International Journal of Research in Engineering, Science and Management
Volume-3, Issue-2, February-2020
www.ijresm.com | ISSN (Online): 2581-5792

ABSE: Attribute Based Searchable Encryption Scheme for Cloud Using Encrypt Index

S. Sabitha[1], G. Balamurugan[2], N. Balasubramanian[3]
[1]*Student, Department of MCA, Mohamed Sathak Engineering College, Ramanathapuram, India*
[2,3]*Assistant Professor, Department of MCA, Mohamed Sathak Engineering College, Ramanathapuram, India*

***Abstract*: Cloud computing is growing now-a-days in the interest of technical and business organizations but this can also be beneficial for solving social issues. We propose to increase the data security during the data transmission between the data owner and data user. It ensures both the freshness and integrity of search results across multiple users and data owner. Data Owner provides encrypted proof index corresponding to their data and authenticators to the cloud services. Cloud Server will provide storage and search services. For efficient searching, the cloud using verification key, to keep privacy preservation and achieving the verification requirements and provides the encrypted document with corresponding proof according to the token. The Data user verifies the document with the proof and decrypt the encrypted file if verification is correct. The user has to download the document within in the particular time limit otherwise, the request will get cancelled. Finally, this project increases the data security and enhancing the performance of the overall process.**

***Keywords*: Searchable Encryption, Cloud Storage, Encrypt Index, Search Authentication, Access Control.**

1. Introduction

A. Domain introduction

Cloud computing is the delivery of different service through the internet. These resource include tools and application like data storage, servers, database, networking and software. Cloud computing is the delivery of computing and storage space as a service to a distributed community of end users. The schema/model of Cloud computing is, all the servers, networks, applications and other elements related to data centers are made available to end users. Cloud computing is growing now-a-days in the interest of technical and business organizations but this can also be beneficial for solving social issues. Cloud computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application.

Cloud computing is the on demand availability of computer system resource especially data storage and computing power without direct active management by the user. The term is generally used to describe data centers available to many users over the internet. Large clouds, predominant today, often have functions distributed over multiple location from central servers. If the connection to the user is relatively close, it may be desingnated an edge server. Cloud may be limited to a single organization (enterprise clouds), or be available to many organizations (public cloud). Cloud computing relies on sharing of recourse to achieve coherence and economics of scale.

Advocates of public and hybrid cloud note that cloud computing allow companies to avoid or minimize up-front IT Infrastructure costs. Proponents also claim that cloud computing allow enterprises to get their application up and running faster, with improved manageability and less maintenance, and that it enable IT teams to more rapidly adjust resource to meet fluctuating.

B. Main contributions

1) I design a ciphertext policy Attribute based searchable encryption scheme. This can achieve search and fine-grained access control over encrypted data.
2) Detailed correctness analysis, performance analysis and security proof for proposed CP-ABSE scheme.
3) I implement ABSE scheme and the similar work CP-ABSE scheme proposed in. Extensive experiments in real data set demonstrate that our scheme outperforms CP-ABSE on many aspects.

2. Cloud security

Cloud computing offers an opportunity for individuals and companies to offload to powerful servers the burden of managing large amounts of data and performing computationally demanding operations. 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. Data owners offer services to a large number of businesses and companies, they stick to high security standards to improve data security by following a layered approach that includes data encryption, key management, strong access controls, and security intelligence.

For cloud applications, especially at large scale, one of the primary impediments to system dependability is human error. Human operator error is attributed with being the root cause of 20-50% of system outages. In many cases of outages caused by human operators, they may not be able to respond quickly enough to minimize the impact (e.g. losing traffic, violating SLAs, etc.). Moreover, operators may perform an action that

cannot be fixed entirely, like irreversibly deleting a data store.

A. *Searchable encryption*

Searchable encryption scheme is a cryptographic technique that allows search of information in an encrypted content, file, documents.

SE (Searchable Encryption) is a positive way to protect user's sensitive data.SE allows the server to search encrypted data.

When data and keywords are encrypted, a tag for search purpose is attached to their respective ciphertexts. These tags are generated from the random number that is used when respective ciphertext is created. Support advanced personalized searches with the high accuracy of the search results by using the user models. The first public-key based searchable encryption scheme. These schemes can perfectly realize trusted and transparent verifiability of search results to resist malicious servers.

B. *Attribute-based encryption*

The main concept of attribute-based searchable encryption was introduced by Sahai and Water. In this scheme, a set of descriptive attributes are used to label a user's keys and a ciphertext. ABE is a type of public-key encryption the secret key of user and the ciphertext are dependent upon attribute.

HABE is derived by wang et a. It is designed to cloud storage services. It is combination of HIBE and CP-ABE scheme. There are multiple keys with different usages.

C. *Types of cryptographic*

1) Symmetric ("Private key")
2) Asymmetric ("Public key")

These schemes can well preserve receivers' attribute privacy by hiding attribute information in ciphertexts. I only focus on the data and query privacy and the anonymous attribute-based searchable encryption will be our future work. The keyword authorized private search on public key encrypted data was proposed based on identity-based encryption. Enhance the expressiveness of access structure and flexibility of keyword search authorization, a few attribute-based searchable encryption schemes have been published.

The data owner is able to flexibly control the data user's keyword search permissions in a fine-grained manner by using the promising attribute-based encryption primitive.

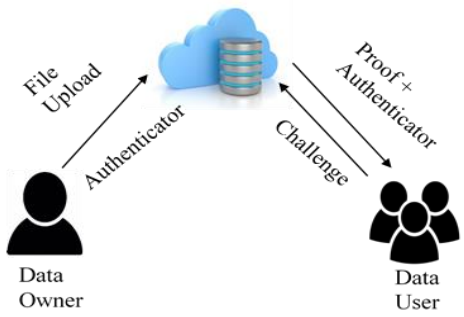

Fig. 1. Architecture

3. System modules

1) Data Owner
2) Encrypt Index
3) Cloud Service Provider
4) Data User

1) Data owner

- Data Owner extracts the keywords of each document and also builds a keyword Index.
- Data Owner encrypts the documents and the keyword Index using a key and outsources in Cloud.
- Data Owner provides the Public Verification Key and Proof Index to the Data User via Cloud for document verification.
- Data Owner is the only authorized person to add, modify, or delete the document(s) from the cloud.

2) Encrypt index

- I introduce cryptography technique to provide data security.
- Searchable encryption provides an effective mechanism that achieves secure search over encrypted data.
- I propose an attribute-based searchable encryption scheme by leveraging the ciphertext-policy attribute-based encryption technique.

3) Cloud service provider

- The Cloud Service Provider can view all the uploaded and downloaded documents in the Cloud.
- The CSP receives the document request from the Data User, verifies the authentication before granting permission.
- Then the CSP executes the query and returns the encrypted document according to the search token.
- And also returns an additional proof with the document, to verify the search result.

4) Data user

- Data User send a request to the cloud server.
- After request granted from the Cloud, the Data User receiving the Public Verification Key from the Cloud generated by Data Owner.
- The Data User now decrypt and download the encrypted documents, after verifying with the Public Verification Key.
- After receiving a verification from cloud, the data user will download the file within a particular time limit.

4. AES algorithm

AES is based on a design structure principle known as a substitution–permutation network, and is efficient in software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael per se is specified with block and key sizes

that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4 × 4 column of bytes. Most AES calculations are done in a particular finite field.

If there are 16 bytes, b0, b1,...,b15 {\display style b_{0},b_{1},...,b_{15}} {\display style b_{0},b_{1},...,b_{15

[b0 b4 b8 b12 b1b5 b9 b13 b2 b6 b10 b14 b3 b7 b11 b15]

{\display style

{\begin{bmatrix}b_{0}&b_{4}&b_{8}&b_{12}\\b_{1}&b_{5}&b_{9}&b_{13}\\b_{2}&b_{6}&b_{10}&b_{14}\\b_{3}&b_{7}&b_{11}&b_{15}\end{bmatrix}}}

{\begin{bmatrix}b_{0}&b_{4}&b_{8}&b_{12}\\b_{1}&b_{5}&b_{9}&b_{13}\\b_{2}&b_{6}&b_{10}&b_{14}\\b_{3}&b_{7}&b_{11}&b_{15}\end{bmatrix}}

The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The numbers of rounds are as follows:

10 rounds for 128-bit keys.

12 rounds for 192-bit keys.

14 rounds for 256-bit keys.

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

5. Conclusion

In this paper, I propose Attribute Based Searchable Encryption Scheme for Cloud Using Encrypt Index ABSE. This scheme can achieve keyword based search and fine-grained access control over encrypted data, simultaneously. I provide detailed performance and security analysis. Also, I implemented by ABSE and a similar work CP-ABSE proposed in. Experimental results demonstrate that our scheme has the better search performance compared with CP-ABSE. The dynamic, forward secure and anonymous attributed-based searchable encryption scheme for Cloud Using Encrypt Index ABSE is our future work.

References

[1] Hui Yin, Jixin Zhang, Yinqiao Xiong, Lu Ou, Fangmin Li, Shaolin Liao and Keqin Li, “CP-ABSE: A Ciphertext-Policy Attribute-Based Searchable Encryption Scheme” IEEE Access, Volume 7, 2019

[2] H. Zhu, L. Wang, H. Ahmad, and X. Niu, ``Key-policy attribute-based encryption with equality test in cloud computing," IEEE Access, vol. 5, pp. 20428-20439, 2018.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, ``Privacy-preserving multi keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222-233, Jan. 2014.

[4] W. Sun et al., ``Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 11, pp. 3025-3035, Nov. 2014.

[5] Z. Xia, X. Wang, X. Sun, and Q. Wang, ``A secure and dynamic multi keyword ranked search scheme over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340-352, Jan. 2016.