International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

ATTRIBUTE BASED ACCESS CONTROL SYSTEM FOR SECURE CLOUD STORAGES

Angel Johny[1], Jomina John[2]

[1]*Student,Department of Computer science, Rajagiri School of Engineering and Technology, Kerala,India*
[2]*Assistant Professor, Department of Computer science, Rajagiri School of Engineering and Technology,Kerala,India*

Abstract - *Secure search over encrypted data is crucial in cloud computing to ensure data privacy and usefulness. To prevent unauthorized data usage, fine-grained access control is necessary for a multi-user system. Authorized users may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the malicious user who abuses the secret key needs to be solved imminently. Thus, it is extremely urgent to identify the malicious user or even prove it in a court of justice. In an attribute-based access control system, the secret key of the user is associated with a set of attributes rather than an individual's identity*

Key Words: secret key, encryption, decryption, ABE, cloud

1. INTRODUCTION

Recently, as a replacement commercial model, cloud computing has attracted much attention from both academia and industry. A serious advantage of cloud computing is that it supplies virtually unlimited storage capabilities and elastic resource provisioning. so as to scale back the capital and operational expenditures for hardware and software, many IT enterprises and individuals are outsourcing their data to cloud servers rather than building and maintaining their own data centers. Despite clear benefits provided by cloud computing, there are many impediments to its widespread adoption. Data security and privacy concerns are probably the most important challenges. As outsourced data may contain much sensitive/private information, like Personal Health Records, personal photos and business documents, some cloud servers or unauthorized users are motivated to access and derive such sensitive/private information. Without addressing such concerns, users may hesitate to outsource their data to cloud servers. encoding is applied on users' data before outsourcing so on address the safety and privacy concerns .

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 unreadability of ciphertext. 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 an outsized amount of complex bilinear pairing operations. These overwhelmed computations become an important burden for user's terminal, which is particularly 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. Thus, it is an important issue to guarantee the correctness of outsourced decryption in public key encryption with keyword search (PEKS) system [12]. The authorized entities may illegally leak their secret key to a third party for profits [13]. 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 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 system, the key key of user is related to a group of attributes instead of individual's identity. As the search and decryption authority can beshared by a set of users who own the same set of attributes, it is hard to trace the original key owner [14], [15]. Providing traceability to a fine-grained search authorization system is critical and not considered in previous searchable encryption systems [7], [8], [12].

2. System Design

The system comprises of 4 entities, whose responsibilities and interactions are:

2.1 Key Generation Centre (KGC)

KGC is responsible to get the general public parameter for the system and therefore the public/secret key pairs for the users. Once the user's secret key's 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.

2.2 Cloud server (CS)

Cloud server has tremendous space for storing and powerful computing capability, which provides on-demand. Cloud server is responsible to store the info owner's encrypted files and respond on the info user's search query.

2.3 Data owner

Data owner utilizes the cloud storage service to store the files. Before the info outsourcing, the info owner extracts keyword set from the file and encrypts it into secure index. The document is additionally encrypted to ciphertext. During the encryption process, the access policy is specified and embedded into the cipher text to understand fine grained access control.

2.4 Data user

Each data user has attribute set to explain his characteristics, like professor, computing college, dean, etc. The attribute set is embedded into user's secret key. Using the key key, data user is in a position to look on the encrypted files stored within the cloud, i.e., chooses a keyword set that he wants to look . Then, the keyword is encrypted to a trapdoor using user's secret key. If the user's attribute set satisfies the access policy defined within 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.

Fig -1: System Design

3. SYSTEM OVERVIEW

3.1 New User Registration

When a user applies to join the application, KGC assigns an attribute set S to the user according to his identity. Then, KGC runs key generation algorithm to generate the public/secret keys for user.

3.2 Data Encryption

Here the data contributor uploads the document. The uploaded data is encrypted using AES encryption and is stored in the cloud.

3.3 Generate Keyword Trapdoor

If the data user wants to find all data owner's files that contain a certain keyword set KW0 = {kwγ1,⋯ ,kwγl2}, he generates a keyword trapdoor TKW0 using his secret key. The data user's attribute set is embedded into the trapdoor TKW0. Then, data owner submits TKW0 to cloud server for secure file retrieval

3.4 Retrieve Match Files and Outsourced Computing

When cloud server receives the keyword trapdoor from data user, it retrieves the data owner's encrypted files to find the match documents by the following two phases:

In the test phase, the encrypted files are deemed as match if the following two conditions satisfy:

1) Data user's attribute set satisfies the access policy of the searched file;
2) The searched keyword set in keyword trapdoor is a subset of that in the secure index

3.5 File Recovery and Verification

The data user uses a simple exponentiation and division operation to recover the plaintext file. It is much more efficient than traditional searchable encryption schemes with fine-grained access control.

4. MODULE DESCRIBTION

4.1 New User Registration

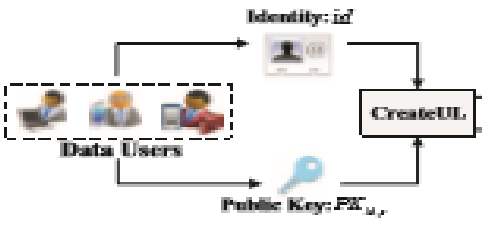

Fig -2: Registration Module Design

The system is implemented as a web application.

Data User

The data User registers in the registration portal using their name, email and other details. Successfully registered users login with username and password. Each users will have their own identity.

Create UserList

Admin will have a userlist for approval process. The data user who enters to this application can only use the operations which is provided after the approval of admin .Admin will authenticate that whether the data user is valid or not.

4.2 Data Encryption

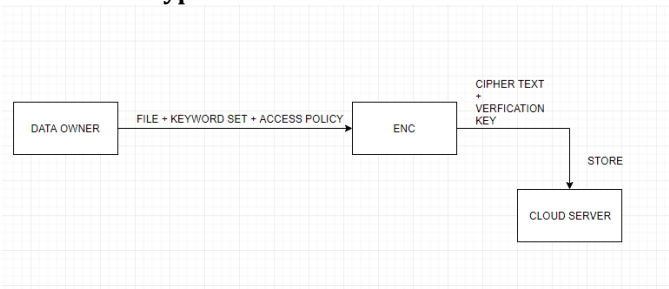

Fig -3: Data Encryption

Userlogin with their username and password and uploads the document. The uploaded document is encrypted using AES encryption.

Attribute-based encryption algorithm

Attribute-based encryption may be a quite algorithm of public key cryptography during which the private key's won't to decrypt data depends on certain user attributes like position, place of residence, type of account. Setup(, U) (PK, MK). The setup algorithm takes as input a security parameter and a universe description U, which defines the set of allowed attributes in the system. It outputs the general public parameters PK and therefore the master secret key MK. Encrypt(PK, M, S) CT. The encryption algorithm takes as input the general public parameters PK, a message M and a group of attributes S and outputs a ciphertext CT related to the attribute set. KeyGen(MK, A) SK. The key generation algorithm takes as input the master secret key MK and an access structure A and outputs a personal key SK related to the attributes. Decrypt(SK, CT) M. The decryption algorithm takes as input a personal key SK related to access structure A and a ciphertext CT related to attribute set S and outputs a message M if S satisfies A or the error message otherwise.

4.3 Generate Keyword Trapdoor

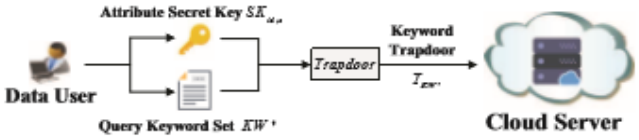

Fig -4: Generate Keyword Trapdoor

If the user wants to find all data owner's files that contain a particular keyword set KW0 = kw1,⋯ ,kwl2, he generates a keyword trapdoor TKW0 using his secret key. The info user's attribute set is embedded into the trapdoor TKW0. Then, data owner submits TKW0 to cloud server for secure file retrieval.

4.4 Retrieve Match Files and Outsourced Computing

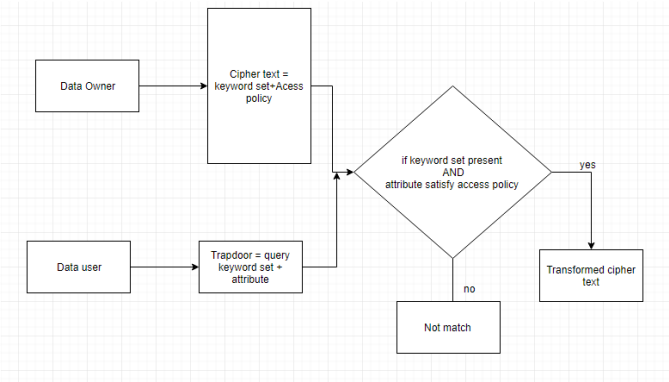

Fig-5 : Retrieve Match Files and Outsourced Computing

When cloud server receives the keyword trapdoor from data user, it retrieves the data owner's encrypted files to find the match documents by the following two phases: test phase and transformation phase. In the test phase, the encrypted files are deemed as match if the following two conditions satisfy: 1) data user's attribute set satisfies the access policy of the searched file; 2) the searched keyword set in keyword trapdoor is a subset of that in the secure index. In the transformation phase, the original cipher text is transformed into another form so that the data user can recover the message.

4.4 File Recovery and Verfication

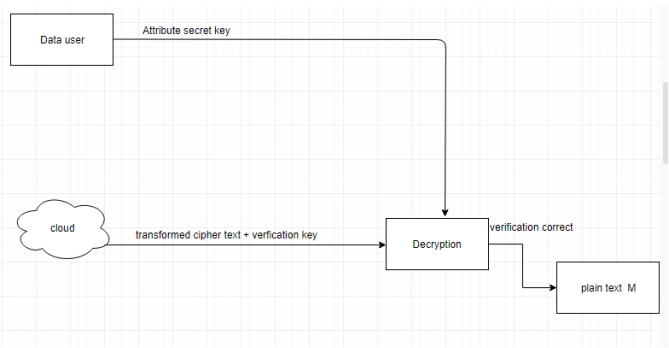

Fig-6: File Recovery and Verification Module Design

The data user uses a simple exponentiation and division operation to recover the plain text file. It is much more efficient than traditional searchable encryption schemes with fine-grained access control.

5. CONCLUSION

In this project, we proposed efficient secure cloud storage, which simultaneously guarantees data truthfulness and privacy .The data users have to truthfully submit their own data. Besides, the service provider is enforced to truthfully collect and process data. Furthermore, both the personally identifiable information and the sensitive raw data of data contributors are well protected. It helps to establish novel security problems, such as privacy preservation and data confidentiality.

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 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 privacypreservingoutsourcedcalculationtoolkitwithmultiple 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 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 Efficient Data Sharing for Secure Cloud Storage,"IEEE Transactions on Information Forensics and Security,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-Based Encryption 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.