CIPHER TEXT ATTRIBUTE-BASED MECHANISM WITH KEYWORD SEARCH AND DATA SHARING FOR CLOUD COMPUTING

Mr.E.Ramesh Reddy, Associate Professor , Dept of CSE,NECG.
B.Kavitha,(17F11A0513), **A.Abhilasha**,(17F11A0503) **N.Nishitha** ,(16F11A0564) Dept of CSE,NECG.

ABSTRACT

The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality. To overcome these problems, cipher text-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword can be updated during the sharing phase without interacting with the PKG CPAB-KSDS as well as its security model. Besides, prove that it is against chosen cipher text attack and chosen keyword attack secure in the random oracle model.

I.INTRODUCTION

Cloud computing has been the remedy to the problem of personal data management and maintenance due to the growth of personal electronic devices[1]. It is because users can outsource their data to the cloud with ease and low cost. The emergence of cloud computing has also influenced and dom inated Information Technology industries. It is unavoidable that cloud computing also suffers from security and privacy challenges[2].

Encryption is the basic method for enabling data confiden tiality and attribute-based encryption is a prominent representative due to its expressiveness in user's identity and data. After the attribute-based encrypted data is uploaded in the cloud, authorized users face two basic operations: data searching and data sharing. Unfortunately, traditional attribute based encryption just ensures the confidentiality of data. Hence, it does not support searching and sharing.

II.LITERATURE SURVEY

1. Identity-based conditional proxy re-encryption with fine grain policy:

An identity-based conditional proxy re-encryption scheme (IB-CPRE) allows a semi-trusted proxy to convert a ciphertext satisfying one condition, which is set by the delegator, under one identity to another without the necessity to reveal the underlying message. In ICISC 2012, Liang, Liu, Tan, Wong and Tang proposed an IB-CPRE scheme, and left an open problem on how to construct chosen-ciphertext secure IB-CPRE supporting OR gates on conditions. aforementioned problem by constructing an identity-based conditional proxy re-encryption scheme with fine grain policy (IB-CPRE-FG)[3][4]. In an IB-CPRE-FG scheme, each ciphertext is labeled with a set of descriptive conditions and each re-encryption key is associated with an access tree that specifies which type of ciphertexts the proxy can re-encrypt. Furthermore, our scheme can be proved secure against adaptive access tree and adaptive identity chosen-ciphertext attack.

2.A cca-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system:

The notion of attribute-based proxy re-encryption extends the traditional proxy re-encryption to the attribute-based setting. In an attribute-based proxy re-encryption scheme, the proxy can convert a ciphertext under one access policy to another ciphertext under a new access policy without revealing the underlying plaintext. Attribute-based proxy re-encryption has been widely used in many

applications, such as personal health record and cloud data sharing systems. the notion of key-policy attribute-based proxy re-encryption, which supports any monotonic access structures on users' keys[5][6]. Furthermore, scheme is proved against chosen-cipher text attack secure in the adaptive model.

3.Privacy-preserving attribute-based keyword search in shared multi-owner setting:

Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) facilitates search queries and supports fine-grained access control over encrypted data in the cloud[7]. However, prior CP-ABKS schemes were designed to support unshared multi-owner setting, and cannot be directly applied in the shared multi-owner setting (where each record is accredited by a fixed number of data owners), without incurring high computational and storage costs. In addition, due to privacy concerns on access policies, most existing schemes are vulnerable to off-line keyword-guessing attacks if the keyword space is of polynomial size. Furthermore, it is difficult to identify malicious users who leak the secret keys when more than one data user has the same subset of attributes. In this paper, a privacy-preserving CP-ABKS system with hidden access policy in Shared Multi-owner setting (basic ABKS-SM system), and demonstrate how it is improved to support malicious user tracing (modified ABKS-SM system). then prove that the proposed ABKS-SM systems achieve selective security and resist off-line keyword-guessing attack in the generic bilinear group model. evaluate their performance using real-world dataset[8].

III.EXISTING SYSTEM

Cloud storage services have several advantages, such as ease of use and cost saving, and they are widely used in many fields. However, several challenges are associated with them. With the increasing popularity of cloud storage, security issues have become an important factor restricting its development. In recent years, data leakage accidents have repeatedly occurred in such companies as Microsoft, Google, Amazon, and China's Home Inn, Hanting, and Ctrip, and these incidents have exacerbated users' worries[9].

To counter the information leakage, data owners and enterprises typically outsource the encrypted business data, rather than the plaintext data, to cloud storage servers. In general, the outsourced data can be divided into three types. The first type is the open-resource-type data, which do not need to be hidden from the cloud server, such as the basic information of the enterprise and the parameters of products.

The second type is the private data, which need to be encrypted but are only accessed and decrypted by the data contributor . This type includes such data as internal confidential information, intellectual properties and patents. The third type is the private data that need to be encrypted but can also be shared with specific users or groups . This type includes internal shared data, hospital's division-wide case information and information by some shared advanced users[10].

Drawbacks

- There is no unified framework to process bulk spatial database data.
- There is no unified cost function to process spatial quires.

IV.PROPOSED SYSTEM

All of these concerns motivate us to design a mechanism that

Allows the data owner to search and share the encrypted health report without the unnecessary decryption process. Supports keyword updating during the data sharing phase. More importantly, does not need the exist of the PKG, either in the phase of data sharing or keyword updating. The data owner can fully decide who could access the data he encrypted.

First point out a notion of ciphertext206 policy attribute-based mechanism with keyword search and data sharing (cpab - ksds), which also supports keyword updating.

In this work, a new notion of cipher text-policy attribute- based mechanism (cpab – ksds) is introduced to support keyword searching and data sharing. A concrete cpab - ksds scheme has been constructed its cc security in the random oracle model. The proposed scheme is demonstrated efficient and practical in the performance and property comparison.

Advantages

- Data leakage with data recovery techniques.
- Fast techniques to find attackers.

V.MODULES

A.Owner

In this module owner will have to register and get authorized before he performs any operations. After the authorization the sender can upload file with trapdoor and will have the update, delete, verify and recovery options for the file uploaded.

B.Cloud Server

In this module Cloud Server will issue SDI for both owner (Alice) and user (bob). And view the file uploaded and the attackers related to files in cloud. View the files in decrypted format and with the corresponding secret keys and its transactions.

C. User

In this module, User has to register and login, and search for the files by entering keyword and request secret key and download the particular file from the cloud if both secret key and the decryption permissions are provided.

D.Security device issuer

Views all the files decrypt permission reqest form the users and provide permission and view its related metadata and the transactions related to the requests from users.

E.Central Authority

In this module the central Authority generates the secret key. It splits the key into two parts such as pkey1 and pkey2. This generated key is unique for different users for same file and view all the generated secret keys and the transactions related to it.

VI.CONCLUSION

In this work, a new notion of ciphertext-policy attribute based mechanism (CPAB-KSDS) is introduced to support keyword searching and data sharing. A concrete CPAB-KSDS scheme has been constructed its CCA security in the random oracle model. The proposed scheme is demonstrated efficient and practical in the performance and property comparison. This paper provides an affirmative answer to the open challenging problem pointed out in the prior work, which is to design an attribute based encryption with keyword searching and data sharing without the PKG during the sharing phase. Furthermore, our work motivates interesting open problems as well including designing CPAB-KSDS scheme without random oracles or proposing a new scheme to support more expressive keyword search.

REFERENCES

[1] C. Ge, W. Susilo, J. Wang, and L. Fang, “Identity-based conditional proxy re-encryption with fine grain policy,” Computer Standards & Interfaces, vol. 52, pp. 1–9, 2017.
[2] C. Ge, W. Susilo, J. Wang, Z. Huang, L. Fang, and Y. Ren, “A key policy attribute-based proxy re-encryption without random oracles,” The Computer Journal, vol. 59, no. 7, pp. 970–982, 2016.
[3] C. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, “A cca-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system,” Designs, Codes and Cryptography, pp. 1– 1065 17, 2018.
[4] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, “Cp-abse: A ciphertext-policy attribute-based searchable encryption scheme,” IEEE Access, vol. 7, pp. 5682–5694, 2019
[5] Y. Miao, X. Liu, K.-K. R. Choo, R. H. Deng, J. Li, H. Li, and J. Ma, “Privacy-preserving attribute-based keyword search in shared multi-owner setting,” IEEE Transactions on Dependable and Secure Computing, 2019
[6] L. Fang, W. Susilo, C. Ge, and J. Wang, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” Information Sciences, vol. 238, pp. 221–241, 2013.
[7] P Ravinder Rao,Dr. V.Sucharita,A Framework to Automate Cloud based Service Attacks Detection and Prevention, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 2, 2019.
[8]P Ravinder Rao,Dr. V.Sucharita,A secure cloud service deployment framework for DevOps Indonesian journal of Electrical Engineering and Computer Science, 2020, 21(2), pp. 874–885
[9] P Ravinder Rao,Dr.V.Sucharita,”A framework to automate cloud based service attacks detection and prevention”. International Journal of Advanced Computer Science and Applications, 2019, 10(2), pp. 241–250
.[10] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie, “A dfa-based functional proxy re-encryption scheme for secure public cloud data sharing,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667–1680, 2014.