ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

A Survey on Identity-Based Authenticated and Efficient Traceable Search System

Shital Khandare[1], Prof.H.A.Hingoliwala[2]

Student, Department of Computer Engineering, JSPM College, Hadapsar, Pune[1]

Associate Professor, Department of Computer Engineering, JSPM College, Hadapsar, Pune[2]

Abstract: Secure search over encrypted remote data is crucial in cloud computing to ensure the data privacy and usability. To prevent unauthorized data access and usage, fine-grained access control is important in multi-user system. Whereas, authorized user may intentionally leak the secret key for financial benefit. So, tracing and revoking such malicious user who abuses secret key needs to be solved. The key escrow free mechanism can be used which will effectively prevent the Key Generation Centre (KGC) from unscrupulously searching and decrypting all encrypted files of users. The decryption process involve here only requires ultra-lightweight computation, which is a desirable feature for energy-limited devices. If we figure out malicious user we can efficiently revoke that user. Again if we have, flexible multiple keywords subset search pattern, which will also not affect the order of search result.

Keywords: Authorized Searchable Encryption, Traceability, Multiple Keywords Subset Search

I. INTRODUCTION

Now a days, with the development of 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 cloud server. Despite the tremendous 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 basic method to protect data privacy in remote storage. However, how to effectively execute keyword search for plaintext becomes difficult for encrypted data due to the unreadability of ciphertext.

Searchable encryption mechanism enables keyword search over encrypted data. For the file sharing system, such as multi-owner multiuser scenario, fine-grained search authorization is a desirable function for the data owners to share their private data with other authorized user. However, 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 user's terminal, which is especially serious for energy constrained devices. The outsourced decryption method allows user to recover the message with ultra-lightweight decryption. However, the cloud server might return wrong half-decrypted information as a result of malicious attack or system malfunction. Thus, it is an important issue to guarantee the correctness of outsourced decryption in public key encryption with keyword search (PEKS) system. The authorized entities 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 his electronic medical data is sold on e-Bay. Such despicable behaviour seriously threatens 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 labour contracts. The intentional secret key leakage seriously undermines 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 attribute based access control system, the secret key of user is associated with a set of attributes rather than individual's identity. As the search and decryption authority 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 search authorization system is critical and not considered in previous searchable encryption systems.

II. RELATED WORK

In this paper, out of the blue we characterize 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 nearer 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].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

In a ciphertext-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 wording of ciphertext 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 ciphertext into a (short) El Gamal-type ciphertext utilizing an open change key given by a client with the goal that the last can be decoded considerably more effectively 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 basically 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 centred around 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 with 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 neighbourhood information administration and upkeep. Nonetheless, secure offer and pursuit for the re-appropriated information is a considerable assignment, which may effectively cause the spillage of touchy individual data. Effective information sharing and seeking with security is of basic significance [7].

This paper proposes a toolkit for efficient and privacy-preserving outsourced calculation 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 user’s (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 number of information, for the most part alluding to huge information, have 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 ciphertext are dependent upon attributes. As a result, a user can decrypt a ciphertext if and only if there is a match between the attributes which are listed in the ciphertext 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 advancement in the research this need is removed because Each user can join the system when he want and can leave the system independent of the other users. This reduces time which we require to change their secret keys and to reinitialize the system [20].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

IV. SECURITY IN SHARED AND ENCRYPTED DATA

Now days, users are outsourcing their data on cloud but while keeping data on cloud it is very necessary to provide security to users data. For example, there is user Alice who stores her data on cloud and shares it with her friends, with this she 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. Practically, 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 users' data with other parties [14].

V. KEYWORD GUESSING ATTACK

Outsourcing searchable encrypted data to a third party is of increasing interest in secure Cloud storage. In a typical application of this kind, a sender encrypts documents to a user who has a storage account in a cloud server. The encrypted documents are uploaded to the storage server. The receiver can retrieve 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 without decryption.

The cryptographic tool facilitating search on encrypted data is referred to as searchable encryption. In this searchable encryption comes in two types symmetric and asymmetric encryption. In a multiuser scenario, symmetric searchable encryption schemes can be used but they suffer from complicated secret key management. In which, each sender needs to securely obtain a secret key from the intended user before the sender can encrypt documents. The attacker generates the cipher texts of all keywords. This is suitable if the keyword space is in a polynomial size. Having a 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 ciphertext containing the keyword is found [13].

VI. 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 ciphertext to Alice with his public key. Alice'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 (for example ''urgent'').Alice can provide 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 Alice [13].

CONCLUSION AND FUTURE WORK

This dissertation proposed a novel method Identity-based Authenticated and Efficient Traceable Search System for Secure Cloud Storage. In this paper, a new Identity-Based Authenticated Data Sharing (IBADS) protocol is designed for cyber-physical cloud systems based on bilinear pairing. We then demonstrated the security and correctness of the protocol, as well as evaluating its performance. The enforcement of access control and the support of keyword search are important issues in secure cloud storage system. In this work, we defined a new paradigm of searchable encryption system, and proposed a concrete construction. It supports flexible multiple keywords subset search, and solves the key escrow problem during the key generation procedure. This proposed work considers store data in only single cloud. In future we can divide data into equal blocks & store into three different cloud using identity based of each user.

ACKNOWLEDGEMENT

I profoundly grateful to **Prof. H. A. Hingoliwala** for his expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. I would like to express my deepest appreciation towards Principal **Dr. M. G. Jadhav**, HOD **Dr. S. B. Chaudhari** department of computer engineering and PG Co-ordinator **Prof. M. D. Ingle**. I must express my sincere heartfelt gratitude to all staff members of computer engineering department who helped me directly or indirectly during this course of work. Finally, I would like to thank my family and friends, for their precious support.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

REFERENCES

[1]. C. Wang, N. Cao, J. Li, K. Ren, W. Lou. "Secure ranked keyword search over encrypted cloud data" IEEE 30th International Conference on Distributed Computing Systems (ICDCS), IEEE
[2]. Q. Zhang, L. T. Yang, Z. Chen, P. Li, M. J. Deen. "Privacy-preserving Double-Projection Deep Computation Model with Crowdsourcing on Cloud for Big Data Feature Learning," IEEE Internet of Things Journal, 2017.
[3]. 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.
[4]. 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)
[5]. 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
[6]. W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, "Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine grained Owner-enforced Search Authorization in the Cloud," IEEE Transactions on Parallel and Distributed Systems, 2016.
[7]. K. Liang, W. Susilo, "Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage," IEEE Transactions on Information Forensics and Security, 2015
[8]. 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
[9]. B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption," IEEE Transactions on Information Forensics and Security, 2015
[10]. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in: 2004
[11]. Z. Liu, Z. Cao, D.S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," IEEE Transactions on Information Forensics and Security,2013
[12]. J. Ning, X. Dong, Z. Cao, L. Wei, X. Lin, "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes," IEEE Transactions on Information Forensics and Security, 2015.
[13]. 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.
[14]. Q. Tang, "Nothing is for Free: Security in Searching Shared and Encrypted Data," IEEE Transactions on Information Forensics and Security, 2014.
[15]. Y. Yang and M. Ma, "Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds," IEEE Transactions on Information Forensics and Security, 2016.
[16]. B. Zhang, F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," Journal of Network and Computer Applications, 2011.
[17]. X. Wang, X. Huang, X. Yang, L. Liu, X. Wu, "Further observation on proxy re-encryption with keyword search," Journal of Systems and Software, 2012.
[18]. L. Fang, W. Susilo, C. Ge, J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Information Sciences, 2013.
[19]. A. Sahai, B.Waters, "Fuzzy identity-based encryption," in: EUROCRYPT, Springer, 2005.
[20]. J. Han, W. Susilo, Y. Mu. "Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption," IEEE Transactions on Information Forensics and Security, 2015.