International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Attribute Based Secured Encryption Storage Supporting Data In Cloud

Rakesh Dey[1], Sanjeeva Polepaka[2]
[1]M. Tech Student, Department of CSE, Malla Reddy Engineering College (A), Telangana, India
[2]Associate Professor, Project Guide, Department of CSE, Malla Reddy Engineering College (A) Telangana, India

ABSTRACT

Encryption has been broadly utilized in cloud computing where a data provider or data owner outsources his/her encrypted records to a cloud service company or provider, and might share the records with users owning particular credentials but, the standard encryption machine like ABE machine does no longer assist secure deduplication, that's essential for getting rid of replica copies of equal information with a purpose to save storage area and community bandwidth. In this paper, we present an attribute based encrypted system with deduplication and malware detection in a hybrid cloud, wherein a non-public cloud is liable for replica detection and a public cloud manages the storage and admin is liable for malware detection, generating keys and so forth.

Keywords : Secured Encryption Storage, Encryption, ABE, Cloud Service

I. INTRODUCTION

In current era there are bunches of quickly developing patterns and cloud registering is one of them. Cloud gives simple, proficient stage to store information, secure information, and get to information at any area with the assistance of web. Additionally it gives client adaptable foundations, storage room and execution. Accordingly, how to securely and efficiently share user data is one of the toughest challenges in the scenario of cloud computing.

Therefore cloud service provider must provide the trust and security, as there is valuable and sensitive data in large amount stored on the clouds. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms. In this paper we going to discuss about attribute based encryption scheme and its categories.

II. LITERATURE SURVEY

By assuming the trusted cloud service issuer provides security additionally to the massive quantity of touchy and valuable information saved. ABE algorithms may be used for protecting the confidentiality of the stored statistics and also gives an entry to control mechanism for facts on the cloud. In cloud surroundings, facts confidentiality is important to shield in opposition to insider assault, collision attack and denial of service assault. This phase affords the existing attribute based encryption mechanisms in cloud environment.

Attribute Based Encryption (ABE)

ABE was delivered through Sahai and Waters in 2005. It is a public key based one to many encryptions that allows user to encrypt and decrypt the facts based totally on user attributes. The secret key and cipher textual content are dependent on the consumer attributes. The decryption of cipher text is feasible

best if the set of attributes of person key matches with the attributes of cipher text. Decryption may be done only when the number of matching keys is same to the mentioned threshold degree.

ABE algorithm consists of four steps: setup, key generation, encryption and decryption.

Collision resistance is an essential function of ABE. An opponent that holds more than one key can get right to entry to the data or facts if the key fits.

Drawbacks

For encryption, the data owner or provider has to use every legal user's public key so it will increase the computation overhead. This approach is constrained because it makes use of monotonic attributes to manipulate person's access to the machine or system.

Key Policy Attribute Based Encryption (KP-ABE)

It's far the modified shape of classical version of ABE. Customers are assigned with an entry to access structure over the data attributes. Threshold gates are the nodes of the access tree.

The attributes are associated with leaf nodes. To show the access tree shape the secret or mystery key of the person is defined. Cipher texts are labeled with units of attributes and private keys are associated with monotonic access systems that control which cipher texts a consumer is able to decrypt. Key policy attribute based encryption (kp-abe) scheme is designed for one-to-many communications.

Drawbacks

The trouble with kp-abe scheme is encrypted cannot decide who can decrypt the encrypted information. It may pick out descriptive attributes for the facts; it's far fallacious in some software or apps due to the fact a data owner or provider has to agree with the key issuer.

Cipher Text Policy Attribute Based Encryption (CP-ABE)

Cp-abe is the advanced or changed form of kp-abe. In cp-abe, cipher text is related to a structure and user's personal secret key is based on set of attributes. A consumer is able to decrypt the cipher text most effective if set of attributes associated with users private key satisfies the access policy associated with the cipher text. Cp-abe is more secured even the trusted third party is compromised.

1) A survey based on attribute encryption scheme in cloud computing

Authors: - Minu George, Dr. C. Suresh Gnanadhas, Saranya. K

With the emergence of sharing personal company records on cloud servers, it's far imperative to undertake an efficient encryption gadget with a satisfactory-grained access manipulate to encrypt outsourced records. Attribute based encryption is a public key primarily based encryption that enables access manage over encrypted records the usage of access regulations and ascribed attributes.

2) An evaluation of attribute based totally encryption method for protection in cloud computing

Authors: - Etti Mathur, Manish Sharma

Attribute Based Encryption is an outstanding method to which provides security and privacy in cloud computing surroundings. Data records is encrypted and controlled by the data owner which removes duplicates data in cloud surroundings. In ABE there are many properties for encryption records which generates public key and used to control entry for the user.

3) Implementation of hybrid cloud method for relaxed legal deduplication

Authors: - Jadapalli Nandini, Rami Reddy, Navateja Reddy

The primary issues inside the cloud computing is de-duplication with differential privileges. The main goal of this paper is to remedy this hassle. This paper represents that, many techniques are the use of for the removal of replica copies of repeating, from that

techniques, one of the important data records compression method is data records duplication.

In most of these above noted paper, the authors are discussing approximately encryption & decryption strategies in order that there can be secure uploading of data records from data owner or provider to cloud & from cloud to a valid consumer from where he can retrieve the uploaded data records but one disadvantage is that if the data provider uploads the malware file then it'll harm the cloud & the user or consumer as well, so here the admin plays a major role to offer more security to cloud & person.

III. EXISTING SYSTEM

Within the present system, an attribute based encryption system which employs cipher text-policy characteristic-based encryption (cp-abe) and supports removal of duplications. Their main contributions may be summarized as follows:-

- ✓ First of all, the system is the first that achieves the usual perception of semantic security for confidentiality in attribute-based system by using resorting to the hybrid cloud architecture.
- ✓ Secondly, a technique is used to regulate a cipher textual content over one accessing policy into cipher text of the same plaintext however under every other get entry to guidelines without revealing the underlying plaintext. This approach is probably of independent interest further to use it in the future proposed system.

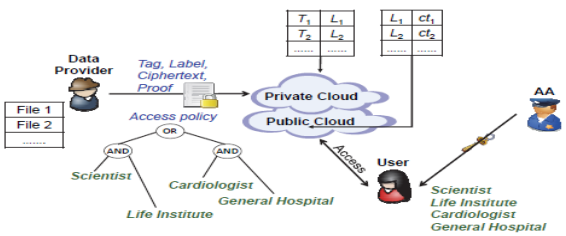

Fig. (1) Current System of Attribute Based Secured Encryption Storage Supporting Data in Cloud

Disadvantages

The prevailing system concerns at the removing of duplications of the information with ABE but not at the content of the file(i.e. malware or not).

IV. PROPOSED SYSTEM

The proposed system has the function of saving area for cloud storage services with at ease deduplication along with malware detection. But this mission flow a few distinct modules in there. In this example, if two users add the identical file, the cloud server can figure the identical cipher textual content and store only one replica of them. An owner wants to outsource to the cloud and share it with users owning some credentials. The admin gives each consumer a decryption key associated with users set of attributes that's taken into consideration to be the maximum critical mission for efficient and comfortable cloud storage saving services inside the environment in which an ownership dynamically changes and additionally by checking the malware.

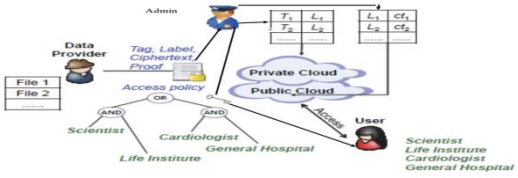

Fig. (2) Proposed System of Attribute Based Secured Encryption Storage Supporting data in Cloud

ALGORITHMS

RSA Algorithm

RSA is an algorithm having a set of rules used by modern systems to encrypt and decrypt messages. It's an asymmetric cryptographic set of rules. This is additionally referred to as public key cryptography having two different keys; due to the fact certainly one of them can be given to anybody. The alternative

key ought to be private. It is primarily based on the truth that the factors of an integer are tough to find (the factoring problem). RSA stands for RonRivest, Adi Shamir and Leonard Adleman, who first publicly defined it in 1978. A consumer of RSA creates and then publishes the made from two prime numbers, at an auxiliary cost, as their public key. The factors need to be saved secret. Each person can use the public key to encrypt a message, however with presently published techniques, if the general public key's is sufficient, and if a person who is expertise in prime factor elements can feasibly decode the message.

I) ENCRYPTION ALGORITM

Encryption permits data to be hidden so that it can't be read without some properknowledge (example password). This is executed with a secret code or cypher. The hidden data is stated to be encrypted.

II) DECRYPTION ALGORITHM

Decryption is a way to exchange encrypted statistics text into plaintext. The examination of encryption is called cryptography. Cryptanalysis may be performed through hand if the cypher is straightforward. Complicated cyphers want a computer to search for feasible keys. Decryption is an area of computer technology and mathematics that looks at how difficult it is to break a cypher.

III) MALWARE DETECTION ALGORITHM

Malware detection can be accomplished on based totally on feature

$$f(x,F)\in x$$

in which x is the set of allowable file codes and F is the report to be stored.

IV) DEDUPLICATION

We deal with the trouble of keeping data private as well as checking deduplication in cloud computing and advise a new deduplication system helping for the proposed model.

- **Differential authorization:** to perform replica test based on privilege of consumer is capable of get his/her token. Without aid from the personal cloud server and for the duplication look at the tokens, cannot be generated by the consumer.
- **Legal duplication test:** legal user is capable of use his/her personal keys to generate question for positive file and the privileges he/she owned with the assist of private cloud, whereas the general public cloud performs replica test immediately and tells the consumer if there is any reproduction. The safety necessities considered in this paper lays here, which include the safety of record token and protection of documents. For the security of file token, factors are defined as un-forge capability/ imitating and in-distinguish ability of report token/ check replica token.
- **Imitating of record token:** unauthorized customers without suitable privileges or report ought to be avoided from getting or producing the report tokens for duplicate take a look at of any document stored on the s-csp.
- **Replica-check token:** it requires that any user without querying the non-public cloud server for a few record token, he can't get any useful data or facts from the token, which have the file facts or the privilege records.

In this assignment, we use set of rules,

For uploading a file

Start

Step –1 read file

Step –2 cloud server assessments for duplication

Step –3 sends duplication response whether or not the report already exists or not

Step – 4 if the document does not exist

4.1 show “report does no longer exist”

Step – 5 then it uploads the report

Step – 6 if the file exists already **Stop**

6.1 displays “record already exists”

Experimental Results

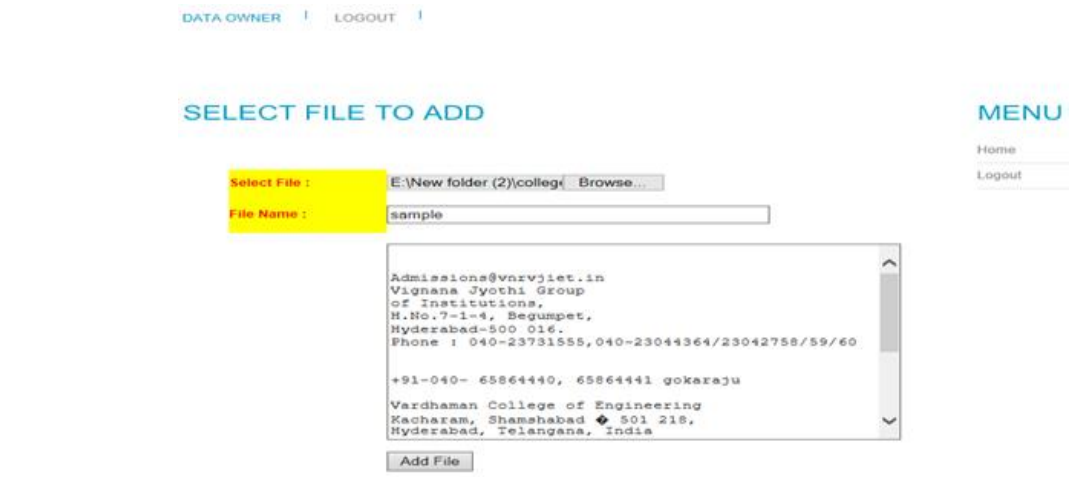

Figure 3. Data Owner Uploading Files

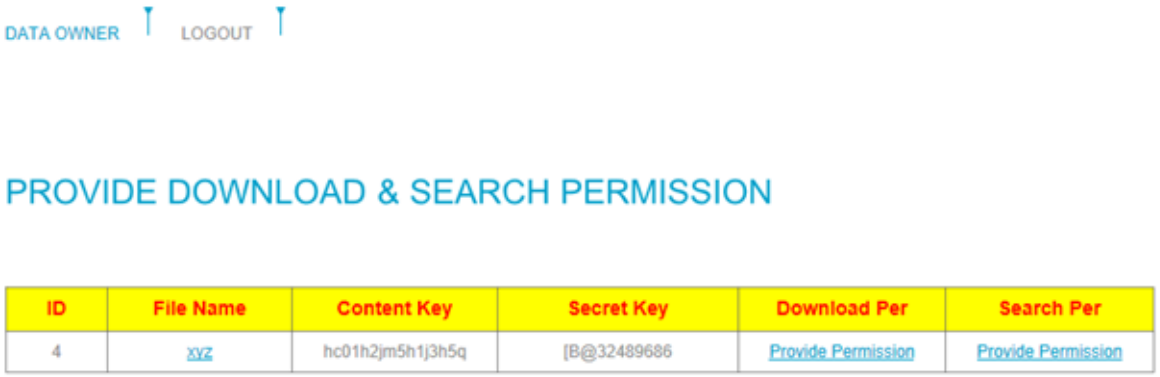

Figure 4. Data Owner providing permissions

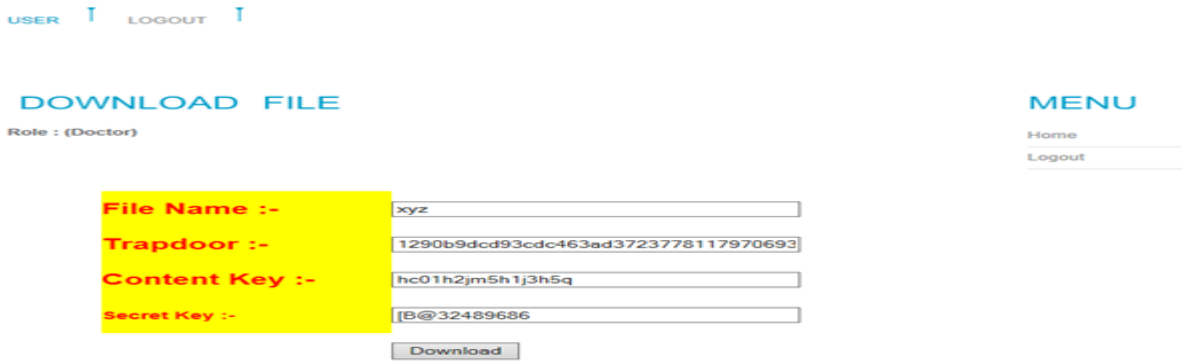

Figure 5. Data User downloading files

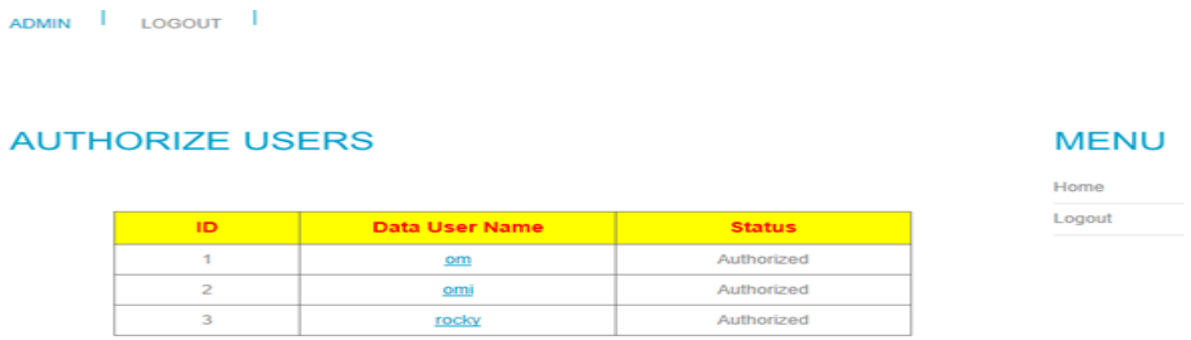

Figure 6. a. Admin Authorizing Data Users

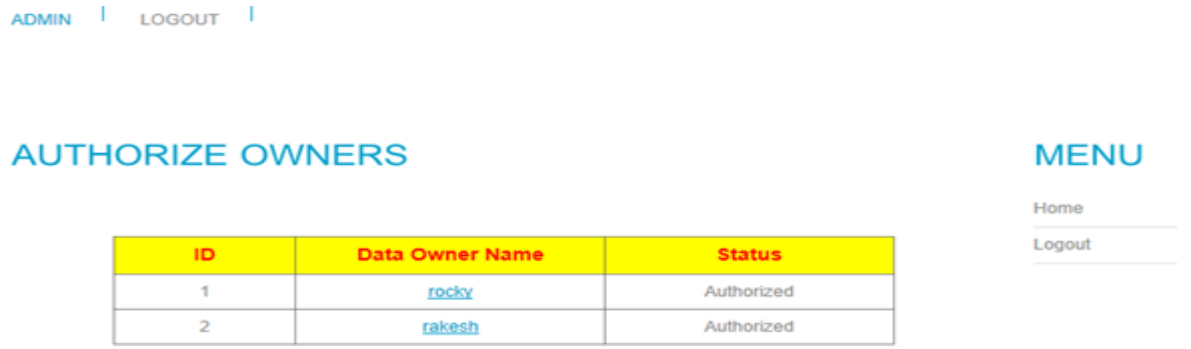

Figure 6.b. Admin Authorizing Data Owners

Figure 7. Cloud Viewing Files

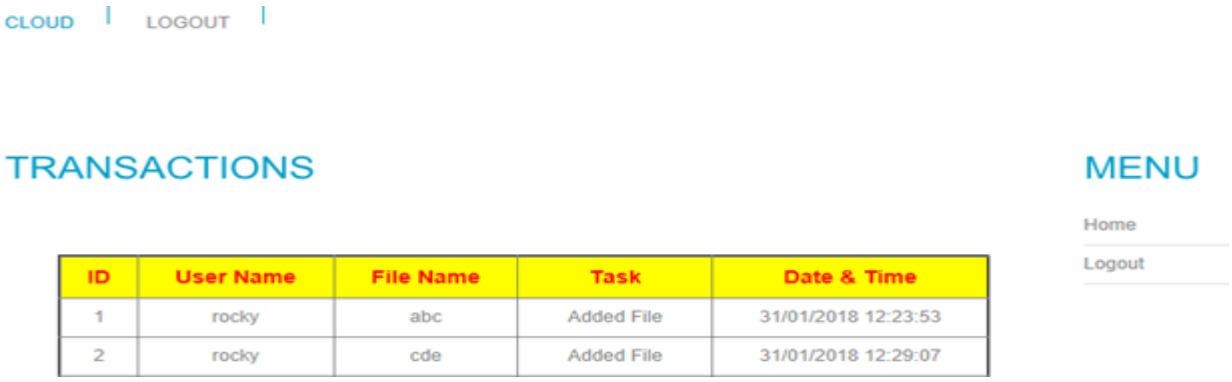

Figure 8. Cloud Having Transaction Lists

V. CONCLUSION

Attribute-Based Encryption (ABE) has been extensively used in cloud computing in which a data provider outsources his/her encrypted records to a cloud service issuer, and can proportion the facts with users owning particular credentials (or attributes). In this paper, we gift an attribute-based storage system with comfortable secured deduplication in a hybrid cloud placing together with malware detection, wherein a private cloud is responsible for replica detection and a public cloud manages the storage & admin exams for legal key & also for malware detection.

VI. REFERENCES

[1]. V. Goyal, O. Pandey, A. Sahai, and B.Waters"Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89{98, 2006}

[2]. Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.

[3]. Muller, S. Katzenbeisser, and C.Eckert, "Distributed attribute-based encryption," in Proceedings of ICISC, pp. 20{36, 2008.}

[4]. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. "Secure attribute-based systems". In Proceedings of the 13th ACM conference on Computer and communications security, pages 99{112. ACM Press New York, NY, USA, 2006.

[5]. Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran,"AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009

[6]. R. Ostrovsky and B. Waters. "Attribute based encryption with non-monotonic access structures". In Proceedings of the 14th ACM conference on Computer and communications security, pages 195{203. ACM New York, NY, USA,2007.

[7]. A. Sahai and B. Waters, "Fuzzy identity-based encryption,"In Proc.EUROCRYPT, 2005, pp. 457473

[8]. G. Wang, Q. Liu, and J.Wu,"Hierachical attibute- based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security