International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 09, September 2017
ISSN: 2455-3778
http://www.ijmtst.com

Outsourced Attribute Based Encryption (OABE) Watchword Search Function for Cloud Computing

Kollipara Anil Kumar[1] | Shaik Akbarm[2]

[1]PG Scholar, Department of CSE, Mandava Institute of Engineering & Technology, Vidya Nagar, Jaggayyapet, Krishna Dt, Andhra Pradesh, India.
[2]Associate Professor, Department of CSE, Mandava Institute of Engineering & Technology, Vidya Nagar, Jaggayyapet, Krishna Dt, Andhra Pradesh, India.

To Cite this Article
Kollipara Anil Kumar and Shaik Akbarm, "Outsourced Attribute Based Encryption (OABE) Watchword Search Function for Cloud Computing", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 09, September 2017, pp.-81-85.

ABSTRACT

Outsourcing information to an outsider regulatory control, as is done in distributed computing, offers ascend to security concerns. The information trade off may happen because of assaults by different clients and hubs inside the cloud. In this manner, high safety efforts are required to ensure information inside the cloud. Notwithstanding, the utilized security system should likewise consider the enhancement of the information recovery time. In this paper, we propose Division and Replication of Data in the Cloud with Attribute based encryption (ABE) that by and large methodologies the security and execution issues. In this framework, we partition a document into sections, and repeat the divided information over the cloud hubs. Each of the hubs stores just a solitary piece of a specific information document that guarantees that even if there should arise an occurrence of a fruitful assault, no important data is uncovered to the aggressor. And furthermore, this sort of processing model conveys difficulties to the security and protection of information put away in cloud. Attribute based encryption (ABE) innovation has been utilized to configuration fine grained get to control framework, which gives one great strategy to understand the security issues in cloud setting. Be that as it may, the calculation cost and ciphertext measure in most ABE plans develop with the intricacy of the entrance arrangement. Outsourced ABE (OABE) with fine-grained get to control framework can to a great extent decrease the calculation cost for clients who need to get to encoded information put away in cloud by outsourcing the substantial calculation to cloud service provider (CSP).

Keywords: *file fragmentation, file replication,attribute-based encryption, outsourced key-issuing; outsourced decryption;*

I. INTRODUCTION

Security is the most important aspects among those the wide-spread adoption eclipse of cloud computing. Cloud security problem supported due to core technology implementation as like virtual machine (VM) escape or session riding, etc. The service offerings by cloud as SQL injection or less authentication system and cloud characteristics like information recovery vulnerability and Internet protocol vulnerability, data storages, etc. To secure cloud all the participating entities must be provides security. In the cloud security of the assets does not completely depend on an individual's security measures because an any given system with one or more units, the highest level of systems security is equal to level of the weak entity and so the neighbouring entities may provides an opportunity to an attacker. The off-line data storage cloud utility requires users to move data in clouds virtualized and shared environment that may result in various security procedures. Pooling and elasticity of cloud storage allows the physical resources to be the shared maximum users. Shared resources may be reassigned to other users at same instance of time that may result in data compromise through data recovery techniques. The information similarly, cross-tenant virtualizes network accessing may also compromise data Safety and data integrity. Inapplicable media sanitization can also hack customer's private data. The Unauthorized information/data accessing by user and processes must be prevented. This system is useful to user for successfully store the fragramts. In such criteria, the security mechanism must be the substantially increasing an attacker's/hacker effort to retrieve a reasonable amount of data even after the successful attack in the cloud storage.The sufficient amount of loss information present public data integrity auditing with division and replication of data in cloud system that judicially fragments user text files into small part and replicates them at strategic locations within the cloud. We develop a scheme for outsourced data that takes into account both the security and performance. The proposed scheme fragments and replicates the data file over cloud nodes. The proposed System scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker.

In ABE Attribute based encryption,We consider the case that the user Alice has a large number of data stored in the cloud. If Alice submits a request for accessing the encrypted data stored in the CSP, according to the traditional outsourced ABE scheme, the CSP downloads all the data, executes partial decryption and responses all corresponding data of Alice. This greatly increases the cost for communication and storage at Alice side. In this article, we organically integrate outsourced -ABE (OABE) with PEKS and present a novel cryptographic paradigm called outsourced attribute-based encryption scheme with keyword search function (KSF-OABE). In our system, when the user wants to outsource his sensitive information to the public cloud, he encrypts the sensitive data under an attribute set and builds indexes of keywords. As a result, the users can decrypt the ciphertext only if their access policies satisfy the corresponding attributes. By this way, when Alice submits the request with a trapdoor corresponding to a keyword "current", CSP downloads all the data intended for Alice and just returns a partial ciphertext associated with the keyword "current". Therefore, Alice can exclude the data what she does not hope to read.Then also Cloud computing is a new computation model in which computing resources is regarded as service to provide computing operations. This kind of computing paradigm enables us to obtain and release computing resources rapidly. So we can access resourcerich, various, and convenient computing resources on demand. The computing paradigm also brings some challenges to the security and privacy of data when a user outsources sensitive data to cloud servers. Many applications use complex access control mechanisms to protect encrypted sensitive information. Sahai and Waters addressed this problem by introducing the concept for ABE. This kind of new public-key cryptographic primitive enables us to implement access control over encrypted files by utilizing access policies associated with ciphertexts or private keys.

II. RELATED WORK

1. "On the characterization of the structural robustness of data center networks,".

In this paper, Author studied the structural robustness of the state-of-the-art data center network (DCN) architectures [1]. Our results revealed that the DCell architecture degrades gracefully under all of the failure types as compared to the FatTree and ThreeTier architecture. Because of the connectivity pattern, layered architecture, and heterogeneous nature of the network, the results demonstrated that the classical robustness metrics are insufficient to quantify the DCN robustness appropriately. Henceforth, signifying and igniting the need for new robustness metrics for the DCN robustness quantification. We proposed deterioration metric to quantify the DCN robustness. The deterioration metric evaluates the network robustness based on the percentage change in the graph structure. The results of the deterioration metric illustrated that the DCell is the most robust architecture among all of the considered DCNs.

2. “Energy-efficient data replication in cloud computing datacenters,”.

This paper reviews the topic of data replication in geographically distributed cloud computing data centers and proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system [2]. Moreover, the optimization of communication delays leads to improvements in quality of user experience of cloud applications. The performance evaluation is carried out using Green Cloud – the simulator focusing on energy efficiency and communication processes in cloud computing data centers. The obtained results confirm that replicating data closer to data consumers, i.e., cloud applications, can reduce energy consumption, bandwidth usage, and communication delays significantly.

3.“An analysis of security issues for cloud computing,”.

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. Author presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines [3].

4. “Fuzzy Identity-Based Encryption.

Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term “attribute-based encryption”. In this paper Author present two constructions of Fuzzy IBE schemes [4]. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

5. “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data.

The Authors develop a new cryptosystem for one-grained sharing of encrypted data that we call Key-Policy Attribute Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Author demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption [5].

III. Implementation

We organically integrate outsourced-ABE (OABE) with PEKS and present a novel cryptographic paradigm called outsourced attribute-based encryption scheme with keyword search function (KSF-OABE).

In our system, when the user wants to outsource his sensitive information to the public cloud, he encrypts the sensitive data under an attribute set and builds indexes of keywords. As a result, the users can decrypt the cipher text only if their access policies satisfy the corresponding attributes. By this way, when Alice submits the request with a trapdoor corresponding to a keyword “current”, CSP downloads all the data intended for Alice and just returns a partial ciphertext associated with the keyword “current”. Therefore, Alice can exclude the data what she does not hope to read.

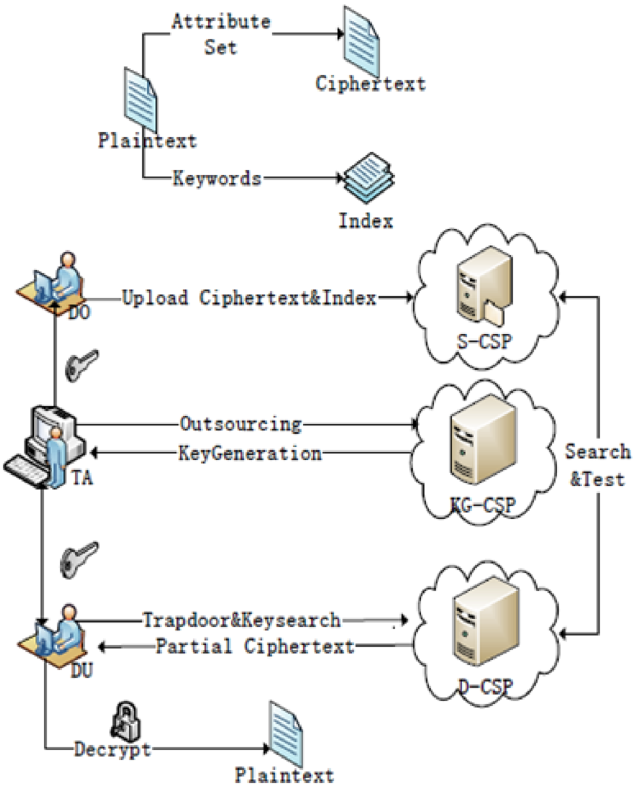
ADVANTAGES OF PROPOSED SYSTEM:

- The proposed scheme is efficient since we only need to download the partial decryption ciphertext corresponding to a specific keyword.
- The proposed system is the time-consuming pairing operation can be outsourced to the cloud service provider, while the slight operations can be

done by users. Thus, the computation cost at both users and trusted authority sides is minimized.

- The proposed scheme supports the function of keywords search which can greatly improve communication efficiency and further protect the security and privacy of users.

SYSTEM ARCHITECTURE:



Complexity Analysis

With the work in *PK, MK, SK, CT, TK, RK, CT* ‘represent the size of public key, master key, private key, ciphertext length, transform key, retrieving key and transformed ciphertext excluding the access structure respectively. Additionally, *Encrypt*, *Transform*, and denote the computational costs of the algorithms encryption, transformation, outsourcing decryption, decryption respectively. , denote the bit-length of the elements belong to, denote the -times calculation over the group, pairing and hash function. Let be the attribute universe. And are amount of the attributes associated with ciphertext and private key respectively.is the number of keywords associated with a ciphertext. As the operation cost over is muchless than group and pairing operation, we ignore the computational time over out Decrypt.

Efficiency Analysis

We compared the performance of the four stages in our scheme with the scheme. Our experiment is simulated with the java pairing-based cryptography (JPBC) library version 2.0.0, which is a port of the pairing-based cryptography (PBC) library C. When selecting a secure elliptic curve, two factors should be considered: the group size l of the elliptic curve and the embedding degree *d*. To achieve the 1024-bit RSA security, these two factors should satisfy. We implement our scheme on Type *A* curve, where *p* is 160 bits, l= 512. We select SHA–as the hash function. We implement our scheme and the scheme on a Windows machine with Intel Core 2 processor running at 2.13 GHz and 4G memory. The running environment of our experiment is Java Runtime Environment 1.7 (JRE1.7), and the Java Virtual Machine (JVM) used to compile our programming is 32 bit (x86) which brings into correspondence with our operation system.

To design a system for Division and replication of data in cloud with Attribute based encryption.Division and Replication of Data in the Cloud that judicially fragments user files into pieces and replicates them at strategic locations within the cloud.In proposed system, we collectively approach the issue of security and performance as a secure data replication problem.The division of a file into fragments is performed based on a given user criteria. Divided File can store in different nodes.Attribute based encryption (ABE) technology has been used to design fine-grained access control system, which provides one good method to solve the security issues in cloud setting.

In this paper, we collectively rules the issues of security and performance as a secure the file.Division and Replication of Data in the Cloud storage that fragments user files into small part and replicates them at strategic locations with into the cloud storage nodes. The division of a file into fragments is performing based on the giving input criteria such that as the individual fragments do not contain any meaningful data. Each of the cloud node(we use the term node to represent storage capacity, physical, and the virtual machines) contains will be distinct fragment to increase the more data security on cloud.

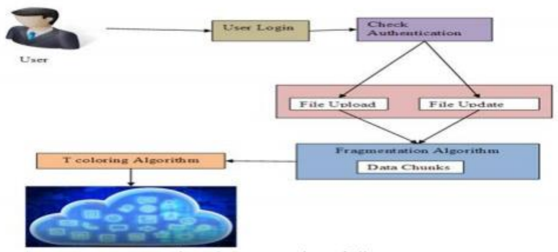


Figure 2: Fragmentations of File

IV. CONCLUSION

In this paper, the proposed that Division and replication of data in cloud with Attribute based encryption.The proposed system, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. And CP-ABE scheme that provides outsourcing key-issuing, decryption and keyword search function. Our scheme is efficient since we only need to download the partial decryption ciphertext corresponding to a specific keyword.In our scheme, the time-consuming pairing operation can be outsourced to the cloud service provider, while the slight operations can be done by users. Thus, the computation cost at both users and trusted authority sides is minimized.The Division and replication of data in cloud with Attribute Based Encryption. With help of trapdoor provider work is reduces.

REFERENCES

[1] K. Bilal, M. Manzano, S.U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013, pp. 64-77.

[2] D.Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446-451.

[3] J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. of IEEE INFOCOM 2014, Toronto, Canada, Apr. 2014, pp. 2121–2129.

[4] A. Sahai and B. Waters,"Fuzzy Identity-Based Encryption,"EUROCRYPT'05, LNCS, vol. 3494, pp. 457-473,2005.

[5] V. Goyal, O. Pandey, A. Sahai, andB. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc.13th ACM Conference on Computer and Communications Security(CCS'06), pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[6] J.G.Han, W. Susilo, Y. Mu andJ. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption,"IEEETransactions on Parallel and Distributed Systems,vol.23, no.11, pp. 2150-2162, Nov.2012, doi: 10.1109/TPDS.2012.50.

[7] T. Okamoto and K. Takashima, "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption,"CRYPTO'10, T. Rabin, ed., LNCS 6223, Berlin: Springer-Verlag, pp. 191-208, 2010.

[8] W.R.Liu, J.W.Liu, Q.H.Wu, B.Qin, and Y.Y.Zhou, "Practical Direct Chosen Ciphertext Secure Key-Policy Attribute-Based Encryption with Public Ciphertext Test,"ESORICS'14, LNCS 8713, Berlin: Springer-Verlag, pp. 91-108, 2014.