|| Volume 2 || Issue 4 || OCTOBER 2017|| ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

# A Review On- Reducing The Data Attacks On The Cloud By Dividing And Replicating The Data Over Multiple Cloud Nodes

**Prof. Khan Faisal Ali[1],Kanade Kalpana[2]**
*Asst Professor[1], P.G. Student[2],Department of Computer Science & Engineering, Everest College of Engineering & Technology, Aurangabad, Maharashtra, India*

*Abstract*— **The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, we propose Division and Replication of Data in the Cloud with Attribute based encryption (ABE) that collectively approaches the security and performance issues. In this system, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. And also, This kind of computing model brings challenges to the security and privacy of data stored in cloud. 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. However, the computation cost and cipher text size in most ABE schemes grow with the complexity of the access policy. Outsourced ABE (OABE) with fine-grained access control system can largely reduce the computation cost for users who want to access encrypted data stored in cloud by outsourcing the heavy computation to cloud service provider (CSP).**

***Keywords:*** *Attribute-based encryption; cloud computing; outsourced key-issuing, outsourced decryption, Division of Cloud Data.*

## I INTRODUCTION

The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes must be prevented. The main aim of our project is secure the files store on cloud. The division of a file into fragments is performed based on a given user criteria. A successful attack on a single node must not reveal the locations of other fragments within the cloud. [1]To keep an attacker uncertain about the locations of the file fragments and to further improve the security. These systems select the nodes in a manner that they are not adjacent and are at certain distance from each other. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time.

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. This system does not rely on traditional cryptographic techniques for data security. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations (placement and retrieval) on the data. this system ensure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security.[3]

Division and Replication of Data in the Cloud for Optimal Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (this system use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, this system select the nodes in a manner that they are not adjacent and are at certain distance from each other. The node separation is ensured by the means of the T-coloring[2]

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 cipher texts or private keys. Two types of ABE schemes, namely key-policy ABE (KPABE) and cipher text- policy ABE (CP-ABE) are proposed. For KP-ABE scheme, each cipher text is related to a set of attributes, and each users private key is

associated with an access policy for attributes. A user is able to decrypt a cipher text if and only if the attribute set related to the cipher text satisfies the ac- cess policy associated with the user s private key. For CP-ABE scheme, the roles of an attribute set and an access policy are reversed. Be then court provided a CP-ABE scheme, which ensures encrypted data is kept confidential even if the storage server is un trusted. In order to withstand collusion attack and avoid sensitive information leakage from access structure, Qian et al. proposed a privacy-preserving decentralized ABE scheme with fully hidden access structure. Deng et al. constructed a cipher text-policy hierarchical attribute based encryption (CP-HABE) with short cipher texts, which enables a CP-HABE system to host many users from different organizations by delegating keys. In CPABE scheme, a malicious user maybe shares his attributes with other users, which might leak his decryption privilege as a decryption black box due to financial profits.[4]

## II RELATED WORK

The shared resources may be reassigned to other users at some instance of time that may result in data compromise through data recovery methodologies. User module uploads the text file on the cloud storage. Then the admin module fragments the file using algorithms and store on each node. Presented a technique to ensure the integrity, freshness, and availability of data in a cloud. The data migration to the cloud is performed by the Iris file system. A gateway application is designed and employed in the organization that ensures the integrity and freshness of the data using a Markel tree. The file blocks, MAC codes, and version numbers are stored at various levels of the tree. The proposed technique in heavily depends on the users employed scheme for data confidentiality. Moreover, the probable amount of loss in case of data tempering as a result of intrusion or access by other VMs cannot be decreased. Our proposed strategy does not depend on the traditional cryptographic techniques for data security

In ABE Attribute based encryption, this system 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, this system 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 cipher text associated with the keyword “current”. Therefore, Alice can exclude the data what she does not hope to read.[5][6]

## III PROPOSED MODEL

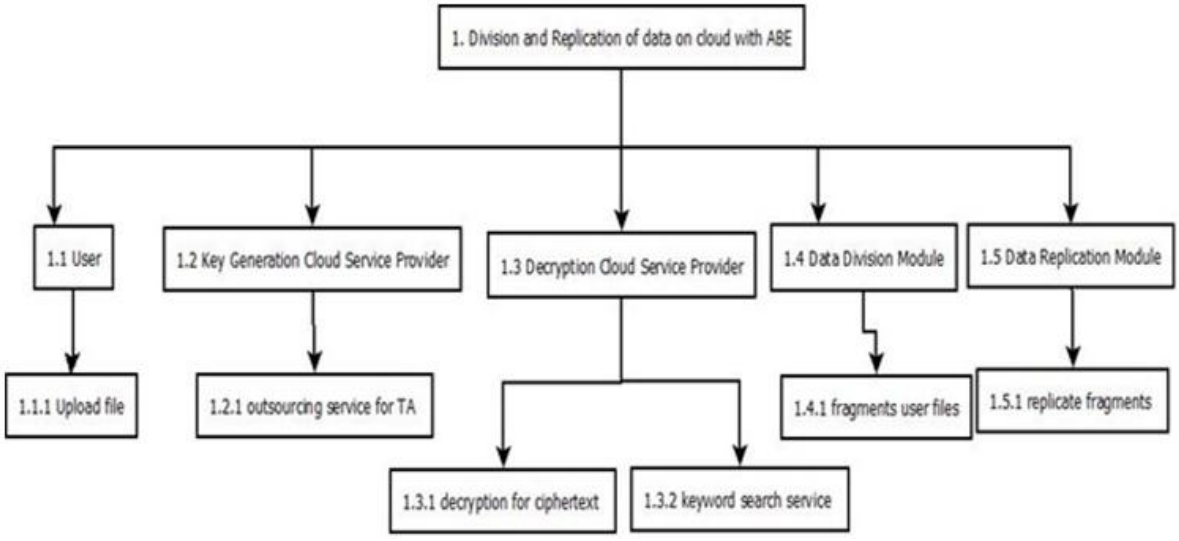


***Figure 1: Architecture***

1. **User module:**
**Data Owner (DO):** This is a participant who intends to upload and share his data files on the cloud storage system in a secure way. The encrypted cipher texts will be shared with intended receivers whose access structure will be satisfied by attribute set embedded in cipher texts, that is to say the predicate. The

responsibility of DO is to generate indexes for some keywords and upload encrypted data with the indexes.

**Data User (DU):** This is a participant who decrypts the encrypted data stored in S-CSP with the help of D-CSP. If the attribute set for DU satisfies the access structures, DU is able to access the encrypted files and recover the original files from it. DU downloads

**Key Generation Cloud Service Provider:**

**Trusted Authority (TA):** TA is the attribute authority centre, which is responsible for the initialization of system parameters, and the generation of attribute private keys and trap- door.

**Decryption Cloud Service Provider:** Decryption-Cloud Service Provider (D-CSP):It is a participant that supplies outsourcing computing service through accomplishing partial decryption for cipher texts and key- word search service on the partially decrypted cipher texts for data users who want to access the cipher text.

**Data Division (Fragmentation)/Replication Module:** The file fragmented means to be broken up into small pieces. This is exactly what happens to files when they become fragmented. They are broken down into small individual pieces and stored in random locations.

In a fragmentation schema file f is split into n fragments, all fragments are signed and distributed to n multiples nodes, one fragment per node. The user can reconstruct file f by accessing m fragments arbitrarily chosen.

## III PROPOSED ALGORITHM

### A. Attribute Based Encryption

**1. Setup**

This is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public parameters PK and a private key SK

**2. Encryption**

This algorithm takes as input a message m, a set of attributes , and the public
parameters PK. It outputs the cipher text E.

**3. Key Generation**

This algorithm takes as input an access structure A, the Private key SK and the public parameters PK. It outputs a decryption key D.

**4. Decryption**

This algorithm takes as input the cipher text E that was encrypted under the set of attributes, the decryption key D for access control structure A and the public parameters PK. It outputs the message M if A.

### B. Attribute Based Selection

An Attribute-Based Signature (ABS) scheme is parameterized by a universe of possible attributes A and message space M, and consists of the following algorithms.ABS. TSetup (to be run by a signature trustee): Generates public reference information TPK.[8] An Attribute-Based Signature (ABS) scheme is parameterized by a universe of possible attributes A and message space M, and consists of the following algorithms.[9][10]

1. ABS.TSetup (to be run by a signature trustee): Generates public reference
Information TPK.
2. ABS.ASetup (to be run by an attribute-issuing authority): generates a key pair
APK, ASK ABS.ASetup.
3. ABS.AttrGen: On input (ASK,AA), outputs a signing key SKA
4. ABS.Sign: On input (PK = (TPK, APK), SKA ,m M, ˆI), where ˆI(A) = 1, outputs a signature ¨I.
5. ABS.Ver: On input (PK = (TPK, APK), m, ˆI, 1), outputs a Boolean value.

## IV CONCLUSION

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. This system proposes a CP-ABE scheme that provides out- sourcing key-issuing, decryption and keyword search function. This proposed system will be efficient since this system only need to download the partial decryption cipher text corresponding to a specific keyword. 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 will be minimized. The Division and replication of data in cloud with Attribute Based Encryption. With help of trapdoor provider work is reduces

## REFERENCES

[1] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.

[2] 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.

[3] 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. .

[4] L. M. Kaufman, “Data security in the world of cloud computing,” IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[5] S. Pearson, Y. Shen and M. Mowbray, “A Privacy Manager for Cloud Computing,”Proc. First International Conference Cloud Computing(CloudCom09), M. Gilje-Jaatun,

G. Zhao and C. Rong, eds., LNCS 5931, Berlin: Springer-Verlag, pp. 90-106, 2009.

[6] W. K. Hale, "Frequency assignment: Theory and applications," Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.

[7] S. Pearson, Y. Shen and M. Mowbray, "A Privacy Manager for Cloud Computing,"Proc. First International Conference Cloud Computing(CloudCom'09), M. Gilje-Jaatun, G. Zhao and C. Rong, eds., LNCS 5931, Berlin: Springer-Verlag, pp. 90-106, 2009.

[8] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption,"EUROCRYPT05, LNCS, vol.3494, pp. 457-473,2005.

[9] V. Goyal, O. Pandey, A. Sahai, and B. 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.

[10] A. Lewko, T. Okamoto, A. Sahai, K. Takashimaand B. Waters, "Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,"EUROCRYPT10, H. Gilbert, ed., LNCS 6110, Berlin: Springer-Verlag, pp. 62-91, 2010.