A Review on Circuit hybrid attribute based encryption of data with fragmentation for increasing ideal performance and security in cloud computing

Ahuja Roma[1], Hailkar Kalyani[2], Kale Saurabh[3] Prof A.A.Khatri[4]

[1,2,3]*UG Scholar*, [4]*Assist.* Professor, *Dept. of Computer Engineering, JCOE, Pune (India)*

ABSTRACT

Cloud computing is innovation that uses advanced computational power and improved storage capacities. Cloud computing offer the number of significant advantages. One of the main advantage of cloud computing is pay-as-per-use, which means according to the use of service the customer has to pay. Where the prime disadvantage of cloud computing is achieving security to the data which is store in cloud. The data compromise may occur due to attacks by other users and node within cloud. In this paper, We propose Hd-ABE (Hybrid Attribute Based Encryption) In which data owner should set the access structure of attributes with encrypted data , The user only whose attributes are match with access structure of owner only that user can decrypt the data. To secure data which is store in single node with in cloud we use DROPS (Division and Replication of Data in the cloud for Optimal Performance and Security) methodology, in which we divide the file into fragments, and replicate the fragmented data over the cloud.

Keywords: Cloud computing, Security, Hybrid attribute based encryption, Fragmentation.

I. INTRODUCTION

Cloud computing is computing technique which describes the combination of different data, software which are accessible via internet. Cloud computing is innovation that uses advanced computational power and improved storage capacities. In this cloud computing prime disadvantage is security of data, to provide end-to-end data security and privacy in the cloud, sensitive data has to encrypt before outsourcing to protect data privacy.In cloud computing, effective data utilization is very difficult task because data may hack by other users and node within cloud .As application move to cloud computing platform, A hybrid attribute based encryption in which every cipher text is label with some attribute, location and a time interval while private key is associated with a time instant. The cipher text can only be decrypted if both the time instance is in the allowed time interval and attributes associated with ciphertext satisfy the key's access structure.

Consider the example like health care organizations store data files in the cloud by using CP-ABE and L-ABE under certain access policies. in this system doctor encrypt the data with access structure of attributes and location attribute , the patient who's attributes are match with access structure only that patient can decrypt or download the data , It provide multiple parallel efforts underway to modernize medical record system for greater efficiency , improved patient care, patient safety and cost saving.

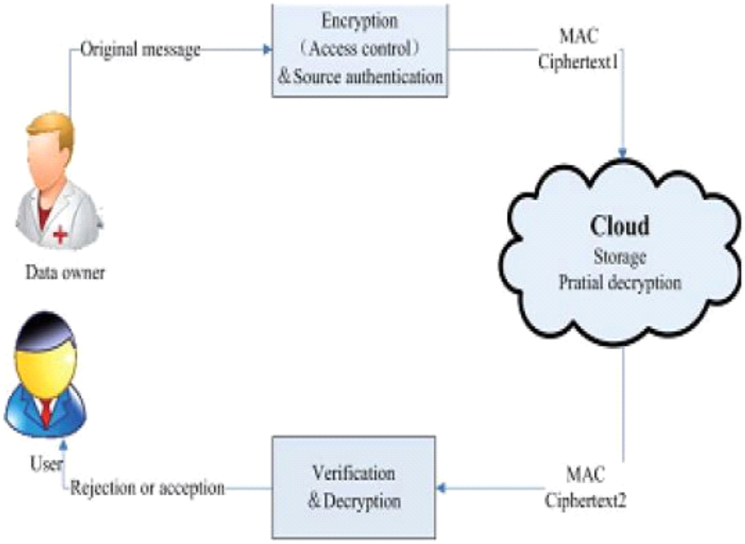

Fig 1. Medical data sharing system

To increase more security in cloud data which is store in single node we can use DROPS (Division and Replication of Data in the cloud for Optimal Performance and Security) methodology, in which we divide the 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. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments.

II. LITERATURE REVIEW

a) Title: Identity Based Cryptosystem and signification schemes.

Authors: Adi Shamir.

Description:

IDE is nothing but Identity based encryption. Original IDE gives by Adi Shamir in [1]1984. In Identity based encryption view the identities as a string of characters. Identity based encryption (IDE), is an important primitive of ID_based cryptography. As such it is a type of public key encryption in which the public key of user is some unique information about the identity of the user for example a user's email address, if owner of data want to send same message or same data to multiple user at a time then it is necessary to select email ID of all users. So it is a time consuming process and not so secure.

b) Title: Fuzzy Identity Based encryption.

Authors: Sahai and Waters.

Description:

Fuzzy identity based was introduced by sahai and waters in 2005. They modify original IDE given by Adi Shamir in [1]1984.In fuzzy identity based encryption view the identities as a set of attribute; It is also called as Attribute Based Encryption. Fuzzy IBE is first paper give the concept of attribute based encryption with public key cryptography. Fuzzy IBE is an attribute type encryption where set of attributes are used to represent an identity. The set of attribute are set by owner when owner wants to send one data to multiple users, the users whose attributes get matched with specified attribute, will only get the access to the data. The disadvantage of Fuzzy IBE is data owner need to use every authorized user's public key.

c) Title: Key-Policy Attribute Based Encryption (KP-ABE).

Authors: Parmar Vipul Kumar
Rajanikanth Aluvalu

Description:

KP-ABE (Key-Policy Attribute Based Encryption)is modified form of classical model of ABE. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. [3, 4] Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications. In a Key-policy attribute based encryption system, Cipher text are branched by the sender with the set of descriptive attributes. The disadvantages of KP-ABE are like Encryptor can not decide who can decrypt the encrypted data, it can only choose descriptive attributes for the data, and has no choice but to trust the key issuers.

d) Title: Cipher text-Policy Attribute Based Encryption An Expressive, Efficiently and provably secure Realization.

Authors: Brent Waters

Description:

CP-ABE is modified form of classical model of ABE, It fulfill some drawbacks of KP-ABE. In CP-ABE encryptor can decide who can decrypt the encrypted data. In CP-ABE, each user is linked with a set of attributes. His secret key is generated based on his attributes. While encrypting a message, the encryptor specifies the threshold access structure for his interested attributes. This message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP-ABE technique, encrypted data can be kept confidential and secure against collusion attacks. The disadvantage is in CP-ABE only static attribute are specified there is no dynamic attribute is used.

e)Title: Designing a Hybrid attribute-Based encryption scheme supporting Dynamic Attribute.

Authors: Stefan G.Weber

Description:

Hybrid attribute based encryption is attributes based, as it allows encryption under logical combination of attributes i.e. properties that users satisfy. It is hybrid; as it combines Ciphertext attribute based encryption (CP-ABE) [5] with location based encryption (LBE) on the level of symmetric key. It handle both static and dynamic attribute like location.The location based encryption is used for security mobile communication by limiting area inside which the recipient can decrypt the message.

f)Title: SECURE DYNAMIC FRAGMENT AND REPLICA ALLOCATION IN CLOUD STORAGE

Authors: P.Anand, R.Bharath, C.Ganapathy, S. Sam Victor.

Description:

In this paper we get information about hoe the data is fragment and store in different nodes in cloud. This is used to increasing security of data which is store in cloud. For achieving this security DROP Methodology is used. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, 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. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments.

III. MOTIVATION

1) Tampering: Tampering of sensitive data by buisness opponent for profit reasons otherwise ranking:- Tampering here means manipulating the data, making changes to the originally stored data .This action is performed by business opponents or hackers for profit reason ,ranking , emotional or mental harassment .

2) Data is stored in single node:-In this the data is stored in cloud, but on a single node. If successful attack takes place on that node the whole data gets hacked.

3) Insecure key management system:-In cloud computing the data is stored in cloud. And the key required to decrypt the ciphertext data is also provided by the cloud. If the key gets hacked by the hacker the entire data gets in control of the hacker.

IV. OBJECTIVE

1) Provide security to data by using a strong data encryption algorithm which is difficult to break.

2) A strong data storage infrastructure for cloud is to be built.

3) To improve the network bandwidth efficiency and usability of cloud data.

4) Propose a new cryptographic primitive called attribute based encryption scheme with outsourcing key issuing and outsourcing decryption, which can implement keyword search function (KSF- OABE).

5) Fragmented data is directed to different nodes.

V. PROPOSED SYSTEM

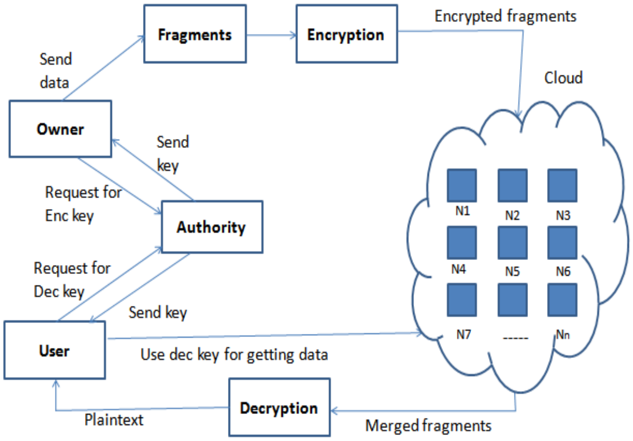

Fig 2. .Proposed system

The proposed system design circuit ciphertext-policy attribute-based encryption with time-specified attributes scheme has been developed. In this scheme, every ciphertext is labeled with some attribute and a time interval while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key’s access structure.

The system contains four modules,

1) Owner
2) User
3) Authority
4) Cloud Server

Owner: Owner is responsible to upload the data in numbers of fragments and assign the attribute to data and create the access structure.

Authority: Authority is responsible to perform authentication of owner and user as well as to send keys, for encryption and decryption to owner and user respectively if they are valid.

User: User is responsible to access or download the data which is given by owner.

Cloud Server: Cloud server is responsible to provide storage space to store the data into different nodes and partially decrypt the data when user wants to access.

V. CONCLUSION

From the above decision and debate we come to a conclusion, that use of circuit hybrid attributes based encryption we will convert a simple plain text data to strong and high level cipher text data with attribute access structure, this will gradually increases the data security and increase the load of unauthorized users from accessing the data. The cost of the computation and communication consumption is low, which open the gates for implementing the system in real. We also conclude that we can also increase the security of data stored in cloud by fragmenting the data and storing it on different nodes this will increase the security of stored data. The use of TPA has made the system more secure to an extent. So overall discussion states that this system can be a great advantage for security in cloud computing.

VI. FUTURE WORK PLANNING

The entire plan to design the system is divided into three phases. The first phase deals with partial front end part which includes the login and registration page for owner and user. It will contain different attributes with fine grained access policy. Our second phase will contain authority i.e. TPA which will make owner and user check and depending on the result , if valid then it will assign the encryption and decryption key to owner and user respectively. Our third phase will be introducing another concept, in which we are going to make fragments of data to be transferred. This fragment will be stored in the cloud individually at different nodes. Rather than storing it as an entire data on single node. This technology will help us in the case of security of stored data. This means even if single node is found. It will very difficult to tack other sibling nodes. This is our total planning. On which we will be working further.

REFERENCE

[1.] Adi Shamir,"Identity Based Cryptosystem and signification schemes"

[2.] A. Sahai and B. Waters, "Fuzzy identity based encryption", Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph. Techn, pp. 457-473, 2005

[3.] N.krishna L.Bhavani "HASBE A Hierarchical Attribute Set Based Encryption For Flexible Scalable And Fine Grained Access Control In Cloud Computing" International Journal of Computer & Organization Trends –Volume 3 Issue 9 – Oct 2013.

[4.] Parmar Vipul Kumar, Rajanikanth Aluvalu" Key-Policy Attribute Based Encryption(KP-ABE)",International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 2, 2015.

[5.] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. 14th Int. Conf. Practice Theory Public Key Cryptograph. Conf. Public Key Cryptograph, 2011.

[6.] Stefan G.Weber," Designing a Hybrid attribute-Based encryption scheme supporting Dynamic Attribute",in Proc. 27th Int. Cryptol.Conf.,2016

[7.] P.Anand, R.Bharath, C.Ganapathy, S. Sam Victor,"SECURE DYNAMIC FRAGMENT AND REPLICA ALLOCATION IN CLOUD STORAGE", International Journal of Computer Informatics & Technological Engineering Volume (3) Issue (3) March 2016