OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SURVEY ON ROBUST TRACEABLE KEYWORD SEARCH ON CLOUD STORAGE

Suraj Shinde[1], Toshal Gore[2], Achla Kumari[3], Prof. Anuja Palhade[4]

UG Student, Department of Information Technology Engineering, DPCOE, Pune[1,2,3]
Assistant Professor, Department of Information Technology Engineering, DPCOE, Pune[4]
shindesuraj2611@gmail.com[1], tosh2901@gmail.com[2], achlajha110@gmail.com[3], anujhapalhadedpcoe@gmail.com[4]

Abstract: The administration of access control and the support of keyword search are some issues which are important in secure cloud storage system. With the use of cloud computing, data owners outsource their tricky data management systems from local sites to the commercial public cloud to achieve flexibility and economic savings. But to protect data privacy, sensitive data has to be encrypted before outsourcing the data, which outdated the traditional data utilization based on plaintext keyword search. Considering a number of data users and documents in the cloud, it is mandatory to allow multiple keywords in the search request and return documents in the order of their relevance of these keywords. This system design will provide an efficient traceable authorization search system for secure cloud storage, which overcomes these entire limitations- inflexible authorized keyword search, abuse of attribute secret key, inefficient decryption.

Keywords— *Authorized searchable encryption, Traceability, Multiple keywords subset search, Cloud computing.*

I INTRODUCTION

Secure search over encrypted remote data is crucial in cloud computing to provide guaranteed data privacy and usability. Avoiding unauthorized data usage, fine-grained access control is necessary in multi-user system. Sometimes, authorized users also leak the secret key for financial benefit. Thus, tracing and revoking the malicious person who abuses the secret key needs to be solved imminently. Cloud computing is a totally fascinating computing paradigm, wherein computation and storage are moved far from terminal gadgets to the cloud. This new and popular paradigm brings important revolutions and makes bold improvements for the way wherein businesses and individuals manipulate, distribute, and proportion content. By outsourcing their information technology skills to a few cloud carrier providers, cloud users may also achieve significant fee financial savings. With the arrival of cloud computing, data owners are motivated to outsource their complex records management systems from local websites to the commercial public cloud for notable flexibility and economic savings. But for protective data privateness, data must be encrypted before outsourcing, which obsoletes conventional facts utilization based on plaintext key-word search. Thus, allowing an encrypted cloud data search service is of paramount significance. Considering the multiple number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords.

II LITERATURE SUREVY

Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE) is defined and solved. A set of strict privacy requirements for such a secure cloud data utilization system is established. Among various multi-keyword semantics, a concept of e efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query is used. Also, "inner product similarity" is used to quantitatively evaluate such similarity measure. First a basic idea for the MRSE based on secure inner product computation is proposed, and then two significantly improved MRSE schemes are given to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, these two schemes to support more search semantics are extended further. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is performed. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication. [4]

Adaptively Secure Identity-Based Broadcast Encryption with a Constant-sized Cipher text

An adaptively secure identity-based broadcast encryption system featuring constant sized cipher text in the standard model is presented. The size of the public key and the private keys of the system are both linear in the maximum number of receivers. Also, the system is fully collusion-resistant and has stateless receivers. Compared with the state-of-the-art, the scheme is well optimized for the broadcast encryption. The computational complexity of decryption of this scheme depends only on the number of receivers, not the maximum number of receivers of the system. Technically, dual system encryption technique is employed and the proposal offers adaptive security under the general subgroup decisional assumption. The scheme demonstrates that the adaptive security of the schemes utilizing a composite order group can be proven under the general subgroup decisional assumption, while many existing systems working in a composite order group are secure under multiple subgroup decision assumptions. It is noted that this finding is of an independent interest, which may be useful in other scenarios. [1]

Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption

Attribute-based encryption (ABE) provides a mechanism for complex access control over encrypted data. However in most ABE systems, the ciphertext size and the decryption overhead, which grow with the complexity of the access policy, are becoming critical barriers in applications running on resource-limited devices. Outsourcing decryption of ABE ciphertexts to a powerful third party is a considerable manner to solve this problem. Since the third party is usually believed to be untrusted, the security requirements of ABE with outsourced decryption should include privacy and verifiability. Namely, any adversary including the third party should learn nothing about the encrypted message, and the correctness of the outsourced decryption is supposed to be verified efficiently. Generic constructions of CPA-secure and RCCA-secure ABE systems with verifiable outsourced decryption from CPA-secure ABE with outsourced decryption, respectively are proposed. Also instantiate our CPA-secure construction in the standard model is instantiated and then, an implementation of this instantiation is shown. The experimental results show that, compared with the existing scheme, this CPA-secure construction has more compact ciphertext and less computational costs. Moreover, the techniques involved in the RCCA-secure construction can be applied in generally constructing CCA-secure ABE, which we believe to be of independent interest. [2]

Efficient Privacy-Preserving Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption

A new construction of CP-ABE, named Privacy Preserving Constant CP-ABE that significantly reduces the ciphertext to a constant size with any given number of attributesis proposed. Furthermore, PP-CP-ABE leverages a hidden policy construction such that the recipients' privacy is preserved efficiently. As far as it is known, PP-CP-ABE is the first construction with such properties. Furthermore, a Privacy Preserving Attribute Based Broadcast Encryption (PP-AB-BE) scheme is developed. Compared to existing Broadcast Encryption (BE) schemes, PP-AB-BE is more flexible because a broadcasted message can be encrypted by an expressive hidden access policy, either with or without explicit specifying the receivers. Moreover, PP-AB-BE significantly reduces the storage and communication overhead to the order of O(log N), where N is the system size. Also, it is proved using information theoretical approaches that PP-AB-BE attains minimal bound on storage overhead for each user to cover all possible subgroups in the communication system. [3]

Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Gussing Attack

In public-key encryption with fuzzy keyword search (PEFKS), each keyword corresponds to an exact keyword search trapdoor and a fuzzy keyword search trapdoor. Two or more keywords share the same fuzzy keyword trapdoor. To search encrypted documents containing a specific keyword, only the fuzzy keyword search trapdoor is provided to the third party, i.e., the searcher. Thus, in PEFKS, a malicious searcher can no longer learn the exact keyword to be searched even if the keyword space is small. A universal transformation is proposed, which converts any anonymous identity-based encryption (IBE) scheme into a secure PEFKS scheme. Following the generic construction, the first PEFKS scheme is instantiated, which is proven to be secure under KGA in the case that the keyword space is in a polynomial size. [5]

J. Lai, R. H. Deng, C. Guan, and J. Weng, “Attribute-based encryption with verifiable outsourced decryption,” IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 1343-1354.

A simple and generic method to convert any ABE scheme with non-verifiable outsourced decryption to an ABE scheme with verifiable outsourced decryption in the standard model is proposed. To concretely assess the performance of the new method, an instantiation of the generic method based on Green et al.’s outsourced CPABE scheme without verifiability is presented. [6]

III EXISTING SYSTEM

A distributed attribute based encryption technique is introduced because Ciphertext Policy Attribute-Based Encryption allows encrypting data under an access policy, specified as a logical combination of attributes. Such cipher-texts can be decrypted by anyone with a set of attributes that fits the policy. But in distributed attribute-based encryption, an arbitrary number of parties can be present to maintain attributes and their corresponding secret keys. This is in bare difference to the classic ciphertext policy attribute based encryption schemes, where all keys are distributed by one central trusted party. We provide the construction of a DABE scheme; the construction is very efficient for encryption and decryption.

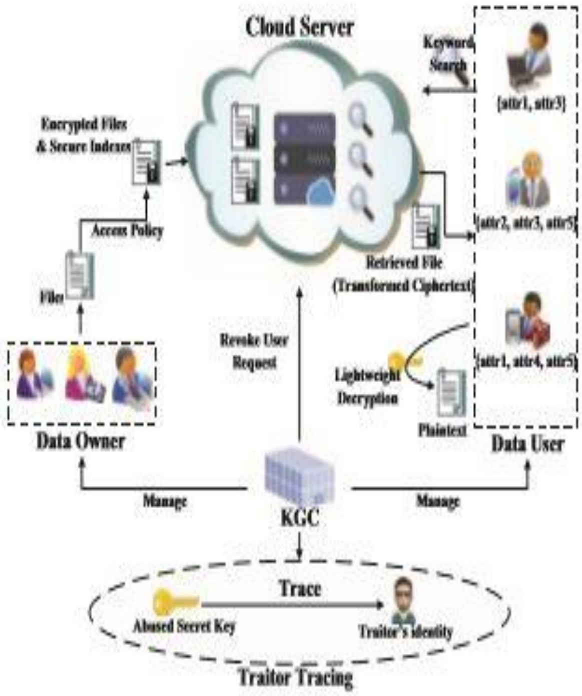

Figure 1: Existing System Architecture

In Secure Attribute-Based systems, attributes define and classify the data to which they are assigned. However, traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments. Novel secure information management architecture is introduced based on emerging attribute-based encryption primitives. A policy system that meets the needs of complex policies is defined and illustrated. Based on the needs of those policies, cryptographic optimizations that vastly improve enforcement efficiency are proposed.

IV PROPOSE SYSTEM

This system design will provide an efficient traceable authorization search system for secure cloud storage, which overcomes all limitations of existing system. Inflexible authorized keyword search, abuse of attribute secret key, inefficient decryption. Sometimes authorized user may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the unauthorized user who abuses secret key needs to be solved imminently.

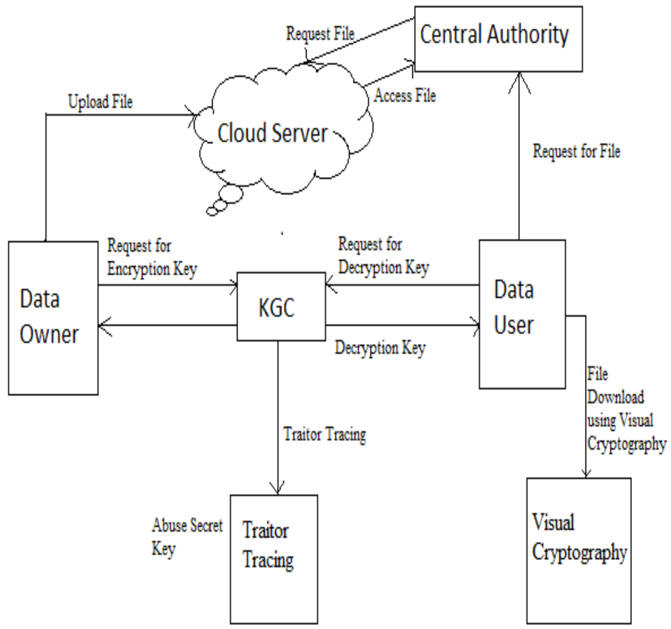

Figure 2: Propose System Architecture

V CONCLUSION

In this work, a new paradigm of searchable encryption system and a concrete construction is proposed, and a system that will provide secure, trustful and reliable communication is developed. In future the data can be divided and placed on multiple cloud servers to achieve more security.

REFERENCES

[1] J. Kim, W. Susilo, M. Au and J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 3, pp. 679-693.

[2] X. Mao, J. Lai, Q. Mei, K. Chen and J. Weng, "Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption," IEEE Transactions on Dependable and Secure Computing, publish online, DOI: 10.1109/TDSC.2015.2423669.

[3] Zhou, D. Huang, and Z. Wang. "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption." IEEE Transactions on Computers, 2015, vol. 64, no.1, pp. 126- 138.

[4]. N. Cao, C. Wang, M. Li, K. Ren, W. Lou. "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on parallel and distributed systems, 2014, 25(1): 222- 233.

[5]. P. Xu, H. Jin, Q. Wu and W. Wang, "Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Gusssing Attack," IEEE Transactions on Computers, 2013, vol. 62, no. 11, 2266-2277.

[6]. J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 1343- 1354.