A Review On Efficient Traceable Authorization Search System for Secure Cloud Storage

CHADALAVADA MANI #1, K.JOHN PAUL #2
1Student, Computer Science and Engineering, NOVA College of Engineering and Technology, Vegavaram(V), Jangareddigudem(M) West Godavari(D) Andhra Pradesh
2Guide, Associate Professor, Computer Science and Engineering NOVA College of Engineering and Technology, Vegavaram(V), Jangareddigudem(M) West Godavari(D) Andhra Pradesh

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

Cloud computing goal is to exploit large use of distributed resources by the customer to achieve high volume of throughput and to overcome large amount of computational problems. Cloud computing holds these entities: cloud server, cloud service provider, data owner, and data user. Cloud Server is the data center in which large collection of applications are hosted as services. Data center will be called as cloud. Cloud service provider deliver services or computing resources to the users from the cloud server over the internet through web browser interface. Cloud is maintained by the cloud service provider. Data owner is the owner of the document. Authorized Data user can access document from the cloud server. Cloud services are provided to the users for pay per use. Cloud service frameworks are Software as a service, Platform as a service, and Infrastructure as a service. Cloud computing models the user to access the document from anywhere wherever network connection available. Characteristics of cloud computing are on demand self-service, broad network access, resource grouping, rapid elasticity and assessed service [11]. Cloud services are available as public cloud, private cloud, community cloud, hybrid cloud [11]. Public cloud is offered over the internet to the general public in pay as you go manner. Private cloud is operated for specific organization. Community cloud is available only to groups. Hybrid cloud is the combination of public cloud and community cloud.

Cloud document will be shared among the dynamic group. Dynamic group refers the changes of membership over the group. Outsourcing the document to the third party group causes the security and privacy issue. Because the members in the group are considered as dynamic. In a group each group member can read and modify the data of the file which is shared by the company. The changes of membership make secure data sharing extremely difficult. Any member in the group can store the data and share the services by the cloud which will be called as multiple owner models. In a single owner model group manager can only store and modify the data in the cloud. Security issue is the main problem of the development and widespread use of cloud computing. Cloud service provider should be trustworthy by providing trust and secure computing and data storage [11]. In the untrusted server data owner depot the encrypted data files and disseminate the comparable decryption keys only to authorized people. So that, unauthorized people and file servers cannot able to learn the content of the document.

II.PRELIMINARIES

A. Triple DES algorithm

Triple DES algorithm takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks. Group members encrypt the data by using Triple DES algorithm so that only authorized user can decrypt the data. Triple DES algorithm allows the system administrator to dynamically include new members to the group and also conserves previously computed information. Triple DES is an excellent and reliable choice for the security needs of highly sensitive information while sharing the documents among the group members.

B. Secure Assertion Markup Language

SAML is the data format for exchanging the authentication and authorization data between user and cloud service provider. SAML description

involved among group people, system administrator and cloud service provider. Group people calls for service from the cloud service provider. Cloud service provider requests and obtains an identity assertion from the service provider. Service Provider requests information such as user name and password from the user to authenticate. Cloud service provider makes access control decision and decides whether to perform service for the connected user.

C.Single Sign-On

In a single sign on system user logs in once and gains access to all systems without being prompted to log in again at each of them. In single sign on user enter one name and password to access multiple applications. The process certifies the user for all the applications. Single sign on focuses more on protection of the user credentials. In a single sign on system single action of user authentication and authorization permit a user to access all resources. The single sign on maintains a mapping between a user or group of users and the username and password needed to access a particular data source.

III. RELATED WORK

In [2] Lu et al proposed a scheme based on bilinear pairing techniques for secure provenance. Secure provenance furnishes confidentiality on sensible documents which is stored in cloud, secret authentication on user access, and provenance tracking on disputed documents. Each user acquires two keys after the registration: a group signature and an attribute key. Group people can encrypt the document using attribute based encryption and also group can decrypt the encrypted document using their attribute keys. Group people sign on the encrypted data with group signature key for confidentiality of the data. User revocation is not supported in secure provenance.

In [9] Ateniese et al proposed atomic proxy re-encryption technique in which partly trusted proxy converts a ciphertext without seeing the underlying plaintext. Unique and symmetric content keys used to encrypt the document which is again encrypted with master public key. Proxy re-encryption allows the centrally managed access control.

In [1] Kallahlla et al proposed a cryptographic storage system to reduce the numbers of cryptographic keys exchanged between users and achieves strong security. Filegroups divided as files and encrypted with distinctive fileblock key, data owner deliver the filegroups to group people with lockbox key. Fileblock keys encrypted with lockbox key. Accumulating keys into filegroups has the discernible advantage that it reduces the number of keys that users need to manage, distribute and receive. System brings heavy key distribution overhead for secure file sharing. System updates file block key and distribute for user revocation.

In [3] Wang et al proposed a System in that for constructing homomorphic authentication group signature is used. By doing this without retrieving the whole data third party auditor can verify the integrity of the data. The identity of the signer on each block in apportioned data is held private from the third party auditor. System supports expeditiously audit the correctness of the document, apportioned among large number of people. System feats homomorphic MACs to shorten the space utilized to depot such verification information.

To contribute the document with dynamic group, need to propose system with certain unique features: In a cloud any people in the group can store and contribute the document with group people. The complexity of encryption and ciphertext size are independent with the number of revoked users in the scheme.

IV.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].

V.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].

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].

VII.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.

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.

Author's Profile

Chadalavada Mani Studying M.Tech (2nd year Pursuing) Computer Science and Engineering.

K.JOHN PAUL Working as Associate Professor
Qualification:M.Tech