Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 9, Issue. 1, January 2020, pg.137 – 143

Identity-Based Authentication with Efficient Traceable System in Cloud Storage

[1]R.Prabhu; [2]G.Haripriya; [3]V.S.Janasathyaa; [4]M.Keerthika; [5]T.Pushpalatha
[1]Assistant Professor, Department of CSE, VSBCETC, Coimbatore, India
[2]UG Scholar, Department of CSE, VSBCETC, Coimbatore, India

ABSTRACT: Secure search over encrypted remote data is crucial in cloud computing to ensure data privacy andusability. To prevent unofficial data access and usage fine-grained access control is important in the multi-user system. Whereas, an authorized user may intentionally leak the secret key for financial benefit. So, tracing and revoking such maltreat user who abuses secret key needs to be solved. The key escrow free procedure can be used which will effectively prevent the Key Generation Centre (KGC) from unprincipled searching and decrypt all encrypted filesof users. The decryption process involves here only requires ultra-lightweight computation, which is a desirable featurefor energy-limited devices. If we figure out malevolent user we can efficiently revoke that user. Again if we haveadaptable multiple keywords subset search pattern, which will also not affect the order of search results.
Keywords: Authorized Penetrating Encryption, Traceability, Multiple Keywords Subset Search

I. INTRODUCTION

Nowadays, with the development of a new computing paradigm, cloud computing becomes the most notable one, which provides convenient, on-demand services from a shared pool of configurable computing resources. Therefore, an increasing number of companies and individuals prefer to outsource their data storage to the cloud server. Despite the huge economic and technical advantages, unpredictable security and privacy concerns become the most prominent problem that hinders the widespread adoption of data storage in public cloud infrastructure. Encryption is a essential method to protect data privacy in

remote storage. But, how to effectively carry out keyword searches for plaintext becomes difficult for encrypted data due to the unread ability of cipher text. A searchable encryption mechanism enables keyword to search over encrypted data. For the file-sharing system, such as a multi-owner multiuser scenario, fine-grained search authorization is a desirable function for the data owners to share their private data with other authorized users. But, most of the available systems [7], [8] require the user to perform a large amount of complex bilinear pairing operations. These overwhelmed computations become a heavy burden for the user's terminal, which is especially serious for energy-constrained devices. The outsourced decryption method allows users to recover the message with ultra-lightweight decryption. But, the cloud server might return the incorrect half- decrypted information as a result of a malicious attack or system malfunction. Thus, it is an important issue to guarantee the exactness of outsourced decryption in public-key encryption with keyword search (PEKS) system.

The authorized organization may illegally leak their secret key to a third party for profits. Suppose that a patient someday suddenly finds out that a secret key corresponding to his electronic medical data is sold on e-Bay. Such despicable behavior seriously intimidates the patient's data privacy. Even worse, if the private electronic health data that contain serious health disease is abused by the insurance company or the patient's employment corporation, the patient would be declined to renew the medical insurance or labor contracts. The intentional secret key leakage seriously wear away the foundation of authorized access control and data privacy protection. Thus, it is extremely urgent to identify the malicious user or even prove it in a court of justice. In an attribute-based access control system, the secret key of the user is associated with a set of attributes rather than an individual's identity. As the search and decryption officials can be shared by a set of users who own the same set of attributes, it is hard to trace the original key owner. Providing traceability to a fine-grained explore authorization structure is critical and not considered in previous searchable encryption systems.

II. RELATED WORK

In this paper, out of the blue we distinguish and take care of the issue of successful yet secure positioned catchphrase look over scrambled cloud information. Positioned seek incredibly improves framework convenience by restoring the coordinating records in a positioned request with respect to certain importance criteria (e.g., watchword recurrence), in this way making one step closer towards down to earth arrangement of protection safeguarding information facilitating administrations in Cloud Computing. Supports efficient ranked keyword search for achieving effective utilization of remotely stored encrypted data in Cloud Computing [1].

In a cipher text-policy attribute-based encryption (CP-ABE) framework, decoding keys are characterized over characteristics shared by numerous clients. Given an unscrambling key, it may not be continuously conceivable to follow to the first key proprietor. As a decoding benefit could be controlled by various clients who claim the equivalent set of characteristics, vindictive clients may be enticed to release their unscrambling benefits to some outsiders, for monetary benefit or instance, without the danger of being gotten. This issue extremely constrains the uses of CP-ABE. A few traceable CP-ABE (T-CP-ABE) frameworks have been proposed to address this issue, yet the expressiveness of approaches in those frameworks is restricted where just AND entryway with trump card is as of now bolstered [2].Attribute-Based Encryption (ABE) with re-appropriated unscrambling not just empowers fine-grained sharing of scrambled information, yet additionally beats the proficiency disadvantage (in the wording of cipher text

size and unscrambling cost) of the standard ABE plans. In particular, an ABE plot with redistributed decoding permits an outsider (e.g., a cloud server) to change an ABE cipher text into a (short) El Gama-type cipher text utilizing an open change key given by a client with the goal that the last can be decoded considerably more effective than the previous by the client. In any case, a deficiency of the first redistributed ABE conspire is that the accuracy of the cloud server's change cannot be checked by the client [3].

Inquiry over encoded information is a basic vital empowering strategy in distributed computing, where encryption- before outsourcing is a key answer for securing client information protection in the untrusted cloud server condition. In this paper, we centered on an alternate yet additionally difficult situation where the re-appropriated dataset can be contributed from different proprietors furthermore, are accessible by different clients, i.e. multi-client multi-contributor case [4].

Double Server Public Key Encryption with Keyword Search (DS-PEKS). As another primary commitment, we characterize another variation of the Smooth Projective Hash Functions (SPHFs) alluded to as straight and homomorphic SPHF (LH-SPHF) [5].

Attribute-based encryption (ABE) is an open key-based one-to-numerous encryption that enables clients to encode and unscramble information dependent on client properties. A promising application of ABE is adaptable access control of scrambled information put away in the cloud, utilizing access polices and credited characteristics related to private keys and cipher texts [6].

To date, the development of electronic individual information leads to a pattern that information proprietors want to remotely redistribute their information to mists for the satisfaction in the astounding recovery also, capacity benefit without stressing the weight of neighborhood information administration and upkeep. Nonetheless, a secure offer and pursuit of the re-appropriated information is a considerable assignment, which may effectively cause the spillage of touchy individual data. Effective information sharing and seeking security are of basic significance [7].

This paper proposes a toolkit for efficient and privacy-preserving outsourced calculations under multiple encrypted keys, which we refer to as EPOM. Using EPOM, a large scale of users can securely outsource their data to a cloud server for storage. Moreover, encrypted data belonging to multiple users can be processed without compromising on the security of the individual users (original) data and the final computed results. To reduce the associated key management cost and private key exposure risk in EPOM, we present a Distributed Two-Trapdoor Public-Key Cryptosystem (DT-PKC), the core cryptographic primitive [8].

An extensive of information, for the most part alluding to huge information, has been produced from Web of Things. In this paper, we present a twofold projection profound calculation demonstrate (DPDCM) for enormous information include learning, which extends the crude contribution to two separate subspaces in the shrouded layers to learn associated highlights of huge information by supplanting the shrouded layers of the ordinary profound calculation demonstrate (DCM) with twofold projection layers [9].

Multi-catchphrase rank accessible encryption (MRSE) restores the best k results in light of an information client's demand of multi-catchphrase seek over encoded information, and henceforth gives a productive path for safeguarding information security in distributed storage frameworks while without loss of information ease of use. MRSE framework which conquers every one of the deformities of the KNN-SE based MRSE frameworks [10].

III. ATTRIBUTES-BASED PREDICTION

Attribute-based encryption is a type of encryption in which the secret key of a user and the cipher text are dependent upon attributes. As a result, a user can decrypt a cipher text if and only if there is a match between the attributes which are listed in the cipher text and the attributes which he holds. ABE schemes have been the primary focus in the research community nowadays as it allows flexible access control and can protect the confidentiality of sensitive data. This scheme requires the central authority. But with the advancement in the research, this need is removed because each user can join the system when he wants and can leave the system independent of the other users. This reduces the time that we require to change their secret keys and to reinitialize the system [20].

Security Requirement

TAMKS-VOD system needs to satisfy the following security requirements.

The cipher text and keyword are indistinguishable. If the TAMKS-VOD system possesses the property of indistinguishable then the attacker is not capable to distinguish pairs of cipher texts based on pairs of plain text files. Similarly, pairs of secure keyword index cannot be distinguished based on pairs of keyword. The TAMKS-VOD system should be indistinguishable against chosen keyword set and chosen plain text attack (IND-CKCPA). The security model Of IND-CKCPA is defined.

1 In the Supplemental Materials, where the explanation of the security model is provided.

Tractability: The security need of tractability means that any adversary cannot forge a well-formed secret key. In that way, any well-formed secret key that is sold for benefit can be traced. The identity of malicious user who leaks the key can be discovered. The security model of tractability is defined in Section B.

2 in the Supplemental Materials, where the explanation of the security model is provided.

SYSTEM MODEL

The system model of TAMKS-VOD is show in Fig. 1, and the formal definition was provided.

The system comprises of four entities, whose responsibilities and interactions are described below.

(1) Key generation centre (KGC). It is responsible for generating the public parameter for the system and the public/secret key pairs for the users. Once the user's secret key is leaked for profits or other purposes, It runs trace algorithm to find the malicious user. After the traitor is traced, KGC sends user revocation request to cloud server to revoke the user's search privilege.

(2) Cloud server (CS). Cloud server has tremendous storage space and powerful computing capability, which provides on-demand service to the system. Cloud server is only responsible to store the data owner's encrypted files, data and respond to data user's search query.

(3) Data owner. Data owner uses the cloud storage service to store the files. Before the data outsourcing, the data owner retrieved the keyword set from the file and encrypts it into secure index. The document is also encrypted to cipher text. During the encryption process, the access policy was specified and embedded into the cipher text to realize fine grained access control.

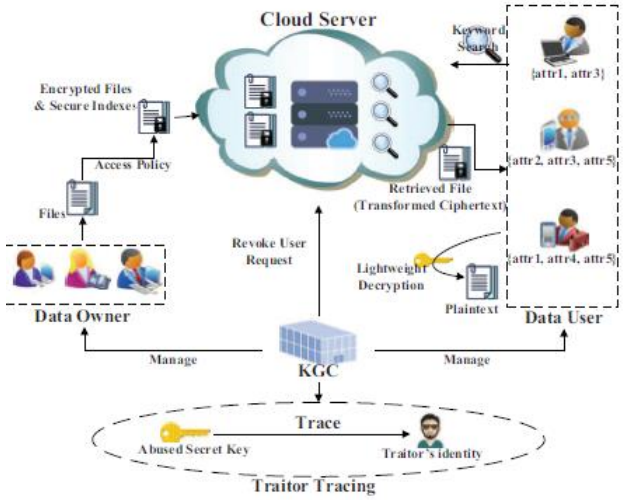

Fig. 1: System Model

(4) Data user. Each data user has attribute set to describe his characteristics, such as professor, computer science college, dean, etc. The attribute set was embedded into user's

SECURITY IN SHARED AND ENCRYPTED DATA

Now days, users are outsourcing their data based on cloud but while keeping their data on cloud it is very necessary to provide security to users data. For example, there is user Ashok who stores her data on cloud and shares it with her friends, with this he may have access to her friends data too. But personal data is always private in nature, so that user needs to selectively share their data with recipients. Similarly, what user can do is to set some access control policies and then remain on cloud server to enforce them. Unfortunately, this approach is not realistic because of two reasons. One is the users can't stop server from accessing their data. The other is that, even if the server is honest, it may also be forced to share user data with other parties [14].

KEYWORD GUESSING ATTACK

Nowadays searchable encrypted data to a third-party is of increasing interest in secure Cloud storage. In a typical application, a sender encrypts documents to a user who has a storage account in a cloud server or database. The data owner encrypted documents are uploaded to the storage server. The user can download some encrypted documents containing a specific keyword by providing the server with a keyword search trapdoor corresponding to that keyword. With this keyword search trapdoor, the storage server can find the matching documents or related documents without decryption. The cryptographic tool facilities search on encrypted data can be referred to as searchable encryption. In this searchable encryption comes in two types symmetric and asymmetric encryption. In a multiple user scenario, symmetric searchable encryption schemes can be used but they suffer from complicated secret key management. In which, each

sender needs to securely get a secret key from the intended user before the sender can encrypt documents. The attacker generates the cipher texts of all keywords. This is only suitable for the keyword space is in a polynomial size. The keyword as trapdoor, the attacker can launch a Keyword Guessing Attack (KGA) by testing the cipher texts of the keywords; and the keyword associated with the search trapdoor is discovered once a matching cipher text containing the keyword is found [13].

PUBLIC KEY ENCRYPTION WITH KEYWORD SEARCH

In this scheme the system allows the server to search for a keyword, given the trapdoor. Because of that the verifier can merely use an untrusted server [18]. It basically deals with the search problems between the user and untrusted server. Example of this is, there is a user Bob who sends a cipher text to Ashok with his public key. Ashok's public key, is an encrypted version of Bob's message under hiss public key and w is the keyword that Bob wants to attach to the email (such as „„urgent"").Alice can give the server with a certain trapdoor Tw (which is a trapdoor constructed by Alice on a keyword w) through a secure channel that enables the server to test whether the encrypted keyword associated with the message (CPEKS) is equal to the keyword w selected by Ashok [13].

Conclusion

The performance of access control and the support of keyword search are important issues in secure cloud storage system. In this work, we defined a new model of searchable encryption system, and proposed a concrete construction. It supports flexible multiple keywords subset can be searched, and solve the key problem during the key generation procedure. Malicious user who sells secret key for benefit is traced. The decryption operation is partially outsourced to cloud server and the correct of half-decrypted result is verified by data user. The performance analysis and simulation show its efficiency in computation and storage overhead. Experimental results show that the computation overhead at user's terminal is much reduced, which greatly saves the energy for resource-constrained devices of users. This proposed work considers store data in only cloud and if the users try to upload the virus files or any other unwanted files, it can be detected and block the particular user account. In future, they use some other techniques o improve the security.

REFERENCES

[1] R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, "Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage", IEEE Transactions on Information Forensics and Security, 2016, vol.11, no. 4, 789-798.

[2] X. Liu, R.H. Deng, K.K.R. Choo, J. Weng. "An efficient privacy preserving outsourced calculation toolkit with multiple keys", IEEE Transactions on Information Forensics and Security 11.11 (2016): 2401-2414.

[3] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in NDSS, 2004.

[4] Y. Yang, X. Liu, R.H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language". IEEE Transactions on Dependable and Secure Computing, 2018, publish online, DOI: 10.1109/TDSC.2017.2787588.
[5] K. Liang, W. Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 9, pp. 1981-1992.
[6] M. Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," in USENIX Security Symposium, ACM, 2011, pp. 34-34.

