Encryption With Authorized Deduplication In Cloud

Prof. Yogesh Shepal [1], Rushikesh Deshmukh [2], Himanshu Barhate [3], Pooja Daundkar [4]

Computer Engineering Department [1,2,3,4]

Nutan Maharashtra Institute of Engineering and Technology Pune, Maharashtra [1,2,3,4]

Abstract — To secure deduplication plans we have proposed to spare the capacity space in the cloud firstly the AES encryption conspires which utilizes a message inferred key to scramble the message. Subsequently, indistinguishable plaintexts deliver the same cipher writings. Proposed AES, which subsumes concurrent encryption and gives nitty gritty security definitions. Moreover, we utilize an MD5 calculation (message-digest calculation) cryptographic strategy for advanced marks, substance confirmation, and message confirmation. Based on a hash calculation, MD5 checks that the record you send and the beneficiary both get the same record. Thus, cloud computing is the headway to the shared volume of data through the arrange. There are parts of procedures that are utilized to give security for information in the cloud. But current procedures are way better related to the cipher content. So here, we propose data gathering, sharing, and prohibitive dissemination arranged with multi-proprietor security protection in the cloud. Here, the information proprietor can give private data to gather clients through the cloud in a secure.

Index Terms—MD-5 (Message-Digest Algorithm)

I. INTRODUCTION

The project title "Image And Text Encrypted Data With Authorized Deduplication In Cloud" briefly describes the main goals and objectives of a system designed to enhance cloud security management through the use of cryptographic techniques. In brief, this paper outlines the major parts of the project.

It is an arranged-based computing framework and it is an expansive capacity space range where by the authorized client can get to the stage from any place and anytime with a great web or arranged network.[1] Due to the blast development of media substance secure deduplication plans have been proposed to spare space in the cloud.

Firstly, we presented a Progressed Encryption Plot which employments a determined key from a message. In this way, indistinguishable plaintexts lead to the same cipher writings. Proposed AES, which subsumes focalized encryption and gives point-by-point security definitions. Cloud computing is a headway towards the shared volume of data throughout the organization. There are numerous methods utilized for information security in the cloud. But show day strategies are as well distant way better than those related to the cipher content.

So here, we propose data gathering, sharing, and prohibitive conveyance arranged with multi-owner security protection in cloud. Here, information proprietor can share private data with bunches of clients by means of clouds secretly.

II. LITERATURE SURVEY

A privacy-preserving multi-dimensional media sharing scheme named SMACD in mobile cloud computing.[5] Firstly, every media layer is encrypted along with an access strategy based on attribute-based encryption, which guarantees media concealment as well as fine-grained access authority.[6] Then we present a multi-level access strategy construction with a confidential sharing plot. It secures that the mobile users who obtain a media layer at a higher access level must content the access trees of its child layers at the bottom access level., which is cooperative with the characteristics of a multi-dimensional media pool and also decreases the complexity of access strategies. [5] The results declare that SMACD guard's media centers and unsanctioned parties while experiencing less computational and storage costs.

Deduplication reduces storage costs for cloud providers by eliminating duplicate data, but it's tough with encrypted data.[2] Current solutions rely on third parties and don't consider data popularity, leading to security and efficiency issues. A new scheme based on data popularity aims to address these challenges. Check tags are analyzed via bilinear mapping to decide whether different encrypted data emerge from the same plaintext.[8] Ciphertext policy attribute-based encryption is applied to protect the tags. A robust key delivery policy is established to securely transfer the data encryption key from the initial data uploader to subsequent uploaders through the cloud server, employing an offline method.[4]The cloud server can accomplish deduplication without the support of any online third party. Security investigation and simulation experiments are provided, proving the feasibility and efficiency of the proposed policy.

A reliable data deduplication scheme with an efficient PoW process for dynamic ownership management.[8] Our scheme supports cross-level deduplication with a new Proof of Work (PoW) mechanism ensuring tag consistency and mutual ownership verification. We also employ a lazy update strategy for efficient ownership management. Intra-user block-level

deduplication utilizes user-aided keys to minimize key storage.[9] Security and performance analyses confirm our scheme's effectiveness in ensuring data confidentiality, tag consistency, and efficient ownership management.

Deduplication stands out as a crucial technology in cloud storage services, enabling servers to conserve storage space through the removal of duplicate file copies.[7] To thwart this kind of attack, we sort to the anonymity privacy concept to design a secure threshold deduplication protocol. a groundbreaking cryptographic primitive termed "dispersed convergent encryption" (DCE) and introduced two distinct constructions of this scheme. With these DCE policies, we successfully build secure threshold deduplication rules that do not rely on any trusted third party.[1] Our protocols provide not only confidentiality safeguards and ownership verifications but also come with formal security assurances against template side-channel attacks, even in scenarios where the cloud server acts as a "covert adversary," potentially breaching predefined thresholds and covertly performing deduplication.

An efficient secure deduplication scheme includes support for user-defined access control. Specifically, it permits only the cloud service provider to authorize data access on behalf of data owners, ensuring maximal duplicate elimination without compromising cloud users' security and privacy.[7] A thorough security analysis reveals that our authorized secure deduplication scheme upholds data confidentiality and tag consistency while remaining resilient against brute-force attacks. Moreover, comprehensive simulations illustrate that our scheme surpasses existing competitors in computational, communication, and storage overheads, as well as deduplication effectiveness.

The efficient secure deduplication scheme that supports user-defined access control. In particular, by allowing only the cloud service provider to authorize data access on behalf of data owners, our scheme can maximally eliminate duplicates without violating the security and privacy of cloud users.[9] Detailed security analysis shows that our authorized secure deduplication scheme achieves data confidentiality and tag consistency while resisting brute-force attacks. Furthermore, extensive simulations demonstrate that our scheme outperforms the existing competing schemes, in terms of computational, communication, and storage overheads as well as the effectiveness of deduplication.

A Secure and efficient data deduplication scheme (named SED) in a joint cloud storage system that provides global services via collaboration with various clouds. Moreover, SED can overcome the single point of failure that commonly occurs in the classic cloud storage system.[3] According to the theoretical analysis, our SED guarantees semantic security in the random oracle model and has powerful anti-attack resistance and collusion attack resistance. Moreover, SED boasts the capability to efficiently eradicate data redundancies, all while maintaining minimal computational complexity and imposing negligible burdens on communication and storage resources. The efficiency and convenient functionality of SED improve the practicability on the client-side.[3] Finally, the comparing results show that the performance of our scheme is supercilious to that of the existing schemes.

III. SYSTEM ARCHITECTURE

SYSTEM DESIGN

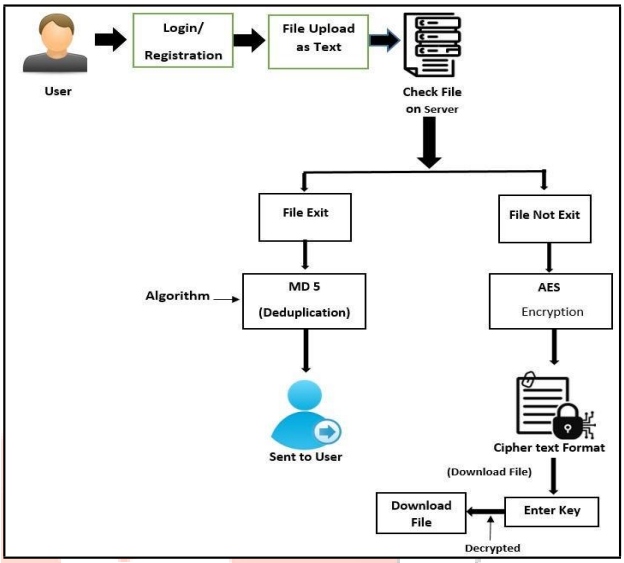


Fig: 1 System Architecture

I. Module

Administrator

In this module, administrators must log in with a valid usernm e and password. Once successfully logged in, you can view a ll users and permissions, view all ecommerce sites and permis sions, view all products and reviews, view all old products, vi ew all search terms, view all search comparisons, view all sea rch terms, and view all search results.

View and authorize users

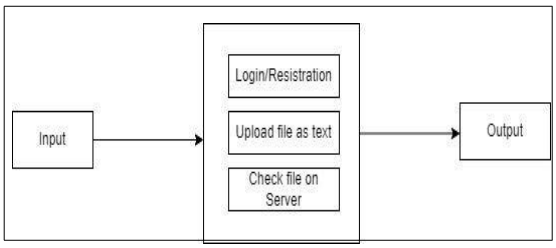
In this model, administrators can view the names of all registe red users. Here the administrator deals with the user details su ch as the user's name, email address, address and the permissi ons the administrator gives to the user.

View chart

View all product price searches, view all search terms, and vie w all product analysis results.

E-Commerce Users

There are n users in this module. Users must register before doi ng this. When a user registers, their information will be stored i n the database. After the registration process is completed, you must log in with your username and password. After successful



IV. CONCLUSION

We have studied various methods to avoid Deduplication using the Encryption and decryption method. For the text uploading we are using the two algorithms, For the uploading in the cloud system we are using the AES Algorithm. To store huge amounts of data efficiently, and to avoid duplicate text and images we are using this encryption technique.

V. OUTPUTS AND RESULTS:

Fig .5 Home Page

Fig .7 Data Uploading Page

Fig .6 Home Page

REFERENCES

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

[2] 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.

[3] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion avoidance cp-abe with efficient attribute revocation for cloud storage," IEEE Systems Journal, pp. 1–11, 2020.

[4] 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 2020.

[5] 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.

[6] 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," IEEE Transactions on Multimedia, vol. 18, no. 5, pp. 940–950, May 2016.

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

[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] 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.

[10] Q Prof. Yogesh Shepal, Hemant C. Chavan, Gaurav B. Khatate, Yogesh P. More "A System To Filter Unwanted Messages From OSN Users Walls," International Journal for Research in Engineering Application & Management (IJREAM) ISSN : 2454- 9150 Vol-03, Issue 03, Apr 2017