Secure Access Control Method in Cloud Environment Using Improved Attribute Based Encryption Technique

S.U.Muthunagai , R. Anitha

Abstract*: Maintaining the user data on a proprietary nearby storage device becomes challenging task and the cloud-based storage addresses this issue possibly by storing them in a remote database through which user can access the files from anywhere. Cloud computing is on-demand computing, which provides various resources to the users, especially data storage and computing power, without the direct intervention of the user in the mode of pay per use. On moving to the Cloud storage, resources are shared but that hardware is likely being shared by other organizations too. The suspicion is due largely to the fact that the approach itself feels insecure, with user data deposited on servers and systems do not own or access control over the data. The data agreement may occur due to the intrusion of attackers in the cloud environment. Therefore, highly secure and dynamic access control methods are required to preserve and access the data in the cloud environment with minimal delay in network traffic. In this paper, the above security issues are addressed by fragmenting the user uploaded data and wrapping of fragmented data with the proposed Improved Attribute Based Encryption technique to accumulate at various locations. Preserving of cipher text at various points prevents the user uploaded data not been intervened by any intruders. Finally, the data located at the distinct point are retrieved with decryption technique and hence it scales down the network traffic occurred during the retrieval of user-uploaded data from the various point.

***Index Terms*:**
Cloud Security, Fragmentation, Encryption, Decryption, Network Traffic, Attribute Based Encryption.

I. INTRODUCTION

Cloud storage is a massive storage space aggregated from various cloud service provider through the network in which the enormous amount of digitalized data can be stored. Cloud computing is a new paradigm for the majority of users. Cloud refers to the chain of distributed computers which is used by many organizations, companies, institutions etc., to store the user data in remotely and transfer it as a service. A typical cloud storage system includes a master control over the server that connects both the client computers and a mesh of several database storage servers. The storage space extents multiple servers, in various locations which is frequently retained and governed by a hosting company. These cloud storage providers holds the responsibility of providing the user data available, accessible, and protected at all the time to the user. The user or organization who requires storage space will buy storage space from the cloud storage providers to store their owned data. The user data that is moved to the cloud storage, exists on allotted servers contained in huge warehouses. Once the data is placed into the cloud, it may be stored in different places. In fact, cloud storage providers take multiple copies of the data upload data and intentionally store those data in various spot to ensure that the data is not to be destroyed or be inaccessible.

In large-scale distributed storage systems, the issues related to availability of data and the time taken to response the user query is dealt with data replication strategies. However, placing of replica data over a number of nodes proportionally increases the attack surface for the user data. The proposed system, divides the user uploaded data to store at strategic locations to achieve optimal performance and security in the cloud environment. In order to avoid compromising with attackers the proposed technique stores the data at various places in encrypted format instead of storing the whole data on a single node so that the attacker cannot steal the data in readable format and also they were unaware of remaining part of data. The network traffic during the retrieval of large amount of data from same point is high and this has been addressed by the proposed system since the proposed system retrieves the data from various locations instead from same location.

This paper is organized as follows: Section 2 gives the framework for enhancing the attribute based encryption technique which is obtained from the related studies on attribute based encryption technique over cloud storage. The proposed model has been discussed in Section 3. Some of the Ideal Constraints of Attribute-Based Encryption were illustrated in Section 4. The proposed, Improved Attribute Based Encryption Technique with the implementation result is shown in Section 5 and Section 6. Finally Section 7 draws conclusions of proposed work with the challenges.

II. RELATED WORK

A methodology called DROPS, which divides the file into various fragments, and replicate each fragmented data over the cloud nodes. Each node in the cloud storage server stores a single fragment of a file that ensures that even in case of an attack of the data no meaningful information

Revised Manuscript Received on June 12, 2019

S.U.Muthunagai , Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, India,
R. Anitha, Department of Computer Science and Engineering, Sri Venkateswara College of Engineering , Chennai, India,

is revealed to the attacker meanwhile retrieval time and optimization of data also has been addressed in [1]. Distributed storage servers provides the facility of maintaining and managing the user data in remote method as a service. When user initiates communication with the other end, data has been transferred over a network and is directed to the store the data in server. But gathering redundant data will cause the server to store excess amount of data which has been addressed in [2]. The encryption technique in a cloud computing and security over static data is described in [3]. The security control strength at real-time congestion level of the system with the activated permissions for privacy of users is explained in [4]. In [5], cloud computing security strategy to ensure data integrity, confidentiality and availability, the storage provider is illustrated. These security measures involve the use of strong encryption techniques for data security and fine-grained authorization to control user access to data is identified in [6]. In [8] scheme at any time, data owner and/or TA is freely able to revoke any attribute of user. In [9] Goyal et al introduced another variant of ABE: Ciphertext-Policy ABE (CP-ABE). CP-ABE is reverse way of KP-ABE. This means ciphertext is associated with access structure and user secret key is embedded in set of attributes. Here the need of mechanism of fine-grained data access control is raised to work efficiently with semi trusted server. A promising approach would be to encrypt the data before it is outsourced to the semi trusted server. The best way to do so is to let allow data owner to decide with encryption and access mechanism [10]. Access to original data should only be given to those users who hold the proper decryption key. Besides this, data owner must hold the right to grant and revoke access privileges whenever necessary [11]. Fine-grained access control is in demand whenever the sensitive data needs to be disclosed. The access control method like, ACL-based access control is discussed in [12], capability-based access control is proposed in [13] whereas role-based access control in [14]. Making use of ACL based and capability-based cryptographic method leads towards the scalability issue. When ACL's are used as cryptographic method, complexity for encrypting the user data is increased linearly to the number of system users which leads to less scalable system. Capability-based access control does have the same system scalability issue. In role-based access control, remembering the authorized users list is not expected as access to data is granted on the basis of user's role [14]. For cryptographically enforced access control, Sahai and Waters [15] first introduced Public-Key Cryptography (PKC) ABE. ABE has potential of enforcing access policies to large scale systems. It means they will execute the task given honestly, but they do have incentive to learn as much as encrypted data they can. Keeping this assumption in mind, [3] allows data owner to delegate user revocation task to Trusted Authority (TA) without even leaking user data information to them.

III. SYSTEM MODEL

The architecture diagram in Fig. 1 shows the proposed model, in which the operations are performed in order to secure and access the data stored in cloud.In this proposed system, when a user loads their data into the cloud storage through admin, the admin initially stores the data in the local server and the data has been sent to fragmentation process. In order to update data appropriately and access it with optimal time fragmentation has been carried out. The fragmented data is wrapped with Improved Attribute-Based Encryption technique which converts the plain text to cipher text, to keep attacker unaware of original data.

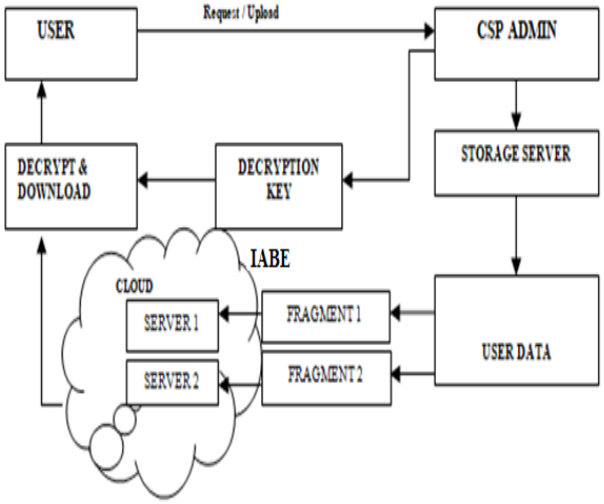

Fig. 1. Proposed System Architecture

The various fragmented cipher text is uploaded into the different storage nodes located in the cloud environment which makes hacker unaware about the location of fragments through which the proposed system improves the security level in cloud storage. The fragmented cipher data is moved to storage nodes in the cloud and is ensured by T coloring method. Once the user gives request to download their uploaded data, admin gathers the fragmented data and it has been converted to original data with the key issued by the admin to the user during the time of downloading data from the cloud storage.

I. IDEAL CONSTRAINTS OF ATTRIBUTE BASED ENCRYPTION

Before applying Attribute Based Encryption (ABE) in real time system some of the security issues need to be addressed.

User Key Revocation:

In real time systems, user may leave the system at some time and hence the scheme can revoke the access rights from system. The user cannot progress further with storage and access of data in the system. In cryptography, user key revocation is one of the main things to be concerned and hence user key revocation in ABE is found one of the challenge issue need to be addressed.

User Accountability:

In data access control technique, decryption key is allowed to access encrypted data only if the user who hold proper key. But the sharing of decryption key to unauthorized user by the authorized user happens at some time which leads to stealing of sensitive information from the semi- trusted storage servers.

Privacy Preservation:

The user discloses their privacy information to un-trusted servers which leads to abuse of attack in storage servers. Thus necessary privacy preservation needs to be constructed in ABE than the existing one.

Efficiency:

Efficiency of ABE is depending on kind of application. Some application expects it by reducing cost of operations like bilinear pairings on encryptor and/or decryptor.

II. IMPROVED ATTRIBUTE BASED ENCRYPTION TECHNIQUE

In cloud computing, deploying of data to a third-party administrative control, gives rise to security and access control concerns. In Cloud Computing Paradigm, building and maintaining specialized data centers for storing and accessing data is quite costly. So the data storage is kept with a third-party cloud service provider who manages this cost. In such scenario, maintaining the privacy of user's data from unauthorized users and denying the access privileges to an unauthorized user is not an easy task and main concern is how user could actually have access control over sharing of data which is reserved on semi-trusted server. Here the need for mechanism in data access control is raised to work efficiently with semi-trusted server. The approach to encrypt the data before it is outsourced to the semi-trusted server should be implemented.

ABE allows access policies to be expressed based on attributes. The Number of attributes involved decides the complexity per encryption, decryption & key generation, and it is linear. However, on demand key revocation, key co-ordination, dynamic access policies, and key management scalability, privacy preservation and efficiency are the important issues which remain open when integrating ABE with large scale application.

To this end, Improved ABE based framework addresses the user key revocation in Attribute Based Encryption. In this proposed technique, key separation technique is adopted in order to provide each user periodically a different private key with a time interval from the central authority, corresponding to their attribute, or else the user will be unable to store or access the data in the cloud environment. The un-trusted storage data servers are neither can be relied upon to enforce data access policies nor allowed to learn contents of sensitive data. So the data owner encrypts the data before outsourcing it on the storage server. This helps to preserve data confidentiality. The user who holds a decryption key is granted to get access to encrypted data.

A. ALGORITHM

The following algorithms are used to provide a solution to user revocation problem. Setup, Encryption, KeyGeneration, ReKeyGeneration, ReEncryption, ReKey, Encryption, Decryption. Trusted Authority is responsible for KeyGeneration & ReKeyGeneration , while ReEncryption, ReKey are done by server. Encryptor and Decryptor call Enc and Dec respectively.

The algorithms are defined as below:

Setup(1λ): It takes *1λ* as input for security parameter and results in the generation of system master key *mk*, public key *pk* as output.

Encryption(M,AS,pk): With the input, message *M* access structure *AS* and public key *pk* the ciphertext *CT is produced*.

KeyGeneration(mk,S): It takes *mk* and set of attribute *S* (key) as input and returns users secret key *SK* in the form of *(S,D,oD= {Di, Fi}iεs)*

ReKeyGeneration(α, mk): The new master key *mk'*, new public key *pk'* and set of proxy rekeys *rk* for all attributes is produced with attribute set *α* and master key *mk* as input.

ReEncryption(CT,rk,β): The input for this process are *CT*, *rk* and a set of attributes *β* which includes all the attributes in cipher text access structure with proxy re-key. It produces output as re-encrypted ciphertext *CT'* with the same access structure as *CT*.

ReKey(oD,rk,θ): It takes input as *oD* of *SK*, *rk* as a set of attributes *θ* which includes all the attributes in *SK* with proxy re-key and results in the updation of user secret key components *oD'*.

Decryption(CT,PK,SK): It takes input as *CT, PK, SK* same version of *CT*. It returns *M* if attribute set of *SK* satisfies the ciphertext access structure.

The algorithm for user key revocation is as follows:

Input: Attribute is chosen as a key

Algorithm:

Step : 1 Set the index value i=0 for an attribute

Step : 2 Check each character in an attribute

Step : 3 Checks whether the character is numeric and float then assign special characters

Step : 4 if the input character is operator then assign numbers from (0-30)

Step :5 Assign symbols to alphabet characters in attribute.

Output: Key for Encryption

The attribute of encrypted data is stored in the cloud storage server. If server searches the user data, the key attribute is compared with encrypted data attribute. The matched files return to the user.

III. IMPLEMENTATION RESULTS

In our experiment, the encryption scheme is implemented in Java language and the output is shown in figure 2, figure 3 and figure 4. In implementation, the files were considered to move to the storage system.

Once the file is uploaded, the user data is taken from Trusted Authority to forward it to fragmentation process. The below Figure shows that the user uploads the file to the admin (Trusted Authority).

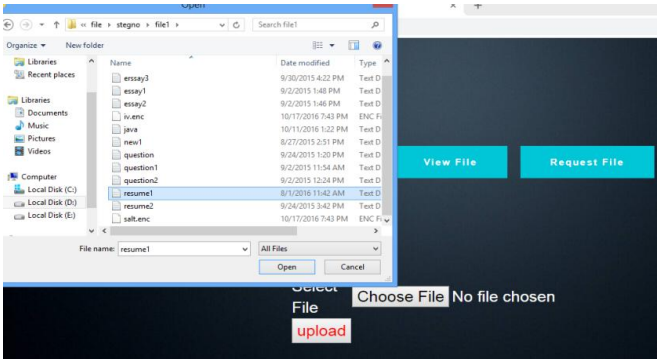

Fig.2 Uploading of File to storage

Once the file has been uploaded the replication of file is taken for fragmenting. This fragmentation process is carried out by admin.

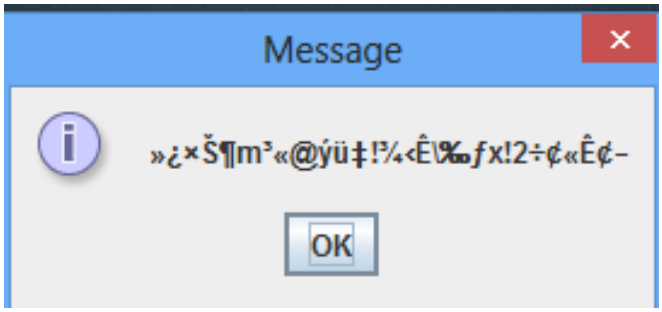

Fig. Encrypted Fragment of file with IABE

When the fragmentation of file is completed it has been wrapped with encryption technique called IABE to convert the plain text to cipher text which cannot be interpreted by the attacker. The above figure shows the Encrypted form of fragmented file with the key generated using IABE. Hence after the encryption process the fragmented files are stored in various storage server of cloud.

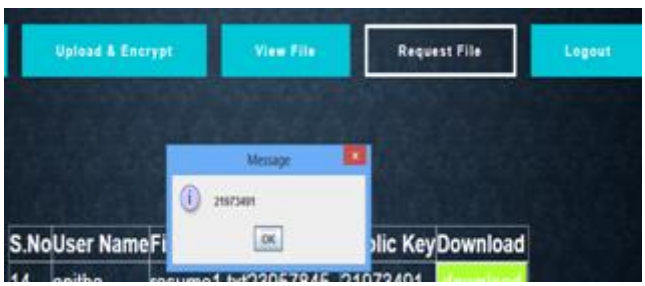

Fig 4. Key Generated to Decrypt before Downloading the File.

When the user passes the request to download their file, the decryption key is generated by the admin and it has been sent to the user to download the file from their site.

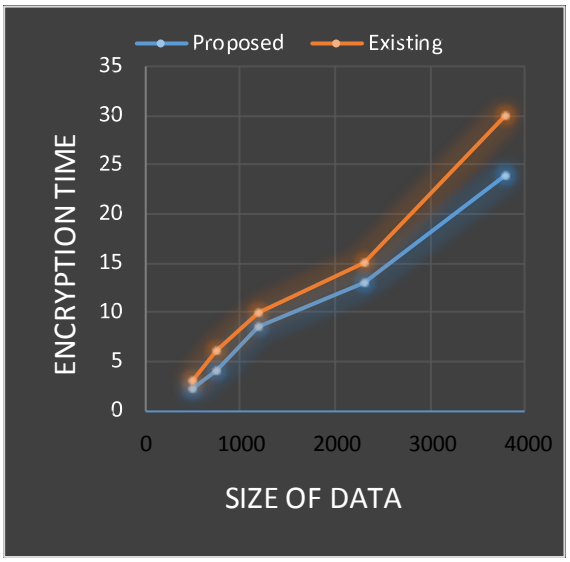

Fig 5. Encryption Time of proposed and existing technique

The above figure shows that the time taken to encrypt the file by the proposed technique is less when compared to existing technique. Since it encrypts all the characters in the attribute which is chosen as key

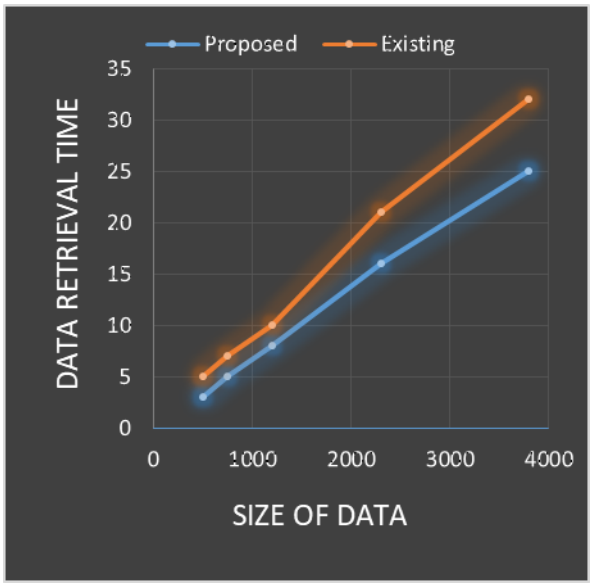

Fig 6. Data Retrieval Time of proposed and existing technique

The proposed system retrieves the file from various location instead from same location. The files are fragmented, encrypted and placed at different location, due to that the time taken to retrieve the file from various location is minimal than existing system.

IV. CONCLUSION

In this paper, the fragmentation and encryption ensures no significant information is leaked and access control method over the cloud storage server is preserved. The proposed systems also ensure that no single node stores more than one fragments of the file and provides data

security and fine access control over the data which is stored in the cloud. The important issue of data access control of user data on cloud storage is addressed with Improved Attribute Based Encryption technique. The other issues in ABE like user accountability and privacy preservation are planned to be addressed in future work.

REFERENCES

1. Mazhar Ali, Samee.U.Khan, Kashif Bilal, Bharadwaj Veeravali,Kequin Li, Albert , "Division and Replication of Data in Cloud for Optimal Performance and Security", IEEE transactions on cloud computing, vol. 6 ,No. 2, 2018.
2. Jin Li, Xiaofeng Chen, Xinyi Huang, Shaohua Tang, Yang Xiang, Mohammad Mehedi Hassan, Abdulhameed Alelaiwi "Secure Distributed Deduplication Systems with Improved Reliability", IEEE Transaction on Computers, Vol. 64, Issue 12, pp. 3569-3579, 2015.
3. Rabia Latif , Haider Abbas, Said Assar and Qasim Ali, "Cloud computing risk assessment:A systematic literature review", IEEE cloud computing risk, vol. 4, 2016.
4. W. A. Jansen, "Cloud hooks: Security and privacy issues in cloudcomputing", IEEE Int. Conf. Syst. Sci., pp. 1–10, 2011
5. Yubo Tan, Xiniel Wang ,"Research of cloud computing data security technology", IEEE International Conference, 2012.
6. A. Juels and A. Opera, "New approaches to security and availability for cloud data," Commun. ACM, vol. 56, no. 2, pp. 64–73, 2013.
7. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer System, vol. 28, no. 3, pp. 583–592, 2012.
8. RanjanaBadre, "Cloud storage with improved access control and assured deletion", International Journal of Innovations in Engineering and Technology, vol. 3 , No. 3, 2014.
9. Meiko Jensen, Jorg Schwenk, Nils Gruschka , Luigi Lo Lacono ,"On technical security issues in cloud computing", IEEE conference on Cloud computing , 2009.
10. P. R. Jaiswal, A. W. Rohankar, " Attribute-Based Encryption: An Efficient Way to Secure Cloud Storage", International Journal of Scientific & Engineering Research, vol. 4, No. 11, 2013.
11. M. Blaze, G. Bleumer, and M. Strauss. "Divertible Protocols and Atomic Proxy Cryptography". In Proc. of EUROCRYPT '98, Espoo, Finland, 1998.
12. ACL. http://en.wikipedia.org/wiki/Access control list
13. H. M. Levy, "Capability-Based Computer Systems", Digital Equipment Corporation 1984. ISBN 0-932376-22-3.
14. NIST. "Role Based Access Control (RBAC) and Role Based Security". http://csrc.nist.gov/groups/SNS/rbac/
15. A. Sahai and B. Waters. "Fuzzy Identity-Based Encryption". In Proc. of EUROCRYPT' 05, Aarhus, enmark, 2005.
16. D. Boneh and M. Franklin. "Identity-Based Encryption from The Weil Pairing". In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.
17. V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data". In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.
18. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. "Over-encryption: Management of Access Control Evolution on Outsourced Data". In Proc. of VLDB'07, Vienna, Austria, 2007.

AUTHORS PROFILE

S.U.Muthunagai is currently working as Assistant Professor in the Department of Computer Science & Engineering at Sri Venkateswara College of Engineering, Sriperumbudur. She received her B.E and M.E from Anna University, Tamilnadu, India. Currently she is pursuing Ph.D in Anna University, Chennai in the domain of cloud computing. Her research area includes Cloud Computing, Big Data Analytics, Wireless Sensor Networks, and Internet of Things. She has published over 6 research papers in various international conferences and journals.

With an experience of 18 years in Teaching & Research, Dr. R. Anitha is currently working at Sri Venkateswara College of Engineering, Sriperumbudur as Professor & Head in the Department of Computer Science & Engineering. Dr. Anitha received her B.E from Bharathidasan University and her M.E and Ph.D in the niche area Cloud Computing from Anna University, Chennai-25. Her primary research interests are in the field of Grid & Cloud Computing, Big Data Analytics. She has published over 35 research papers in various refereed international journals and in the international conferences. As a principal investigator, she is currently involved in one funded project of worth Rs. 21 lakhs from DST-SERB, New Delhi Project titled "DigiCert: Data Security in Federated DigiCloud Environment using Homomorphic Technique". Recently Dr. Anitha has received a funded project from AICTE of worth Rs. 9.73 lakhs. She has also published one patent under IPR, India.