Volume 4 || Special Issue 12 || ICCEME 2019-2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

AUTHORIZATION SEARCH SYSTEM FOR SECURE CLOUD STORAGE WITH TRACING MALICIOUS USER

Sanjeev Narayan[1] , Santosh Subramanian[2] , Twinkal Sakhare[3] , Diksha Motinagare [4]
Mrs. Rohini Patil[5]

SKN SINHGAD INSTITUE OF TECHNOLOGY AND SCIENCE, LONAVALA[1,2,3,4,5]

Abstract- Secure search over encrypted remote knowledge is crucial in cloud computing to ensure the info privacy and usefulness. to stop unauthorized knowledge usage, fine-grained access management is important in a multi-user system. However, the approved users could by choice leak the key for monetary profit. Thus, tracing and revoking the malicious user WHO abuses secret key must be resolved imminently. During this paper, we have a tendency to propose associate degree written agreement free traceable attribute primarily based multiple keywords set search system with verifiable outsourced secret writing (EF-TAMKS-VOD). The key written agreement free mechanism may effectively forestall the key generation center (KGC) from unscrupulously looking out and decrypting all encrypted files of users. Also, the secret writing method solely needs radical light-weight computation, which could be a fascinating feature for energy-limited devices. Additionally, economical user revocation is enabled when the malicious user is puzzled out. Moreover, the projected system is in a position to support versatile range of attributes instead of polynomial finite. Versatile multiple keywords set search pattern is realized, and also the modification of the question keywords order doesn't have an effect on the search result. Security analysis indicates that EF-TAMKS-VOD is incontrovertibly secure. Potency analysis and experimental results show that EF-TAMKS-VOD improves the potency and greatly reduces the computation overhead of users' terminals.

Keyword: *Authorized searchable encryption, traceability, verifiable outsourced decryption, key escrow free, and multiple keywords subset search.*

I INTRODUCTION

Secure search over encrypted remote knowledge is crucial in cloud computing to ensure the info privacy and usefulness. to stop unauthorized knowledge usage, fine-grained access management is important in a multi-user system. However, the approved users could by choice leak the key for monetary profit. Thus, tracing and revoking the malicious user WHO abuses secret key must be resolved imminently. during this paper, we have a tendency to propose associate degree written agreement free traceable attribute primarily based multiple keywords set search system with verifiable outsourced secret writing (EF-TAMKS-VOD). The key written agreement free mechanism may effectively forestall the key generation center (KGC) from unscrupulously looking out and decrypting all encrypted files of users. Also, the secret writing method solely needs radical light-weight computation, which could be a fascinating feature for energy-limited devices. additionally, economical user revocation is enabled when the malicious user is puzzled out. Moreover, the projected system is in a position to support a versatile range of attributes instead of polynomial finite. versatile multiple keywords set search pattern is realized, and also the modification of the question keywords order doesn't have an effect on the search result. Security analysis indicates that EF-TAMKS-VOD is incontrovertibly secure. Analysis results show that EF-TAMKS-VOD that improves the potency and greatly reduces the overhead of users' terminals.

II LITERATURE SURVEY:

Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud[1] Wenhai Sun, Shucheng Yu, Wenjing Lou, Y. Thomas Hou Search over encrypted data is a critically important enabling technique in cloud computing, where encryption-before outsourcing is a fundamental solution to protecting user data privacy in the untrusted cloud server environment. Many secure search schemes have been focusing on the

single-contributor scenario, where the outsourced dataset or the secure searchable index of the dataset are encrypted and managed by a single owner, typically based on symmetric cryptography. In this paper, we focus on a different yet more challenging scenario where the outsourced dataset can be contributed from multiple owners and are searchable by multiple users, i.e. multi-user multi-contributor case. Inspired by attribute-based encryption (ABE), we present the first attribute-based keyword search scheme with efficient user revocation (ABKS-UR) that enables scalable fine-grained (i.e. file-level) search authorization. Our scheme allows multiple owners to encrypt and outsource their data to the cloud server independently. Users can generate their own search capabilities without relying on an always online trusted authority. Fine-grained search authorization is also implemented by the owner-enforced access policy on the index of each file. Further, by incorporating proxy re-encryption and lazy re-encryption techniques, we are able to delegate heavy system update workload during user revocation to the resourceful semi-trusted cloud server. We formalize the security definition and prove the proposed ABKS-UR scheme selectively secure against chosen-keyword attack.

Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption[2] Baodong Qin, Robert H. Deng, Shengli Liu, and Siqi Ma

Attribute-Based Encryption (ABE) with outsourced decryption not only enables fine-grained sharing of encrypted data, but also overcomes the efficiency drawback (in terms of ciphertext size and decryption cost) of the standard ABE schemes. Specifically, an ABE scheme with outsourced decryption allows a third party (e.g., a cloud server) to transform an ABE ciphertext into a (short) El Gamal-type ciphertext using a public transformation key provided by a user so that the latter can be decrypted much more efficiently than the former by the user. However, a shortcoming of the original outsourced ABE scheme is that the correctness of the cloud server's transformation can not be verified by the user. That is, an end user could be cheated into accepting a wrong or maliciously transformed output. In this paper we first formalize a security model of ABE with verifiable outsourced decryption by introducing a verification key in the output of the encryption algorithm. Then, we present an approach to convert any ABE scheme with outsourced deryption into an ABE scheme with verifiable outsourced decryption. The new approach is simple, general and almost optimal. Compared with the original outsourced ABE, our verifiable outsourced ABE neither increases the user's and the cloud server's computation costs except some non-dominant operations (e.g., hash computations), nor expands the ciphertext size except adding a hash value (which is less than 20 byte for 80-bit security level).

White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes[3] Jianting Ning, Xiaolei Dong, Zhenfu Cao

Ciphertext-policy attribute-based encryption

(CP-ABE) enables fine-grained access control to the encrypted data for commercial applications. There has been significant progress in CP-ABE over the recent years because of two properties called traceability and large universe, greatly enriching the commercial applications of CP-ABE. Traceability is the ability of ABE to trace the malicious users or traitors who intentionally leak the partial or modified decryption keys for profits. Nevertheless, due to the nature of CP-ABE, it is difficult to identify the original key owner from an exposed key since the decryption privilege is shared by multiple users who have the same attributes. On the other hand, the property of large universe in ABE enlarges the practical applications by supporting flexible number of attributes. Several systems have been proposed to obtain either of the above properties. However, none of them achieve the two properties simultaneously in practice, which limits the commercial applications of CP-ABE to a certain extent. In this paper, we propose two practical large universe CP-ABE systems supporting white-box traceability. Compared with existing systems, both the two proposed systems have two advantages: 1) the number of attributes is not polynomially bounded and 2) malicious users who leak their decryption keys could be traced.

Traceable CP-ABE: How to Trace Decryption Devices Found in the Wild[4] Zhen Liu, Zhenfu Cao, and Duncan S. Wong

In Ciphertext-policy attribute-based encryption (CP-ABE), ciphertexts are associated with access policies, which do not have to contain the identities of eligible

receivers, and attributes are shared by multiple users. CP-ABE is useful for providing fine-grained access control on encrypted data. However, it also has a practicality concern that a malicious user, with his attributes shared with other users, might leak his decryption privilege as a decryption blackbox, for some financial gain or other incentives, as there is little risk of getting caught. There are two types of decryption blackboxes that reflect different practical scenarios. A key-like decryption blackbox is associated with an attribute set *SD* and can decrypt ciphertexts with access policies satisfied by *SD*. A policy-specific decryption blackbox is associated with an access policy A*D* and can decrypt ciphertexts with A*D*. Policy-specific decryption blackbox has weaker decryption capacity than key-like decryption blackbox, but tracing it is deemed to be more difficult. In the preliminary version (in CCS 2013) of this paper, we proposed a new CP-ABE scheme which is adaptively traceable against key-like decryption blackbox. The scheme has sublinear overhead, which is the most efficient one to date supporting fully collusion-resistant blackbox traceability. The scheme is fully secure in the standard model, and supports any monotonic access structures. In this paper, we further show that the scheme is also selectively traceable against policy-specific decryption blackbox. Furthermore, and more importantly, we prove a general statement that if a CP-ABE scheme is (selectively) traceable against policy-specific decryption blackbox, it is also (selectively) traceable against key-like decryption blackbox, which implies that we now only need to focus on building CP-ABE schemes which are traceable against policy-specific decryption blackbox.

Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-encryption Function for E-health Clouds[5] Yang Yang and Maode Ma

Electronic health (e-health) record system is a novel application that will bring great convenience in healthcare. The privacy and security of the sensitive personal information is the major concern of the users, which could hinder further development and widely adoption of the systems. The searchable encryption (SE) scheme is a technology to incorporate security protection and favorable operability functions together, which can play an important role in the e-health record system. In this paper, we introduce a novel cryptographic primitive named as conjunctive keyword search with designated tester and timing enabled proxy re-encryption function (Re-dtPECK), which is a kind of time-dependent searchable encryption scheme. It could enable patients to delegate partial access rights to others to operate search functions over their records in a limited time period. The length of the time period for the delegatee to search and decrypt the delegator's encrypted documents can be controlled. Moreover, the

delegatee could be automatically deprived of the access and search authority after a specified period of effective time. It can also support the conjunctive keywords search and resist the keyword guessing (KG) attacks. By the solution, only the designated tester isable to test the existence of certain keywords. We formulate a system model and a security model for the proposed Re-dtPECK scheme to show that it is an efficient scheme proved secure in the standard model. The comparison and extensive simulations demonstrate that it has a low computation and storage overhead.

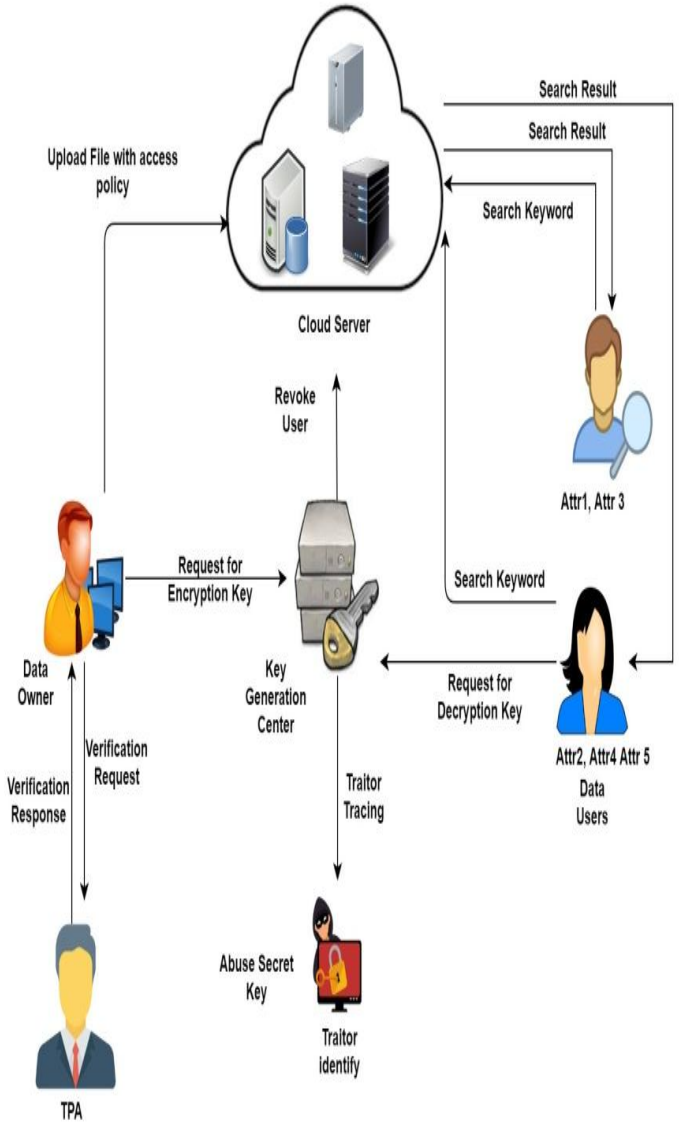
III PROPOSED SYSTEM:

We propose associate written agreement free traceable attribute primarily based multiple keywords set search system with verifiable outsourced cryptography (EF-TAMKS-VOD). The key written agreement free mechanism may effectively forestall the key generation center (KGC) from unscrupulously looking out and decrypting all encrypted files of users. Also, the cryptography method solely needs extremist light-weight computation, which could be a fascinating feature for energy-limited devices. Additionally, economical user revocation is enabled when the malicious user is discovered. Moreover, the projected system is ready to support a versatile variety of attributes instead of polynomial delimited. Versatile multiple keywords set search pattern is accomplished, and also the modification of the question keywords order doesn't have an effect on the search result.

ADVANTAGES:

1. Improves the efficiency.
2. Reduces the computation overhead

IV SYSTEM ARCHITECTURE:

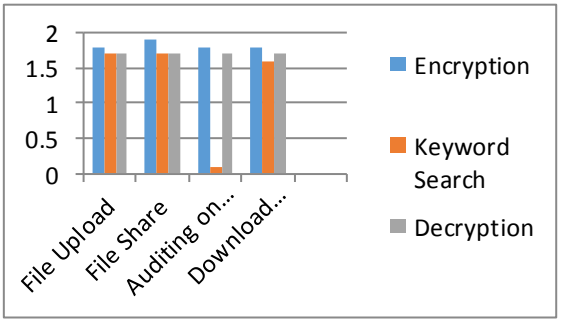


V ALGORITHM DETAILS

AES Algorithm

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (ciphertext).

VI RESULT AND SCREEN SHOTS



	Encryption	Keyword Search	Decryption
File Upload	1.8	1.7	1.7
File Share	1.9	1.7	1.7
Auditing on File	1.8	0.1	1.7
Download File	1.8	1.6	1.7

VII CONCLUSION:

The social control of access control and also the support of keyword search square measure necessary problems in a secure cloud storage system. during this work, we tend to outline a replacement paradigm of a searchable encoding system and planned a concrete construction. It supports versatile multiple keywords set search and solves the key written agreement downside throughout the key generation procedure. Malicious user United Nations agency sells secret key for profit is copied. The coding operation is partially outsourced to a cloud server and also the correctness of half-decrypted result is verified by the information user. The performance analysis and simulation show its potency in computation and storage overhead. Experimental results indicate that the computation overhead at the user's terminal is considerably reduced, which greatly saves the energy for resource-constrained devices of users.

REFERENCES:

[1] W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, "Protecting Your Right: Verifiable Attribute-based Keyword Search with Finegrained Owner-enforced Search Authorization in the Cloud," IEEE Transactions on Parallel and Distributed Systems, 2016, vol. 27, no. 4, pp. 1187-1198.

[2] 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, vol. 10, no. 7, pp. 1384-1394.

[3] 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, vol. 10, no. 6, pp. 1274-1288.

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

[5] 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, vol. 11, no. 4, 746-759.

[6] 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, vol. 238, pp. 221-241.

[7] A. Sahai, B.Waters, "Fuzzy identity-based encryption," in: EUROCRYPT, Springer, 2005, vol. 3494, pp. 457-473.

[8] J. Han, W. Susilo, Y. Mu. "Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption," IEEE Transactions on on Information Forensics and Security, 2015, vol. 10, no. 3, 665-678.

[9] Y. Shi, Q. Zheng, J. Liu. "Directly revocable key-policy attributebased encryption with verifiable ciphertext delegation," Information Sciences, 2015, vol. 295, pp. 221-231.

[10] X. Ma , J. Lai, Q. Mei, K. Chen and J.Weng, "Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption," IEEE Transactions on Dependable and Secure Computing, publish online, DOI: 10.1109/TDSC.2015.2423669.

[11] R. Ostrovsky, A. Sahai, B. Waters, "Attribute-based encryption with nonmonotonic access structures," in: 14th ACM Conference on Computer and Communications Security, ACM, 2007, pp. 195-203.

[12] C. Wang, J. Luo, "A key-policy attribute-based encryption scheme with constant size ciphertext," in: 8th International Conference on Computational Intelligence and Security, 2012, pp. 447-451.

[13] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," In: 5th International Conference on Provable Security, Springer, 2011, pp. 84-101.

[14] S. Hohenberger, B. Waters, "Attribute-based encryption with fast decryption," in: PKC, springer, 2013, vol. 7778, pp. 162-179.

[15] D. Nishant, J. Devesh, "Fully secure ciphertext policy attributebased encryption with constant length ciphertext and faster decryption," Security and Communication Networks, 2014, vol. 7, no. 11, pp. 1988-2002.