International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

A Secure Code Based Storage System in Cloud

Dr. K. Karuppasamy[1], Margret Sharmila[2]

[1]Professor & Head, RVS College of Engineering and Technology, Coimbatore, India
margretsharmilait[at]gmail.com

[2]Assistant Professor, SNS College of Engineering, Coimbatore, Tamil Nadu, India

Abstract: ***The characteristics of intrinsic information sharing and low maintenance, provides a more robust utilization of resources. In cloud computing, cloud service suppliers provide associate degree abstraction of infinite cupboard space for shoppers to host information. It will facilitate shoppers scale back their money overhead of information managements by migrating the native managements system into cloud servers. However, security issues become the most constraint as we have a tendency to currently source the storage of information that is probably sensitive, to cloud suppliers. To preserve information privacy, a typical approach is to inscribe information files before the shoppers transfer the encrypted information into the cloud. It is tough to style a secure and economical information sharing theme, for dynamic teams within the cloud. and encrypting every file group with a file- block key. However, the file-block keys have to be compelled to be updated and distributed for a user revocation, here for; the system had a significant key distribution overhead. Alternative schemes for information sharing on un-trusted servers are planned. However, the complexities of user participation and revocation in these schemes square measure linearly increasing with the quantity of information house owners and also the revoked users.***

Keywords: Data security, Encryption

1. Introduction

The project deals with the network security of cloud that provides an enhanced data sharing and protects the data from the hackers. The project focuses mainly on Network Security

Existing System

The untrusted data sharing have been proposed in this the encrypted data files are stored by the data owners and the respective decryption keys are distributed to the authorized users. The content of the files cannot be earn by the unauthorized users as they have no knowledge of the decryption keys. The Complexities and revocation is increased. Hence proposed a secure scheme which is based on encryption techniques, it allows the sharing of data between the groups. In the key policy attribute based encryption any user can share and store the data

2. Literature Survey

The fine-grained data owner-side access control in public cloud storage is dishonest. Attribute-based Encryption(ABE) is introduced. Among ABE schemes, CP-ABE is practical in public cloud storage, in which the ciphertext is encrypted under an access policy and only users whose attributes satisfy the access policy can decrypt the ciphertext. Subsequently, many variants and relevant protocols] have been proposed to make CP- ABE more suitable for real scenarios with rich functionalities and security properties in public cloud storage. The cryptography-driven access control does not protect the cloud provider against many other attacks. Since the cloud provider does not conduct the access control, it cannot stop those unauthorized users. One attack that is originated from this limitation is Distributed Denial of Services (DDoS). The power of DDoS attacks has been showed to incur significant resource consumption in CPU, memory, I/O, and network. The attacks can exist in public clouds. In, the limitation of cloud-side static resource allocation model is analyzed, including the risk of Economic Denial of Sustainability (EDoS) attacks, which is the case of DDoS attacks in the cloud setting in, or the Fraudulent Resource Consumption (FRC) attack in. These attacks are intended to break the budget of public cloud customers. Some existing works try to mitigate EDoS attacks. In, the authors proposed a mitigation technique by verifying whether a request comes from a cloud user or is generated by bots. Some existing works discuss the necessary of accounting resource consumption in the public cloud arouses some concerns. In the literature, the authors discussed key issues and challenges about how to achieve accountability in cloud computing. In the literature, the authors surveyed existing accounting and accountability in content distribution architectures. In the literatures and the authors respectively proposed a systematic approach for verifiable resource accounting in cloud computing. However, the accounting approach involves changes to the system model, and requires the anonymous verification of users, which is not supported in previous systems. Compared with relevant schemes, our approach works on the protocol level to provide the resource verifiability that relies on authorized users who satisfy the CP-ABE policy, and achieves the covert security which is more practical and secure.

3. Problem Statement

In the existing system Company use a single server to store and retrieve the data from the cloud. In this existing System there is a possibility of Hacking the data by unauthorized person. There are no safe security mechanisms to transmitting data communication in the existing system

4. Objective

The objective of this project is to satisfy the data robustness, confidentiality and forwarding of data through tight integration which makes an efficient storage. This performs encoding and partial decryption process

5. Proposed System

Anti-collusion information sharing scheme for dynamic companies within the cloud, the customers can securely obtain their private keys from team manager certificates Authorities and secure communication channels. Also, our scheme is equipped to help dynamic corporations efficiently, when a brand new user joins within the workforce or a consumer is revoked from the group, the confidential keys of the opposite customers do not have to be recomputed and updated. Moreover, our scheme can reap at ease user revocation; the revoked customers cannot be equipped to get the usual data documents as soon as they are revoked even though they conspire with the un-trusted cloud.

6. Architecture

Figure 1: Architecture

Modules

1) Registration
2) Sharing Data
3) Secure Cloud Storage
4) Proxy re-encryption 5.Data retrieval

Registration

The group manager adds the identity ID in the user list. The user obtains the private key after the registration and it is used for group signature generation

Sharing Data

The canonical application is data sharing. The public auditing property is especially useful when we expect the delegation to be efficient and flexible. The enable a content provider to share the confidential data in a selective way, with a expansion of fixed and small cipher text, by distributing to each authorized user a single and small aggregate key.

Secure Cloud Storage

The major requirement for storage systems is Data. The replication of a message provides data robustness and the copy of a message gets stored.

Proxe Re-Encryption

It allows third parties to alter a cipher text which has been encrypted for one user, and is decrypted by another user. The encrypted data in the cloud is again altered by the user using proxy re- encryption

Data Retrieval

Reports and data are the two primary forms of the retrieved data from servers. There are some overlaps between them, but queries generally select a relatively small portion of the server. While reports show larger amounts of data.

4. Implementation

If the user does not have an account already, new account has to be created by filling in the registration form.

If the user already exists, the username and password is provided and the file is uploaded.

The file is stored in the cloud by encrypting the file using AES encryption and storing it by splitting it in four servers.

The split files are further hashed using MD5 hashing technique and the 32-bit hexadecimal key is stored in the database. (Proxy Re-encryption).

If the files have to be retrieved, the 16-bit pass key that is given during the time of registration has to be provided and the file that has to be downloaded is selected. The file is downloaded to the specified location.

The whole file can be encrypted by AES and stored in the system which can be shared with another user in the encrypted format.

The shared file can be decrypted by the other user by providing his 16-bit pass-key and decrypting it. The choice to encrypt and decrypt

5. Methodologies

Encryption and Decryption process are performed by using AES algorithm which is a public key encryption technique that can be used to create faster, smaller, and more efficient. MD5 algorithm generates the public key and private key. It is 256-bit encryption. Public key is mailed to the client which is used to access the data stored in database.

6. Conclusion

The combined cloud-side and data owner-side access control in encrypted cloud storage, which is resistant to DDoS/ EDoS attacks and provides resource consumption accounting. Our system supports arbitrary CP-ABE constructions. The construction is secure against malicious data users and a covert cloud provider. security requirement of the cloud provider is relaxed to covert adversaries. The bloom filter is used and probabilistic check in the resource consumption accounting to reduce the overhead.

References

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, vol. 1, no. 1, pp. 7–18, 2010.
[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, no. 1, pp. 69–73, 2012.
[3] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner," Computers & Security, vol. 69, pp. 84–96, 2017. 4)
[4] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.
[5] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, 2012