International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Secure and Efficient Traceable Authorization multi keyword search System for cloud storage using Blockchain Technology

Miss.Geeta Bajirao Biradar and Prof. Dr.Archana C Lomte

Department of Computer Engineering Bhivarabai Sawant Institute of Technology and Research Savitribai Phule Pune University

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

A countless data owners have moved their information into cloud servers for their benefit for multiprocessing, where secret and sensitive information must be encrypted first and then they are stored into cloud. Keyword search over encrypted data is very important in cloud computing. To give security to unapproved data access, fine-grained access control is important in multi-owner system. Sometime authorized owner's loss the secret key for some amount. Thus, tracing and revoking the unauthorized user who abuses secret key should be comprehended quickly. In this paper, propose a recognizable attribute based multiple keywords subset search system with verifiable outsourced decryption. Keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords. In our solution, we extract the keywords from the file and encrypted the keywords then added into the index. Instead of storing file and searchable index on a cloud system, the proposed system will store the file on cloud and store searchable index on a private server. Which greatly reduces network congestion and representation overheads, also retrieval fast for files, and reduces the storage by file compression With enhanced security using encryption techniques and permission to access the data, through accurate security analysis, we show that our proposed solution is secure and privacy-preserving.

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

Introduction

Outsourcing data to the public cloud facilitates attractiveness business strategy for many organizations due to demand Availability of data / services at cheaper rates efficiently. However, data security and privacy have become important. Concern for the service provider and service consumers by adopting the cloud service, especially for the public cloud, for the organization's commercial purposes. Outsourced data can contain confidential information, such as financial records of an individual or organization, offers information presented to tender, personal medical records (PHR), etc., where the data may allow the cloud server or unauthorized users access and / or infer sensitive information.

To face the problem of data privacy and access control, a practical solution is Encrypt documents before outsourcing them to the cloud storage server Consider the applications where most data owners use public cloud storage services to upload your encrypted documents and multiple users can access Documents stored on the cloud storage server Of such applications, applying the fine-grained access control policy enable the security check provided when accessing documents. Searchable Encryption provides mechanism to enable keyword search over encrypted data.

Searchable encryption can help a receiver to securely and selectively retrieve the data from public cloud storage, which is of user's interest and which is accessible to user. For example, a doctor wants to search for all the records of his patients who have been diagnosed with chronic kidney disease and for which doctor has been provided the access rights to patient's medical records, where each report is encrypted and uploaded by the patient. The application of single-user searchable symmetric encryption schemes in such scenario is not an effective mechanism, as the patient requires to encrypt his medical reports with his secret key and then shares this secret key with doctor. Therefore, multi-user searchable symmetric encryption schemes [6–8] are most effective, as the requirement of search over encrypted data and enforcing access control policy, where a data owner such as patient can generate the shared secret key or search token from his master secret key and issue them to the authorized users (e.g., doctor in our example) for searching over encrypted data. Although these schemes can work in single-sender multi-

receiver setup, they cannot perform well in multi-sender multi-receiver scenario, because each data sender has to communicate with each of the data receiver in a secure manner to issue the secret key or search token, which will cost large communication overhead.

The authorized entities may illegally leak their secret key to a third party for profits. Suppose that a patient someday suddenly finds out that a secret key corresponding his electronic medical data is sold on e-Bay. Such despicable behavior seriously threatens the patient's data privacy. Even worse, if the private electronic health data that contain serious health disease is abused by the insurance company or the patient's employment corporation, the patient would be declined to renew the medical insurance or labor contracts. The intentional secret key leakage seriously undermines the foundation of authorized access control and data privacy protection. Thus, it is extremely urgent to identify the malicious user or even prove it in a court of justice. In attribute based access control system, the secret key of user is associated with a set of attributes rather than individual's identity. As the search and decryption authority can be shared by a set of users who own the same set of attributes, it is hard to trace the original key owner. Providing traceability to a fine-grained search authorization system is critical and not considered in previous searchable encryption systems.

A. Motivation

Inflexible authorized keyword search - In the secure cloud storage system, a lot of documents are stored in encrypted form. It is necessary to provide flexible secure keyword query function to facilitate the document search. In addition, the cloud files are desired to be shared among different data users using a flexible authorization mechanism.

Inflexible system extension - If a new attribute is to be added to the system, the entire system has to be reconstructed and all encrypted files have to be re-encrypted. It would be a disaster to the cloud storage system.

Abuse of attribute secret key - The authorized entities may illegally leak their secret key to a third party for profits.

Inefficient user revocation - User revocation function is important for a multi-user cloud storage system.

Key escrow problem - In traditional searchable encryption schemes the users' secret keys are all generated by the key generation center (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".

Data Security – main issue is privacy of data

Review of Literature

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 [1].

"Public key encryption with keyword search We consider the issue of looking for on data that is encoded using an open key system. Consider customer Bob who sends email to customer Alice mixed under Alice's open key. An email entryway needs to test whether the email contains the catchphrase "sincere" with the objective that it could course the email fittingly. As another portrayal, consider a mail server that stores various messages straightforwardly encoded for Alice by others. Utilizing our instrument Alice can send the mail server a key that will empower the server to see all messages containing some explicit catchphrase, in any case get nothing else. We depict open key encryption with watchword demand and give two or three enhancements [2].

"Vabks: Verifiable attribute-based keyword search over outsourced encrypted data" Typically nowadays for data proprietors to re-appropriate their data to the cloud. Since the cloud can't be totally trusted, the re-appropriated data should be encoded. This in any case brings an extent of issues, for instance, How should a data proprietor give look capacities to the data customers? In what way can the endorsed data customers look for over a data proprietor's re-appropriated mixed data? By what means can the data customers be ensured that the cloud dependably executed the interest assignments for the wellbeing of they? Impelled by these request, we propose a novel cryptographic course of action, called evident trademark based catchphrase look (VABKS). The game plan allows a data customer, whose accreditations satisfy a data proprietor's passageway control system, to (I) investigate the data proprietor's re-appropriated encoded data, (ii) redistribute the grim interest errands to the cloud, and (iii) affirm whether the cloud has constantly executed the request exercises. We formally describe the security essentials of VABKS and portray an improvement that satisfies them. Execution appraisal exhibits that the proposed plans are reasonable and deployable [3].

Fluffy character based encryption. We present another sort of Identity-Based Encryption (IBE) plot that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we see a way of life as set of illuminating properties. A Fuzzy IBE invent thinks about a private key for a character, , to unravel a figure content encoded with a personality, 0 , if and just if the characters and 0 are near each other as assessed by the ”set cover” clear measurement. A Fuzzy IBE plan can be connected with enable encryption using biometric duties as identities; the error obstruction property of a Fuzzy IBE plot is totally what considers the use of biometric characters, which ordinarily will have some clamor each time they are dismembered. In like manner, we demonstrate that Fuzzy-IBE can be utilized for a sort of utilization that we term ”trademark based encryption”. In this paper we indicate two headways of Fuzzy IBE plans. Our headways can be seen as an Identity-Based Encryption of a message under several properties that shape a (padded) character. Our IBE structures are both blunder tolerant and secure against intrigue ambushes. Moreover, our essential headway does not utilize sporadic prophets. We demonstrate the security of our plans under the Selective-ID security show [4].

“Searchable encryption revisited: Consistency properties, relation to anonymous IBE and extensions” We see and fill two or three openings as to consistency (how much false positives are made) for open key encryption with watchword search for (PEKS). We depict computational and authentic relaxations of the present thought of impeccable consistency, demonstrate that the game plan of is computationally constant, and give another course of action that is quantifiably trustworthy. We in like way give a distinction in a weird IBE plan to an anchored PEKS plot that, not in any way like the past one, ensures consistency. At long last we propose three improvements of the essential insights considered here, explicitly astounding HIBE, open key encryption with brief catchphrase demand, and character based encryption with watchword look [5].

“Anonymous hierarchical identity-based encryption (without random oracles)” We show a character based cryptosystem that highlights absolutely cloud figure writings and distinctive leveled key task. We give a proof of security in the standard model, in light of the fragile Decision Linear multifaceted nature supposition in bilinear social gatherings. The framework is incredible and supportive, with little figure writings of size direct in the noteworthiness of the chain of hugeness. Applications join enthusiasm on encoded information, absolutely private correspondence, and so forth. Our outcomes settle two open issues relating to darken character based encryption, our course of action being the first to offer provable puzzle in the standard model, regardless of being the first to perceive absolutely peculiar HIBE at all measurements in the chain of significance [6].

“Efficient public key encryption with revocable keyword search” Open key encryption with watchword look is a novel cryptographic rough engaging one to look for on the encoded data explicitly. In the known plans, once getting a trapdoor, the server can look for related data without any confinements. In any case, really, it is once in a while crucial to shield the server from glancing through the data all the time in light of the way that the server isn’t totally trusted. In this paper, we propose open key encryption with revocable watchword chase to address the issue. We in like manner develop a strong improvement by dividing the whole presence of the system into specific events to achieve our destinations. The proposed plot achieves the properties of the caprice of cipher texts against a flexible picked watchwords ambush security under the co-decisional bilinear Diffie Hellman assumption in our security illustrate. Differentiated and two somewhat plots, our own offers much better execution to the extent computational expense [7].

“Practical techniques for searches on encrypted data” It is alluring to store information on information stockpiling servers, for example, mail servers and record servers in encoded shape to diminish security and protection dangers. Yet, this as a rule suggests that one needs to forfeit usefulness for security. For instance, if a customer wishes to recover just archives containing certain words, it was not already known how to let the information stockpiling server play out the inquiry and answers the question without loss of information classification [8].

”A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data”proposed the security for preserving Multikeyword Rank Searchable Encryption (MRSE) and establish a set of strict privacy requirement for such secure cloud data. TF x IDF for index construction and query generation was used in encrypted cloud data. Greedy depth first search algorithm was used for multi key search. Security is protected by two threat model KNN. Among various multikeys semantic the efficient principle of matching query is used[9].

”An Efficient Ranked Multi-Keyword search for Multiple Data Owners over Encrypted Cloud Data”:developed novel MDS(Multiple Data Source) model which securely stores data on cloud .The secured data is made available for user using symmetric key encryption .They have used symmetric encryption key for encryption. The same key used for decryption by the user. Their schemes outperform in security, storage and efficiently search data. However, the same key which is used for encryption and decryption by both the parties which can easily hacked and also lengthy process to secure it[10].

”Semantic-based location recommendation with multimodal venue semantics”: Propose a novel multi-keyword fuzzy search scheme by exploiting the locality-sensitive hashing technique. Our proposed scheme achieves fuzzy matching through algorithmic design rather than expanding the index file. It also eliminates the need of a predefined dictionary and effectively supports multiple keyword fuzzy search[11].

”Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud”: Public key encryption algorithm for encrypting the data and invoke ranked keyword search over the encrypted data to retrieve the files from the cloud. We aim to achieve an efficient system for data encryption without sacrificing the privacy of data. Further, our ranked keyword search greatly improves the system usability by enabling ranking based on relevance score for search result, sends top most relevant files instead of sending all files back, and ensures the fi le retrieval accuracy[12].

”An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing”: present a privacy-preserving multikeyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, we propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy[13].

”Privacy preserving multi-keyword text search in the cloud supporting similarity based ranking”: presents a work which give a diagram of the idea of block-chain innovation and its capacity to disturb the universe of managing an account through encouraging worldwide cash settlement, shrewd contracts, mechanized keeping money records and advanced resources. In such manner, they first give a concise outline of the center parts of this innovation, and in addition the second-age contract-based improvements[14].

Proposed Methodology

Key Generation Center (KGC). KGC is responsible to produce the secret key sets for the users. When the users secret key is spilled for benefits or different purposes, KGC runs follow calculation to find the unauthorized users. After the traitor is KGC sends user revocation request to cloud server to revoke the users inquiry benefit.

Cloud server (CS) Cloud server has huge storage space and incredible processing ability, which gives on-request administration to the framework. Cloud server is responsible to store the information and data.

Data Owner Data Owner uses the distributed storage administration to store the documents. Before the data uploading, the Data Owner select the keyword set and scrambles it into secure file. The data is also scrambled to cipher text. During the encryption procedure, the access strategy is indicated and installed into the cipher text to acknowledge fine-grained get to control.

Data user using the secret key, data user can look on the encrypted documents, i.e., picks a keyword set that he needs to look. At that point, the keyword is encrypted to a trapdoor utilizing user 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.

A. Advantages of proposed system

- Flexible authorized keyword search – This proposed framework accomplishes fine-grained data access and supports various multiple keyword search on ciphertext.
- Traceability of Abused Secret Key - authorized user leaks or sells his secret key, white-box traceability is capable to identify who leaks the key.
- Efficient revocation from group - Once a user is identified as traitor through tracing algorithm, proposed system revokes this malicious user from the authorized group.
- Key Escrow Free - lightweight homomorphic encryption algorithm is utilized for key escrow problem.
- Data Security – In proposed system store encrypted data on block chain technology. In block chain data stored on nodes and data loss possibility is less due to data distribution.

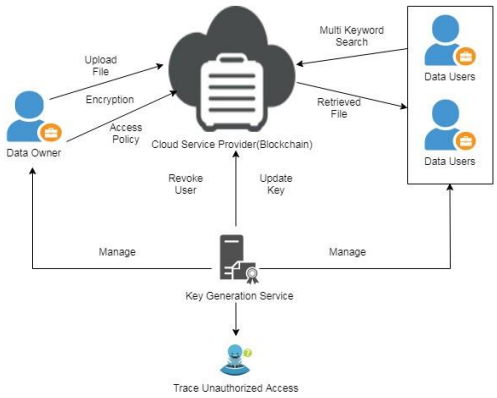

Fig. 1. Proposed System Architecture

C. Algorithm 1.

RSA Algorithms

• Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

• XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent

longer key; for example, if A is a 64-bit key, then AA,

AAA, etc., are equivalent keys.)
• Encrypt the all-zero string with the Blowfish algorithm,
using the data file described in steps (1) and (2).
• Replace P1 and P2 with the output of step (3).
• Encrypt the output of step (3) using the Blowfish algorithm with the modified data
• Replace P3 and P4 with the output of step (5).
2. Fully Homomorphism
• Cipher(plain Block[64],Round Keys[16,48],cipher Block[64])
•Permute
(64,64,plainBlock,intBlock,InitialPermutationTable)
• Split(64,32,inBlock,leftBlock,rightBlock)
• For(round=1 to 16)
• Mixer(left Block, right Block, round Keys[round])
• If(round!=16)swapper(left Block, right Block)
• Combine(32,64,leftBlock,rightBlock,OutBlock)
• Permute.

Results and Discussion

To evaluate the performance, the schemes in [1] and Proposed system are simulated using the Stanford javax.cipher library. The experiments on these schemes are conducted on a laptop running Windows operation system with the following settings: CPU: Intel core i5 CPU at 2.5GHz; RAM memory: 4 GB

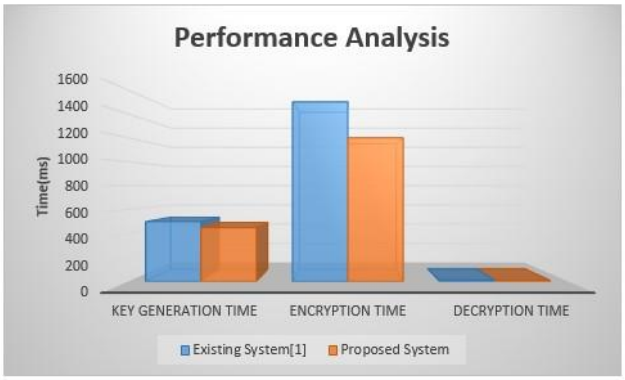

Fig. 2. Encryption Algorithm Performance

	ExistingSystem[1]	Proposed System
Key Generation Time	500ms	450ms
Encryption Time	1500ms	1200ms
Decryption Time	10ms	9ms

Conclusion

In this proposed system, implement multikeyword search on encrypted data and 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 framework of searchable encryption system, and proposed a concrete construction. It supports flexible multiple keywords subsetsearch, and solves the key escrow problem during the key generation procedure. Malicious user who sells secret key for benefit can be traced and encrypted data store in block chain nodes.

References

[1] Yang Yang, Ximeng Liu, Xianghan Zheng,Chunming Rong, Wenzhong Guo"Efficient Traceable Authorization Search System for Secure Cloud Storage"IEEE transactions on cloud computing 2018.
[2] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.
[3] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-K. R. Choo, "Fuzzy identity-based data integrity auditing for reliable cloud storage systems," IEEE Trans. Depend. Sec. Comput., to be published
[4] J. Hur, D. Koo, Y. Shin, and K. Kang, "Secure data deduplication with dynamic ownership management in cloud storage," IEEE Trans. Knowl.Data Eng., vol. 28, no. 11, pp. 3113–3125, Nov. 2016.
[5] J. Li, J. Li, D. Xie, and Z. Cai, "Secure auditing and deduplicating data in cloud," IEEE Trans. Comput., vol. 65, no. 8, pp. 2386–2396, Aug. 2016.
[6] Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," IEEE Trans. Depend. Sec. Comput., to be published.
[7] H. Wang, D. He, J. Yu, and Z. Wang, "Incentive and unconditionally anonymous identity-based public provable data possession," IEEE Trans. Serv. Comput., to be published.
[8] Y. Yu et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 767–778, Apr. 2017.
[9] Zhihua Xia, Xinhui Wang, Xingming Sun and Qian Wang, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE transactions on parallel and distributed systems, VOL. 27, NO. 2, february 2016.
[10] Tianyue Peng, Yaping Lin and Xin Yao, "An Efficient Ranked MultiKeyword search for Multiple Data Owners over Encrypted Cloud Data", IEEE transactions on cloud computing, vol. 18, no. 2 march 2018.
[11] X. Wang, Y. L. Zhao, L. Nie, Y. Gao, W. Nie, Z. J. Zha, and T. S. Chua, "Semantic-based location recommendation with multimodal venue semantics", IEEE Transactions on Multimedia, vol. 17, no. 3, pp. 409- 419, Mar. 2015.
[12] B. Wang, S. Yu, W. Lou, Y. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in: INFOCOM'14, Toronto, Canada, 2014.
[13] S. Pasupuleti, S. Ramalingam, R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," J NETW COMPUT APPL., vol. 64, pp. 12 – 22, 2016.
[14] W. Sun, B. Wang, N. Cao, H. Li, W. Lou, Y. Hou, H. Li, "Privacy preserving multi-keyword text search in the cloud supporting similarity based ranking," IEEE T Parall Distr., vol. 25, no. 11, pp. 3025 – 3035, 2014.