isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 1 ,Apr,2021 ,ISSN_NO: 2321-3337

SECURE AND EFFECTIVE CLOUD INFORMATION DEDUPLICATION IN ENCRYPTED CLOUD NDATA

Mr. R.Selvam M.E., Assistant Professor of Computer Science Department,
Ms. D. Ashifa, Student of Computer Science Department,
Ms. K. Thendral, Student of Computer Science Department,
St. Joseph College of Engineering, Sriperumbudur, Chennai

Abstract

Deduplication eliminates duplicated data copies and reduces storage costs of cloud service providers. However, deduplication of encrypted data is difficult. Current solutions rely heavily on trusted third parties, and do not address the popularity of data, resulting in unsatisfying security and efficiency. A secure encrypted data deduplication scheme based on data popularity is proposed. Check tags are calculated via bilinear mapping to determine whether different encrypted data originate from the same plaintext. Cipher text policy attribute-based encryption is applied to protect the tags. A secure key delivery scheme is designed to pass the data encryption key from an initial data uploader to subsequent uploaders via the Cloud server in an offline manner. The cloud server can perform deduplication without the assistance of any online third party. Security analysis and simulation experiments are provided, proving the practicability and efficiency of the proposed scheme.

1. Introduction

Information deduplication is to lessen possession the storage room. Our end goal is to accomplish secure information deduplication. In this paper, we guarantee information secrecy and proposed a protected information label consistency.

deduplication conspire with proficient PoW process for dynamic administration. At long last, the security and execution investigation show that our plan can

Volume: 6, Issue: 3,Special Issue: 1 ,Apr,2021 ,ISSN_NO: 2321-3337

2. Literature Survey

Zhihua Xia and others [1] Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. Due to the use of our special tree-based index structure, the proposed scheme can achieve sublinear search time and deal with the deletion and insertion of documents flexibly.

Zhirong Shen and others [2] A scalable framework where user can use his attribute values and a search query to locally derive a search capability, and a file can be retrieved only when its keywords match the query and the user's attribute values can pass the policy check. Using this framework, we propose a novel scheme called KSAC, which enables Keyword Search with Access Control over encrypted data. To enhance the privacy, KSAC also plants noises in the query to hide users' access privileges.

Jianwei Yin, Yan Tang and others [3] Deploying deduplication for distributed primary storage is a sophisticated and challenging task, considering that the demands of low read/write latency, stable read/write performance, and efficient space saving are all of paramount importance. In this article, we propose D3,a dynamic dual-phase deduplication framework for distributed primary storage.

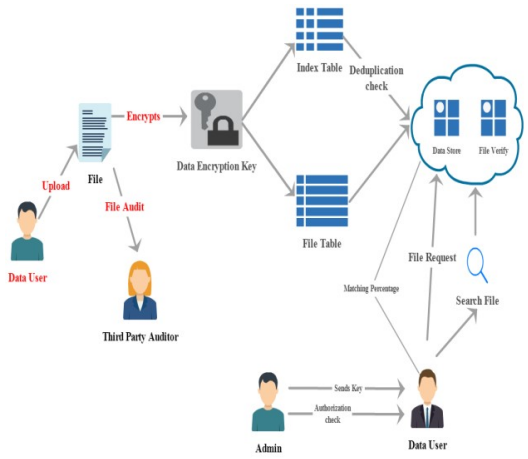
Jiguo Li, Yao Wang and others [4] Attribute based encryption (ABE) is a popular cryptographic technology to protect the security of users' data. However, the decryption cost and ciphertext size restrict the application of ABE in practice. For most existing ABE schemes, the decryption cost and ciphertext size grow linearly with the complexity of access structure. Current research mainly focuses on verifiability of

Volume: 6, Issue: 3,Special Issue: 1 ,Apr,2021 ,ISSN_NO: 2321-3337

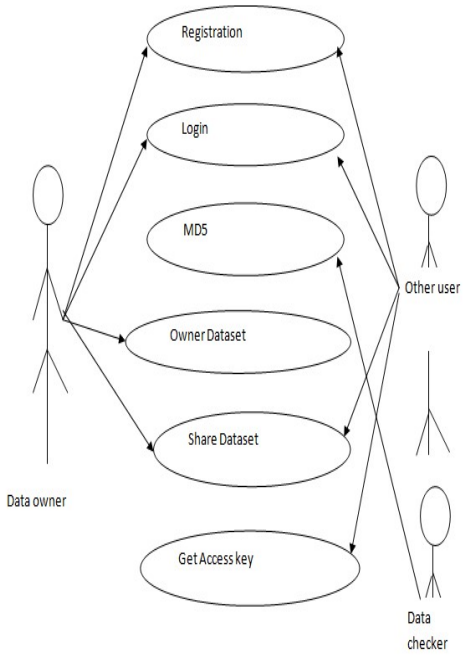
outsourced decryption for the authorized users.

3. System Design

The proposed system solves the drawbacks faced by the existing system while using advanced technologies to ensure future sustainability of the software. Here we uses four modules such as : Data owner, Owner dataset, Third party verifier, Shared dataset and Security.



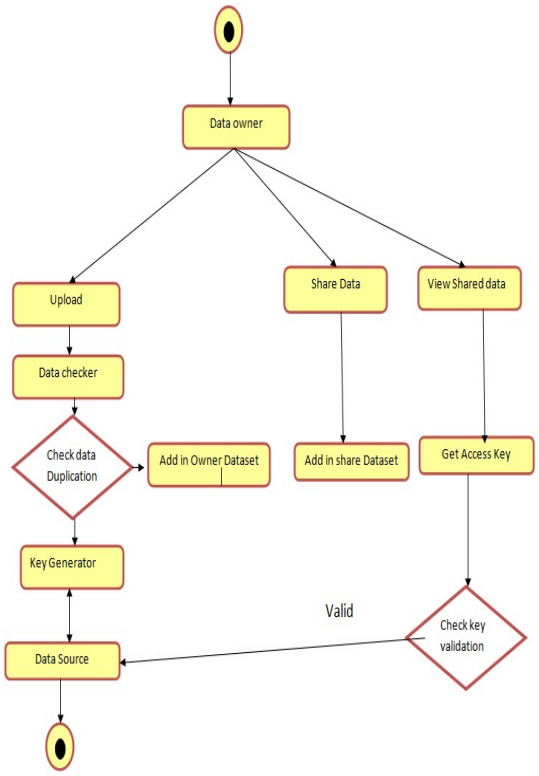
Data owner can upload data's, that data's are split into parts then sends it to trusted data checker, job of the data checker is to generate signature key from MD5 and compare with previous keys, if mismatch then that data send to Key generator Server, Job of the key generator is to generate encryption key as user specified algorithm, finally encrypt then store in Database.



The files will be uploading only once. If another data owner going to upload the same file in database means they will get the notification (the data is already uploaded in database).So data owner can save cost and time. If the file contains the

Volume: 6, Issue: 3,Special Issue: 1 ,Apr,2021 ,ISSN_NO: 2321-3337

same word as was in the file previously saved in the cloud then file will not store instead it shows error .



We are implementing “Dynamic Encryption key Generation”. It means all shared data only view with data owner permission, so we can avoid from unknown access. Social users are group members they can only view and share the data. If want show the data means they need to get permission from data owner. The data owner will send Encryption key after that only they can view the data. If data owner does not provide the

KEY mean user cannot view the file. Data encryption provides an important guarantee for the security and privacy of clients’ data , it limits the manners of the accessibility and availability of the encrypted data.

4. Implementation

AES(acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bit.

STEP1: String name =

res.getString(1);

STEP 2: Byte[] na=name.getBytes()

STEP 3: KeyGenerator keygenerator =

KeyGenerator.getInstance("AES "

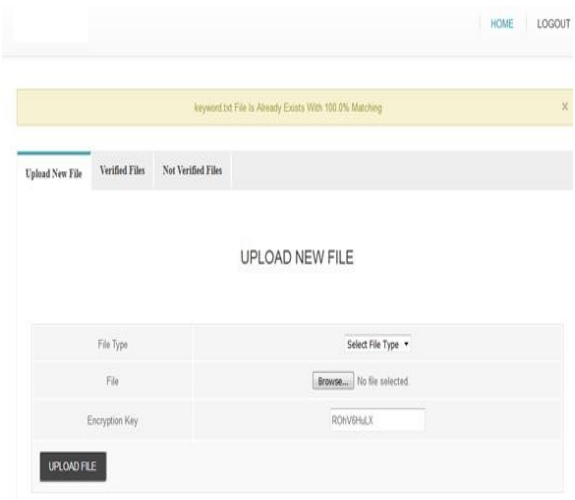
SecretkeymyDeskey=KeyGenerator. generateKey())

STEP 4: Cipher desCipher;

STEP 5: desCipher = Cipher.getInstance("AES");

STEP 6: desCipher.init (Cipher.ENCRYPT_MODE,myDesKey);STEP 7: byte[] na1= desCipher.doFinal(na);

To enhance the security of deduplication and protect the data confidentiality showed how to protect by transforming the predictable message into an unpredictable message. In their system, a third party called key server is introduced to generate the file tag for duplication check. Addressed the key management issue in block-level deduplication by distributing these keys across multiple servers after encrypting the files.



Conclusion and Future Enhancement

we propose a scheme to address the

References

[1]: Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior

deduplication of encrypted data efficiently and securely with the help of ensuring the ownership of the shared file, encrypting data using keys at user's will and realizing the store through the digital credential.

Member, IEEE, and Qian Wang, Member, IEEE 2016 " A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data'' anonymous

[2]: N.Cao, C.Wang, M.Li,K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data" in Proc. of INFOCOM, 2011, pp. 829–837.

[3]: Jianwei Yin,Yan Tang, Shuiguang Deng, Ying Li, and Albert Y. Zomaya, Fellow, IEEE 2017 "A Dynamic Dual-Phase Deduplication Framework for Distributed Primary Storage''

[4]: C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 8, pp. 1467–1479, 2012.