IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

ENHANCED ON DATA ENCRYPTION AUTHORIZATION SEARCH SYSTEM FOR SECURE CLOUD STORAGE

G.ESWARI MEGHANA[1], M.M.BALAKRISHNA[2]
[1] PG SCHOLAR, DEPT OF CSE, ST.MARY'S GROUP OF INSTITUTION,GUNTUR, AP, INDIA.
[2]ASST. PROFESSOR[M.TECH], DEPARTMENT OF CSE, ST.MARY'S GROUP OF INSTITUTION, GUNTUR, AP, INDIA.

Abstract: 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 escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption (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.

1.INTRODUCTION

WITH the development of new computing paradigm, cloud computing [1] 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 [2], [3] become the most prominent problem that hinders the widespread adoption of data storage in public cloud infrastructure. Encryption is a fundamental method to protect data privacy in remote storage [4]. However, how to effectively execute keyword search for plain text becomes difficult for encrypted data due to the unread ability of cipher text. Searchable encryption provides mechanism to enable keyword search over encrypted data [5], [6]. 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 [9] allows user to recover the message with ultra lightweight decryption [10], [11]. However, the cloud server might return wrong half-decrypted information as a result of malicious attack or system malfunction. More importantly, in the original definition of PEKS scheme [12], key generation centre (KGC) generates all the secret keys in the system, which inevitably leads to the key escrow problem. That is, the KGC knows all the secret keys of the users and thus can unscrupulously search and decrypton all encrypted files, which is a significant threat to data security and privacy. Beside, the key escrow problem brings another problem when traceability ability is realized in PEKS. If a secret key is found to be sold and the identity of secret key’s owner (i.e.,thetraitor) is identified, the traitor may claim that the secret key is leaked by KGC. There is no technical method to distinguish who is the true traitor if the key escrow problem is not solved.1.1 Related Work 1.1.1 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.

2.LITERATUREREVIEW

Secure ranked keyword search over encrypted cloud data by C. Wang, N. Cao, J. Li, K. Ren, W. Lou

As Cloud Computing becomes prevalent, sensitive information are being increasingly centralized into the cloud. For the protection of data privacy, sensitive data has to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow users to securely search over encrypted data through keywords, these techniques support only boolean search, without capturing any relevance of data files. This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. On the one hand, users, who do not necessarily have pre-knowledge of the encrypted cloud data, have to post process every retrieved file in order to find ones most matching their interest, On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today's pay-as-you-use cloud paradigm. In this paper, for the first time we define and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE). Thorough analysis shows that our proposed solution enjoys ``as-strong-as-possible" security guarantee compared to previous SSE schemes, while correctly reali...

Privacy-preserving Double-Projection Deep Computation Model with Crowdsourcing on Cloud for Big Data Feature Learning by Q.Zhang,L.T.Yang,Z.Chen,P.Li,M.J.Deen

Recent years have witness a considerable advance of Internet of Things with the tremendous progress of communication theories and sensing technologies. A large number of data, usually referring to big data, have been generated from Internet of Things. In this paper, we present a double-projection deep computation model (DPDCM) for big data feature learning, which projects the raw input into two separate subspaces in the hidden layers to learn interacted features of big data by replacing the hidden layers of the conventional deep computation model (DCM) with double-projection layers. Furthermore, we devise a learning algorithm to train the DPDCM. Cloud computing is used to improve the training efficiency of the learning algorithm by crowdsourcing the data on cloud. To protect the private data, a privacy-preserving DPDCM (PPDPDCM) is proposed based on the BGV encryption scheme. Finally, experiments are carried on Animal-20 and NUS-WIDE-14 to estimate the performance of DPDCM and PPDPDCM by comparing with DCM. Results demonstrate that DPDCM achieves a higher classification accuracy than DCM. More importantly, PPDPDCM can effectively improve the efficiency for training parameters, proving its potential for big data feature learning.

3.EXISTING SYSTEM

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 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.

4. PROPOSED SYSTEM

EF-TAMKSVOD achieves fine-grained data access authorization 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 KW0 and generates a trapdoor TKW0 using his secret key. In the test phase, if the attributes linked with user's secret key satisfy the file's access policy and KW0 (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 KW0 can be arbitrarily changed, which does not affect the search result. EF-TAMKS-VOD supports flexible system extension, which accommodates flexible 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.

5. SYSTEM ARCHITECTURE:

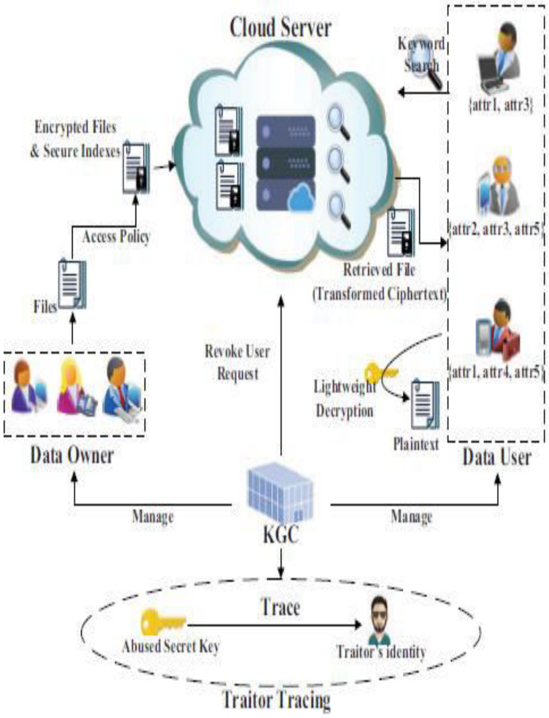


Fig 4.1 architecture Diagram

6.IMPLEMENTATION

Data Owner

In this module, he logs in by using his/her user name and password. After Login the owner Uploads Data, View Files Blocks.

End User

In this module, he logs in by using his/her user name and password. After Login the user will do some operations such as Request Search Permission, Download Request ,View All Files, Download File.

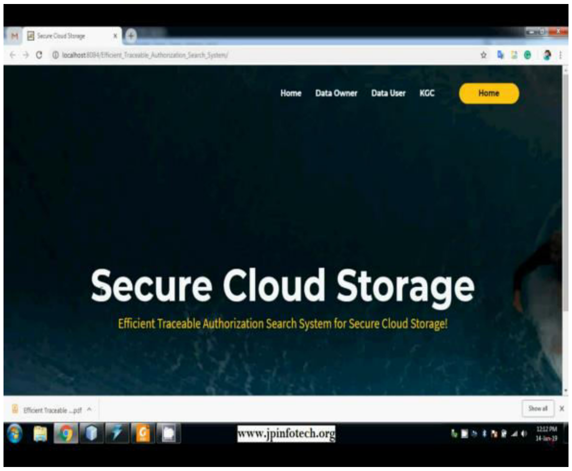
Fog Server

In this module, the Fog Server can do following operations such as View Files Blocks,View All Fog User Details and process the end user operations to send data block.

Cloud Server

The Cloud server as a server to provide data storage service and can also do the following operations such as View End Users and Authorize ,View Data Owners and Authorize, View All Stored Data, View Transactions ,View Attackers, View Search Request, View Download_Request,View Files Rank In Chart, View Time Delay In Chart, View Throughput In Chart

7.SCREEN SHOTS



Secure Cloud Storage

Efficient Traceable Authorization Search System for Secure Cloud Storage!

8.CONCLUSION

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. 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 efficiency 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.

9.BIBILOGRAPHY

[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 PublicKey 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 privacypreservingoutsourcedcalculationtool kitwithmultiplekeys."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 Transactions 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 Finegrained Owner-enforced Search Authorization 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 EfficientDataSharingforSecureCloudStorage

,"IEEETransactions onInformationForensicsandSecurity,2015,vol.10,no.9,pp.19811992.

[9] M.Green,S.Hohenberger,andB.Waters,"Outsourcingthedecryption 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 encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 13431354.

[11] B.Qin,R.H.Deng,S.Liu,andS.Ma,"Attribute-BasedEncryption with Efficient Verifiable Outsourced Decryption," IEEE Transactions 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 traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," 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 Traceable 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, "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.

[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 FuzzyKeywordSearch:AProvablySecureSchemeunderKeyword 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 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.

[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.