AN EFFICIENT MULTIPLE KEYWORD SEARCHABLE SYSTEM FOR SECURITY IN CLOUD STORAGE ENVIRONMENT

Mr. Y. Venkata Vinod Kumar [1]
3rd Year Student,
Department of Computer Science,
SV U CM & CS, Tirupati.

Dr. E. Kesavulu Reddy[2],
Assistant Professor,
Department of Computer Science,
SV U CM & CS,, Tirupati.

Abstract: The Secure search over encrypted remote data is crucial in cloud computing to guarantee the data privacy and usability. To prevent unauthorized data usage, fine-grained access control is necessary in multi-user system. However, authorized user may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the malicious user who abuses secret key needs to be solved imminently. In this paper, we propose an **e**scrow **f**ree **t**raceable **a**ttribute based **m**ultiple **k**eywords **s**ubset **s**earch system with **v**erifiable **o**utsourced **d**ecryption (EF-TAMKS-VOD). The key escrow free mechanism could effectively prevent the key generation centre (KGC) from unscrupulously searching and decrypting all encrypted files of users. Also, the decryption process only requires ultra lightweight computation, which is a desirable feature for energy-limited devices. In addition, efficient user revocation is enabled after the malicious user is figured out. Moreover, the proposed system is able to support flexible number of attributes rather than polynomial bounded. Flexible multiple keyword subset search pattern is realized, and the change of the query keywords order does not affect the search result. Security analysis indicates that EF-TAMKS-VOD is provably secure. Efficiency analysis and experimental results show that EF-TAMKS-VOD improves the efficiency and greatly reduces the computation overhead of users' terminals.

Index Terms*—authorized searchable encryption, traceability, verifiable outsourced decryption, key escrow free, and multiple keywords subset search.*

I INTRODUCTION

Cloud storage services enable users to outsource their data to cloud servers and access the outsourced data remotely whenever they have Internet connections. Such services provide users an efficient and flexible way to manage their data without deploying and maintaining the local storage device and service [1], [2], [3], [4]. Specifically, one can process her data on PC, outsource the processed data to cloud servers, and use the data on other devices (e.g. mobile phone) anywhere. Users enjoy great convenience from such services, and it leads to the growing number of cloud storage providers [5], [6].

Despite the benefits brought by the cloud storage service, critical security concerns in data outsourcing have been raised seriously. One of the most important security concerns is data integrity. Because users do not physically own their data once outsourcing the data to cloud servers, they are always worried about the data integrity, i.e. whether their data remains intact on the cloud servers [7]. Concretely, a cloud service provider may hide data loss incidents in order to maintain his reputation [8].

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 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.

Disadvantages:

Inflexible authorized keyword search

Inflexible system extension

Inefficient decryption

II EXISTING SYSTEM

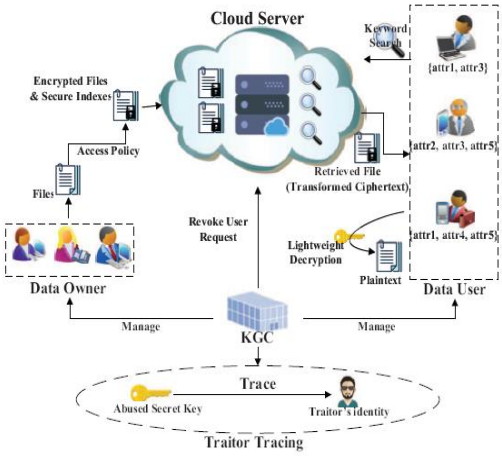
Notwithstanding of being free from mystery key dispersion, PEKS plans to expertise the unwell effects of

Associate in Nursing essential weakness concerning the trapdoor shibboleth protection, to be fixed within Watchword approximation Assault (KGA). The rationale prompting such security impotence is that somebody UN agency kens beneficiary's open key will induce the PEKS ciphertext of self-assertive watchword himself. Completely, given a trapdoor, the antagonistic server will winnow an approximation watchword from the shibboleth house and subsequently use the watchword to cause a PEKS ciphertext. The server at that time will take a look at whether or not the approximation watchword is that the one basic the trapdoor. This approximation then-testing methodology is often emphasized till the purpose that the proper watchword is found. Such an approximation assault has nonetheless been thought of in varied watchword predicated frameworks. In any case, the offenders often propelled all the additional effectively against PEKS plans since the watchword house is usually equipollent to a standard lexicon (e.g., all the important English words), that incorporates a considerably additional minute size than a secret keyword reference (e.g., each one of the words containing half dozen alphanumerical characters). It's important that in SSE plans, simply mystery key holders will induce the shibboleth ciphertext and henceforward the antagonistic server isn't able to dispatch at intervals KGA. Because the shibboleth reliably betokens the protection of the user data, it does therefore of practical significance to surmount this security risk for secure, accessible disorganized data outsourcing.

Traditional PEKS. Following Boneh et al.'s seminal work[5], Abdalla et al. [8] formalized anonymous IBE (AIBE) andpresented a generic construction of searchable encryptionfrom AIBE. They also showed how to transfer a hierarchicalIBE (HIBE) scheme into a public key encryption with temporarykeyword search (PETKS) where the trapdoor is onlyvalid in a specific time interval. Waters [7] showed that thePEKS schemes based on bilinear map could be applied tobuild encrypted and searchable auditing logs. In order toconstruct a PEKS secure in the standard model, Khader [9]proposed a scheme based on the k-resilient IBE and alsogave a construction supporting multiple-keyword search.The first PEKS scheme without pairings was introduced byDi Crescenzo and Saraswat [11]. The construction is derivedfrom Cock's IBE scheme [12] which is not very practical.Secure Channel Free PEKS. The original PEKS scheme[5] requires a secure channel to transmit the trapdoors. Toovercome this limitation, Baek et al. [13] proposed a newPEKS scheme without requiring a secure channel, whichis referred to as a secure channel-free PEKS (SCF-PEKS).The idea is to add the server's public/private key pair intoa PEKS system. The keyword ciphertext and trapdoor aregenerated using the server's public key and hence only theserver (designated tester) is able to perform the search. Rheeet al. [14] later enhanced Baek et al.'s security model [13]for SCF-PEKS where the attacker is allowed to obtain therelationship between the non-challenge ciphertexts and thetrapdoor. They also presented an SCF-PEKS scheme secureunder the enhanced security model in the random oraclemodel. Another extension on SCF-PEKS is by Emura et al.[15]. They enhanced the security model by introducing theadaptively secure SCF-PEKS, wherein an adversary is allowedto issue test queries adaptively.Against Outside KGA.Byun et al. [16] introduced the offlinekeyword guessing attack against PEKS as keywordsare chosen from a much smaller space than passwordsand users usually use well-known keywords for searchingdocuments. They also pointed out that the scheme proposedin Boneh et al. [5] was susceptible to keyword guessingattack. Inspired by the work of Byun et al. [16], Yau et al.[17] demonstrated that outside adversaries that capture thetrapdoors sent in a public channel can reveal the encryptedkeywords through off-line keyword guessing attacks andthey also showed off-line keyword guessing attacks againstthe (SCF-)PEKS schemes in [13], [18]. The first PEKS schemesecure against outside keyword guessing attacks was proposedby Rhee et al. [19]. In [20], the notion of trapdoorin distinguishability was proposed and the authors showedthat trapdoor in distinguishability is a sufficient conditionfor preventing outside keyword-guessing attacks. Fang et al.[21] proposed a concrete SCF-PEKS scheme with (outside)KGA resilience. Similar to the work in [15], they also consideredthe adaptive test oracle in their proposed securitydefinition.

III PROPOSED SYSTEM

A novel primitive: **e**scrow **f**ree **t**raceable **a**ttribute based **m**ultiple **k**eywords **s**ubset **s**earch system with **v**erifiable **o**utsourced **d**ecryption (EF-TAMKSVOD), which has the following contributions. In order to provide an easier way to understand EF-TAMKSVOD, we design a **t**raceable **a**ttribute based **m**ultiple **k**eywords **s**ubset **s**earch system with **v**erifiable **o**utsourced **d**ecryption (TAMKS-VOD), where KGC is responsible to generate user's public/secret key pair like in traditional PEKS schemes. The key escrow problem is resolved using an interactive operation between KGC and cloud server.



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

Data owner. Data owner utilizes the cloud storage service to store the files. Before the data outsourcing, the data owner extracts 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 is specified and embedded into the cipher text to realize fine grained access control.

Data user. Each data user has attribute set to describe his characteristics, such as professor, computer Science College, dean, etc. The attribute set is embedded into user's secret key. Using the secret key, data user is able to search on the encrypted files stored in the cloud, i.e., chooses a keyword set that he wants to search. Then, the keyword is encrypted to a trapdoor using user's secret key. If the user's attribute set satisfies the access policy defined in the encrypted files, the cloud server responds on user's search query and finds the match files. Otherwise, the search query is rejected. After the match files are returned, the user runs decryption algorithm to recover the plaintext.

Traitor Tracing

The security requirement of traceability 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.

Key generation centre (KGC). :

KGC is responsible to generate 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, KGC 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.

IV ADVANTAGES

Flexible Authorized Keyword Search

Flexible System Extension.

Efficient Verifiable Decryption.

White-box Traceability of Abused Secret Key

Efficient User Revocation.

Key Escrow Free

V CONCLUSION

The enforcement of access control and the support of keyword search are important issues in secure cloud storage system. In this, 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. Malicious user who sells secret key for benefit can be traced. The decryption operation is partly outsourced to cloud server and the correctness of half-decrypted result can be verified by data user.

VI REFERENCES

[1] Shui Yu, YonghongTian, Song Guo, and Dapeng Oliver Wu. "Can We Beat DDos Attacks in Clouds?" IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2245-2254, September, 2014.

[2] Shui Yu, Guojun Wang, and Wanlei Zhou."Modeling Malicious Activites in Cyber Space." IEEE Network, vol. 29, no. 6, pp. 83-87, November/December, 2015.

[3] Shui Yu, Song Guo, and Ivan Stojmenovic. "Fool Me If You Can: Mimicking Attacks and Anti-Attacks in Cyberspace." IEEE Transactions on Computers, vol.64, no. 1, pp. 139-151, January, 2015.

[4] Cong Wang, Sherman S.M. Chow, Qian Wang, KuiRen, and Wenjing Lou."Privacy-Preserving Public Auditing for Secure Cloud Storage." IEEE Transactions on Computers, vol. 62, no. 2, pp. 362-375, February, 2013.

[5] Hongwei Li, Yi Yang, Tom H. Luan, Xiaohui Liang, Liang Zhou, and XuemingShen. "Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data." IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 3, pp. 312-325, May/June, 2016.

[6] Hongwei Li, Dongxiao Liu, Yuanshun Dai, and Tom H. Luan. "Engineering Searchable Encryption of Mobile Cloud Networks: When QoE Meets QoP." IEEE Wireless Communications, vol. 22, no. 4, pp. 74-80, August, 2015.

[7] Cong Wang, Qian Wang, KuiRen, and Wenjing Lou. "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing." Proceedings of the 2010 IEEE International Conference on Computer Communications (INFOCOM 2010), IEEE, 2010, pp. 1-9.

[8] ChunxiangXu, Yuan Zhang, Yong Yu, Xiaojun Zhang, and Junwei Wen."An Efficient Provable Secure Public Auditing Scheme for Cloud Storage." KSII Transactions on Internet and Information Systems, vol. 8, no. 11, November, 2014.

[9] Yuan Zhang, ChunxiangXu, Jining Zhao, Xiaojun Zhang, and Junwei Wen. "Cryptanalysis of an Integrity Checking Scheme for Cloud Data Sharing." Journal of Information Security and Applications, vol. 23, pp. 68-73, August, 2015.

[10] Yuan Zhang, ChunxiangXu, Shui Yu, Hongwei Li, and Xiaojun Zhang. "SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors." IEEE Transactions on Computational Social Systems, vol. 2, no. 4, pp. 159-170, December, 2015.

[11] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, and Dawn Song."Provable Data Possession at Untrusted Stores." Proceedings of the 2007 ACM SIGSAC Conference on Computer and Communications Security (CCS 2007), ACM, 2007, pp. 598-609.

[12] Solomon GuadieWorku, ChunxiangXu, Jining Zhao, and Xiaohu He."Secure and Efficient Privacy-Preserving Public Auditing Scheme for Cloud Storage."Computers and Electrical Engineering, vol. 40, no. 5, pp.1703-1713, July, 2014.

[13] HovavShacham and Brent Waters."Compact Proofs of Retrievability." Journal of Cryptology, 26.3 (2013): 442-483.

[14] FrederikArmknecht, Jens-Matthias Bohli, Ghassan O. Karame, Zongren Liu, and Christian A. Reuter. "Outsourced Proofs of Retrievability."Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS 2014). ACM, 2014, pp. 831-843.

[15] Dan Boneh, Ben Lynn, and HovavShacham."Short Signatures from the Weil Pairing."Advances in Cryptology -- ASIACRYPT 2001. Springer Berlin Heidelberg, 2001, pp. 514-532.