A DYNAMIC PATH ENDORESEMENT IN SECURE CLOUD SEARCH SYSTEM

CHILAKALA RAMANI
M.Tech Scholar, Dept of CSE, Indira Institute of Technology & Sciences, Markapur, Prakasam Dist, AP, India
charmani123@gmail.com

K.V.H.N.VISHNUVARDHAN
Assistant Professor, Dept of CSE , Indira Institute of Technology & Sciences, Markapur, Prakasam Dist, AP, India
vishnu960@gmail.com

Abstract

To counteract unapproved information use, fine-grained access control is vital in multi-client framework. Nonetheless, approved client may deliberately release the mystery key for budgetary advantage. In this manner, following and renouncing the noxious client who misuses mystery key should be explained quickly. In this paper, we propose an escrow free way trait based various catchphrases subset search framework with obvious redistributed unscrambling. The key escrow free component could successfully avert the key age focus (KGC) from deceitfully looking and unscrambling all scrambled documents of clients. Additionally, the decoding procedure just requires ultra lightweight calculation, which is an attractive component for vitality constrained gadgets. What's more, productive client repudiation is empowered after the malignant client is made sense of. Additionally, the proposed framework can bolster adaptable number of characteristics as opposed to polynomial limited. Adaptable various watchword subset search example is acknowledged, and the difference in the question catchphrases request does not influence the query output. Security investigation demonstrates that EF-TAMKS-VOD is provably secure. Dynamic investigation and trial results demonstrate that EF-TAMKS-VOD improves the Dynamic and extraordinarily diminishes the calculation overhead of clients' terminals.

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

1 INTRODUCTION

ITH the advancement of new figuring worldview, distributed computing [1] turns into the most striking one, which gives advantageous, on-request benefits from a mutual pool of configurable processing assets. Hence, an expanding number of organizations and people want to re-appropriate their information stockpiling to cloud server. Regardless of the gigantic monetary and specialized focal points, un-unsurprising security and protection concerns [2], [3] become the most unmistakable issue that frustrates the across the board reception of information stockpiling in open cloud framework. Encryption is an essential strategy to secure information protection in remote stockpiling [4]. In any case, how to viably execute watchword scan for plaintext winds up hard for encoded information because of the ambiguity of ciphertext. Accessible encryption gives instrument to empower watchword search over scrambled information [5], [6]. For the record sharing framework, for example, multi-proprietor multi-client situation, fine-grained search Endoresement is a desir-capable capacity for the information proprietors to impart their private information to other approved client. In any case, the greater part of the accessible frameworks [7], [8] require the client to play out a lot of complex bilinear blending activities. These over-whelmed calculations become a substantial weight for client's terminal, which is particularly genuine for vitality compelled gadgets. The redistributed decoding strategy [9] enables client to recoup the message with ultra lightweight unscrambling [10], [11]. Notwithstanding, the cloud server may return wrong half-unscrambled data because of pernicious assault or framework breakdown. Therefore, it is a significant issue to ensure the rightness of redistributed unscrambling in open key encryption with catchphrase search (PEKS) framework [12].

The approved substances may illicitly release their mystery key to an outsider for benefits [13]. Assume that a patient some time or another all of a sudden discovers that a mystery key relating his electronic restorative information is sold on e-Bay. Such disgusting conduct genuinely undermines the patient's information security. Surprisingly more terrible, if the private electronic wellbeing information that contain se-rious wellbeing ailment is mishandled by the insurance agency or the patient's work company, the patient would be declined to recharge the restorative protection or work contracts. The deliberate mystery key spillage truly undermines the establishment of approved access control and information security assurance. In this way, it is very pressing to distinguish the vindictive client or even demonstrate it in a courtroom. In trait based access control framework, the mystery key of client is related with a lot of properties instead of person's character. As the inquiry and decoding specialist can be shared by a lot of clients who possess a similar arrangement of properties, it is difficult to follow the first key proprietor [14], [15]. Providing recognizability [37] to a fine-grained search Endoresement framework is basic and not considered in past accessible encryption frameworks [7], [8], [12].

All the more significantly, in the first meaning of PEKS plot [12], key age focus (KGC) creates all the mystery enters in the framework, which definitely prompts the key escrow issue. That is, the KGC realizes all the mystery keys of the clients and in this way can deceitfully look and unscramble on all scrambled documents, which is a critical risk to information security and protection. Close to, the key escrow issue brings another issue when detectability capacity is acknowledged in PEKS. On the off chance that a mystery key is observed to be sold and the character of mystery key's proprietor (i.e., the backstabber) is recognized, the deceiver may guarantee that the mystery key is spilled by KGC. There is no specialized strategy to recognize who is the genuine trickster if the key escrow issue isn't understood.

Related Work

Searchable Encryption

Searchable encryption enables keyword search over encrypted data. The concept of public key encryption with keyword search (PEKS) was proposed by Boneh et al [12], which is important in protecting the privacy of outsourced data. Data owners in PEKS schemes [7], [8], [16] store their files in encrypted form in the remote untrusted data server. The data users query to search on the encrypted files by generating a keyword trapdoor, and the data server executes the search operation. Waters et al. [5] showed that PEKS schemes could be utilized to construct searchable audit logs. Later, Xu et al. [17] presented a general framework to combine PEKS and fuzzy keyword search without concrete construction. Tang [18] proposed a multiparty searchable encryption scheme together with a bilinear pairing based scheme. In 2016, Chen et al. [3] introduced the concept "dual-server" into PEKS to resist off-line keyword guessing attack. Yang et al. [19] introduced time-release and proxy re- encryption method to PEKS scheme in order to realize time- controlled authority delegation. Wang et al. [1] proposed a ranked keyword search scheme for searchable symmetric encryption, in which the order-preserving symmetric encryption is utilized [35]. Cao et al. [36] designed a novel system to realize multiple keyword ranked search. Searchable encryption is also further studied in [20], [21], [22]. able to decrypt any patients' encrypted medical files with access policies that satisfied by the attribute set doctor, keyword set must be exactly the same as the extracted keyword set from the file. If one of the query keyword is not included in (or different from) the extracted keyword set, the file is not returned. They are far more from satisfying users' realistic requirements.

(1) ***Inflexible SYSTEM extension***: Many existing autho- rization schemes [7], [8], [10], [11], [13], [24], [26], [27] are inflexible for the system extension. The attribute set needs to be predefined during the system establishment phase, and a maximum number of the attribute set should be determined. If a new attribute is to be added to the system, the entire system has to be re-constructed and all encrypted files have to be re-encrypted. It would be a disaster to the cloud storage system.

(2) ***Inefficient decryption***: A main drawback of many ABE based fine-grained access control schemes [7], [8], [13], [14], [24], [27] is that the computation cost required for decryption grows linearly with the complexity of access structure. With the rapid development of mobile terminals (such as mobile phones), the expensive decryption compu- tation will exhaust the battery in a short time. It is a critical obstacle for the deployment in resource constrained devices [33], [34].

(3) ***Abuse of attribute secret key***: In ABE system, the attribute secret keys are not associated with individuals, but with the attributes shared by multiple users, which is the principle for the ABE to implement the one-to-many data encryption and sharing. The data owner only needs to specify the data user's attributes and enforce an access policy over the attributes, rather than exactly define the identities of the data users. The attribute secret keys do not associate with user's identities, which makes the traitor tracing in ABE a hard problem. Given an abused attribute secret key, it is difficult to find the clue for discovering the key owner's identity of the available searchable encryption schemes.

(4) Key escrow prOBLEM: In traditional searchable encryp- tion [21], [22] and ABE schemes [9], [10], [11], [13], [14], [24], [26], [27], the users' secret keys are all generated by the key generation centre (KGC). Thus, all the secret keys are escrowed to KGC, and the secret key of data user is known to both KGC and the user, which is named as "key escrow". In the traitor tracing process, the identified traitor may argue that the secret key is leaked by the KGC rather than himself. In order to eliminate the dispute, the "key escrow" problem must be solved.

Our Contributions

In this paper, we propose a novel primitive: **e**scrow **f**ree **path a**ttribute based **m**ultiple **k**eywords **s**ubset **s**earch system with **v**erifiable **o**utsourced **d**ecryption (EF-TAMKS- VOD), which has the following contributions.

(4) ***Flexible Authorized Keyword Search***. EF-TAMKS- VOD achieves fine-grained data access Endoresement and supports multiple keyword subset search. In the encryption phase, a keyword set KW is extracted from the file, and both of KW and the file are encrypted. An access policy is also enforced to define the authorized types of users. In the search phase, the data user specifies a keyword set KW^J and generates a trapdoor $T_{KW} t$ using his secret key. In the test phase, if the attributes linked with user's secret key satisfy the file's access policy and KW^J (embedded in the trapdoor) is a subset of KW (embedded in the ciphertext), the corresponding file is deemed as a match file and returned to the data user. The order of keywords in KW^J can be arbitrarily changed, which does not affect the search result.

(1) Different random numbers are selected in the attribute secret key generation algorithm. ***Flexible SYSTEM***

Extension. EF-TAMKS-VOD supports flexible system extension, which accommodates flexi- ble number of attributes. The attributes are not fixed in the system initialization phase and the size of attribute set is not restricted to polynomially bound, so that new attribute can be added to the system at any time. Moreover, the size of public parameter does not grow with the number of attributes. No matter how many attributes are supported in the system, no additional communication nor storage costs is brought to EF-TAMKS-VOD. This feature is desirable for the cloud system for its ever increasing user volume.

(2) ***Efficient Verifiable Decryption***. EF-TAMKS-VOD adopts the outsouced decryption mechanism to realize efficient decryption. Most of the decryption computation are outsourced to the cloud server, and the data user is able to complete the final decryption with an ultra lightweight computation. Moreover, the correctness of the cloud server's partial decryption computation can be verified by the user.

(3) ***White-box Traceability of Abused Secret Key***. Traitor tracing can be divided into white-box and black-box trace- ability. If an authorized user leaks or sells his secret key, white-box traceability is capable to identify who leaks the key. Black-box traceability is a stronger conception, in which the leakage of a malicious user is the search and decryp- tion equipment instead of the secret key. EF-TAMKS-VOD achieves white-box traceability. Any subscriber who leaks the secret key to a third party intentionally or unintentionally can be traced. Furthermore, the traceability of EF- TAMKS-VOD does not bring additional computation and transmission overhead.

(4) ***Efficient User Revocation***. Once a user is identified as traitor through tracing algorithm, EF-TAMKS-VOD revokes this malicious user from the authorized group. Compared with the existing scheme [7], the revocation mechanism of EF-TAMKS-VOD has much better Dynamic.

(5) ***Key Escrow Free***. In order to reduce the trust on KGC, an interactive key generation protocol is designed to solve the key escrow problem. EF-TAMKS-VOD adopts an interaction process between KGC and cloud server such that none of them is capable to independently generate the whole secret key of the user, where a lightweight homomor- phic encryption algorithm is utilized. Thus, the user's secret key is not escrowed to any entity and EF-TAMKS-VOD is key escrow free.

2 TAMKS-VOD

In order to provide an easier way to understand EF-TAMKS- VOD, we design a **path** **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. In section 4, the key escrow problem is resolved using an interactive operation between KGC and cloud server.

System Model

The system model of TAMKS-VOD is presented in Fig. 1, and the formal definition is provided in Section A in the Supplemental Materials. The system comprises of four en- tities, whose responsibilities and interactions are described below.

(1) ***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 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.

Security Requirement

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

- *The ciphertext and keyword are indistinguishable*. If the TAMKS-VOD system possesses the property of indistin- guishability, then the attacker is not capable to distinguish pairs of ciphertexts based on pairs of plaintext files. Simi- larly, 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 plaintext attack (IND-CKCPA). The security model of IND-CKCPA is defined in Section B.1 in the Supplemental Materials, where the explanation of the security model is provided.
- *Traceability*. 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. The security model of traceability is defined in Section B.2 in the Supplemental Materials, where the explanation of the security model is provided.

System Workflow

TAMKS-VOD has eight algorithms *Setup*, *Keytten*, *CreteUL*, *Enc*, *Trapdoor*, *Test&Transform*, *Dec*, *KeySanityCheck&Trace*, and the system workflow is shown in Fig. 2.

(1) In of the system establishment phase, KGC runs *Setup* algorithm (illustrated in Fig. 3) to generate the public parameter *PP* and master secret key *MSK* of the system. The master secret key *MSK* is kept secret by KGC. The system public parameter *PP* is disseminated to cloud server, data owners and users.

(2) For a system user (including data owner and data user) with attribute set S and identity *id*, KGC runs *Keytten* algorithm (illustrated in Fig. 3) to generate an attribute public key $PK_{id,S}$ and secret key $SK_{id,S}$, in which the users' identity *id* and attribute set S are implicitly embedded. Th{e attribute set S describes the} characteristic of the user's identity *id*. For example, a doctor Alice of oncology department in Raffles hospital has the attribute set S_a = doctor, oncology department, Raffles hospital , and gets the attribute public/secret key pair $PK_{id,S}/SK_{id,S}$, where identity *id* =“Alice” and attribute set $S = S_A$.

(3) A data user list *UL* is stored by the cloud server.

The data owner runs *CreateUL* algorithm (illustrated in Fig. 4) to generate a pseudonym ζ_{id} and a parameter $\tilde{D}id$ for each authorized user with identity *id*. The tuple

$(\zeta_{id}, \tilde{D}id)$ is inserted into *UL*, which is used in the following *Test&Transform* algorithm and user revocation phase.

(4) The data owner runs *Enc* algorithm (illustrated in Fig. 5) to encrypt the file M and the extracted keyword set KW . In this process, an access policy (A, ρ) is specified to define the set of authorized users, which is embedded into the ciphertext. Meanwhile, a verification key $V K_M$ is generated in the *Enc* algorithm, which is used to verify the cor- rectness of the transformed ciphertext CT_{out} that is generated by the cloud server in the following *Test&Transform* algorithm. The encrypted files, secure keyword set indexes and verification key are outsourced to cloud server.

(5) In the query phase, data user specifies a query key- word set KW^{J} and runs *Trapdoor* algorithm (illustrated in Fig. 6) to generate a trapdoor T_{KW} t using his attribute secret key $SK_{id,S}$. Data user's attribute set S is implicitly embedded into the trapdoor. Then, the data user submits T_{KW} t to the cloud server.

(6) Receiving the search query from the data user, the cloud server runs *Test*&*Transform* algorithm (illustrated in Fig. 7) to search on the data owner's encrypted files. The *Test*&*Transform* algorithm is divided into two algorithms, i.e., *Test* algorithm and *Transform* algorithm.

In the *Test* algorithm, CS tests whether the query key- word set KW^{J} (implicitly embedded in $T_{KW} t$) is a subset of KW (implicitly embedded in CT) and whether the attribute set S (implicitly embedded in $T_{KW}\ t$) satisfies the access policy (A, ρ) (implicitly embedded in CT). If one of the two conditions does not satisfy, the *Test* algorithm outputs "0" and the *Trasform* algorithm outputs a symbol indicating that they do not match. If both of the two conditions satisfy, the *Test* algorithm outputs "1" indicating that the ciphertext CT matches with the trapdoor $T_{KW}t$.

Then, the *Trasform* algorithm outputs a transformed ci- phertext CT_{out}, so that the data user can recover the plain- text M using a lightweight calculation in the following *Dec* algorithm. The transformed ciphertext CT_{out} and the corresponding verification key $V\,K_M$ are returned to the data user.

(7) In *Dec* algorithm (illustrated in Fig. 8), the data user verifies whether the transformed ciphertext CT_{out} is correct using the verification key VK_M.

If invalid, a symbol ⊥ is returned to cloud server. Otherwise, the data user executes lightweight computation to recover the message M .

(8) If a secret key is sold for beneficial gain, *KeySanityCheck*&*Trace* algorithm (illustrated in Fig. 9) is run by KGC to check the validity of the key. If $^{\perp}$the secret key is not well-formed, *KeySanityCheck* algorithm outputs 0, and *Trace* algorithm outputs a symbol . Oth- erwise, *KeySanityCheck* algorithm outputs 1, and *Trace* algorithm recovers the real identity of the sold secret key's owner.

(9) After the traitor is traced, KGC sends a revocation request to CS to revoke the user (illustrated in Fig. 10).

New User Registration

When a user applies to join the TAMKS-VOD system, KGC assigns an attribute set S to the user according to his iden- tity. Then, KGC runs key generation algorithm to generate the public/secret keys for user.

1 Compute the verification key $V\,K_M = H(\mathrm{Y}\ C_M\ )$. This verification key is used to test whether the outsourced computing result is correct or not.

3 CONCLUSION

The enforcement of access control and the support of key- word search are important issues in secure cloud stor- age 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. 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. The performance analysis and simulation show its Dynamic in computation and storage overhead. Experimental results indicate that the computation overhead at user's terminal is significantly reduced, which greatly saves the energy for resource-constrained devices of users.

ACKNOWLEDGMENTS

The authors thank the editor-in-chief, associate editor and reviewers for their constructive and generous feedback. We are thankful for the valuable discussions with Prof. Baodong Qin (Xi'an University of Posts and Telecommunications) to improve this work. This work is supported by National Nat- ural Science Foundation of China (No. 61402112, 61702105, 61672159); Technology Innovation Platform Project of Fujian Province (No.

2014H2005); Fujian Major Project of Regional Industry (No. 2014H4015); Major Science and Technology Project of Fujian Province (No. 2015H6013); Fujian Provin- cial Key Laboratory of Information Processing and Intel- ligent Control (Minjiang University) (No. MJUKF201734); Fujian Collaborative Innovation Center for Big Data Application in Governments; Fujian Engineering Research Center of Big Data Analysis and Processing.

REFERENCES

[1] C. Wang, N. Cao, J. Li, K. Ren, W. Lou. "Secure ranked keyword search over encrypted cloud data"[C]//IEEE 30th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2010: 253-262.

[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, DOI: 10.1109/JIOT.2017.2732735.

[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, vol. 11, no. 4, 789-798.

[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): 2401-2414.

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

[6] Y. Yang, X. Liu, R.H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language". IEEE Transac- tions on Dependable and Secure Computing, 2018, publish online, DOI: 10.1109/TDSC.2017.2787588.

[7] 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 Endoresement in the Cloud," IEEE Transactions on Parallel and Distributed Systems, 2016, vol. 27, no. 4, pp. 1187-1198.

[8] 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.

[9] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryp- tion of ABE ciphertexts," in USENIX Security Symposium, ACM, 2011, pp. 34-34.

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

[11] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption," IEEE Transac- tions on Information Forensics and Security, 2015, vol. 10, no. 7, pp. 1384-1394.

[12] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in: EUROCRYPT, 2004, pp. 506-522.

[13] Z. Liu, Z. Cao, D.S. Wong, "White-box path ciphertext-policy attribute-based encryption supporting any monotone access struc- tures," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 1, pp. 76-88.

[14] J. Ning, X. Dong, Z. Cao, L. Wei, X. Lin, "White-Box Path Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 6, pp. 1274-1288.

[15] Z. Liu, Z. Cao, D.S. Wong, "Path CP-ABE: how to trace decryption devices found in the wild," IEEE Transactions on In- formation Forensics and Security, 2015, vol. 10, no. 1, pp. 55-68.

[16] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in: 4th Theory Cryptogrophy Confonference, 2007, vol. 4392, pp. 535-554.

[17] 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.

[18] Q. Tang, "Nothing is for Free: Security in Searching Shared and Encrypted Data," IEEE Transactions on Information Forensics and Security, 2014, vol. 9, no. 11, 1943-1952.

[19] Y. Yang and M. Ma, "Conjunctive Keyword Search With Desig- nated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds," IEEE Transactions on Information Forensics and Security, 2016, vol. 11, no. 4, 746-759.

[20] B. Zhang, F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," Journal of Network and Computer Applications, 2011, vol. 34, no. 1, pp. 262-267.