ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, october 2015

Suburbanized Access Control with Unsinged Affirmation of Data Stored In Cloud

Raghvendra V.Kulakarani [1], Prof. Sachin Chavan [2]

PG Scholar, Department of Computer Engineering, MGM's College of Engineering & Technology, Kamothe, Navi Mumbai,India

Assistant Professor, Department of Computer Engineering, MGM's College of Engineering & Technology, Kamothe, Navi Mumbai,India

ABSTRACT: Cloud computing is one of the fast growing area in the computer field. The cloud must be secure because it may have sensitive data. There are some traditional techniques available but these are not sufficient. To enhance the security of the cloud we are proposing this scheme. In this proposed system the data i.e. cloud is decentralized and can support the unsigned affirmation of data stored in cloud. In this cloud does not need to authenticate the user before storing the data but to decrypt the data one should authenticate by cloud. This scheme provides protection from reply attacks and may allow creating, modifying and reading the data from cloud. Although access control and authentication is decentralized, the communication and storage is likely be centralized.

KEYWORDS: Cloud; Access control; Affirmation; suburbanized; attribute based encryption.

I. INTRODUCTION

Initially clouds were used to store the data only and considered as replacement for the storage devices hard disks, DVD,CD). But the researchers proved that it's not only for the storage but we can do much more with the cloud. by using the cloud one can deploy computation and storage by using internet. Cloud also provides many types of services (eg. Google Apps)

At most of the times the data stored in cloud is hyper sensitive for example health care records, business documents, personal records, student's record. As its sensitive data there should be a strong security otherwise one can hack the data and can be misused. One aspect is that the user must be authenticate before accessing the data on cloud and another aspect is that cloud should be trusted means cloud does not damage the data. User privacy is also important here, other user do not know the identity of the user.

The main purpose of the proposed system is to provide security to the cloud [1]. There are three types to access the cloud one is user based access. In this only users can access the cloud. Another type is role based access. In this type specific roles means specific users with assigned roles can access the cloud. And the last is attribute based access in which valid set of attributes decides the access control policy.

II. RELATED WORK

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters[2] introduces the concept of attribute based encryption for fine grained access control of encrypted data in 2006. This cryptosystem is known as Key-Policy Attribute based Encryption. In this system encrypted texts are labelled with set of attributes and private keys that decides which user is able to decrypt the data. Sabrina De cappitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati [7] explained combination of access control and cryptography in 2010. It describes the concept for enforcing authorization policies and supporiting dynamic authorizations, permitting policy changes at a limited cost in terms of bandwidth and computational power. Junbeom Hur, Dong Kun Noh [6] introduces the concept of Attribute based access control with efficient revocation in data outsourcing system in 2012. He also introduces the cipher text policy attribute based encryption. Also added two functions one for generation of keys to encrypt attributes and another is for re-encryption that performs re-encryption on cipher text. R. Ranjith, D.Kayathri Devi [3] explained the concept of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, october 2015

secure cloud storage using decentralized access control with anonymous authentication in 2013. He used policy based file access using attribute based encryption (ABE) with RSA key public private key combination. Markulf kohlweiss, ueli Maurer, cristinaOnete, Bjorn Tackmann, Daniele Venturi[4] introduced anonymity Preserving public keys Encryption: A constructive Approach where public key cryptosystem with enchanced security properties have been proposed. It investigates constructions as well as limitations for preserving receiver anonymity when using public key encryption. S Divy Bharathy and T Ramesh[5] introduced the concept of privacy preserving access control scheme for data storage, which supports anonymous authentication and perform decentralized key management in Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control in April 2014. In this scheme, the cloud allows an access control policy and attributes hiding strategy to enhance security. This provides secure and efficient dynamic operation on data blocks, and performs data update, creation, modification and reading data stored in the cloud. Sushmita Ruj, Milos Stojmenovic, Amiya Nayak introduces Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds in 2014. Its a new decentralized access control system for secure data storage in clouds that allows anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the feature of access control in which only valid users are able to decrypt the stored information.

III. PROPOSED SYSTEM

A. *Assumptions:*

- The cloud is trusted i.e. cloud doesn't damage the data.
- User can read or write or read and write the data.
- All communications are secured.

B. *System Design:*

In the proposed system there are following keys used

- Public Key: It's a random generated key. It's binary in nature & maintained by key manager. It's used for encryption or decryption.
- Private Key: It's the combination of user credentials (User name, password, security Question). It is also used for encryption and decryption.
- Access Key: This key is based on the policy. Private access key is maintained by the user. Access key generated on attributed based encryption.

C. Description of proposed system:

According to proposed system user can create and store a file in the cloud. This scheme uses the ABE protocol and RSA algorithm. Let discuss the scheme in detail. Fig 1 shows the actual working mechanism. In figure there are 3 users U1, U2, U3. Each user having different likes roles creator, reader, writer. Creator can create the file on cloud while reader can only read the file but can't modify the file. Writer can write and modify the file. There are KDC's which are located in the different part of the worlds. There may be several KDC's. A trustee is a someone who manages the records of the users such as unique id. On presenting this unique id to the trustee he will provide some token to the user. By using this token a KDC generates the keys which will be used to encrypt/decrypt the file. KDC generates public key and private key to the users. For encrypt the data one can use the public key but to decrypt one must have the private key. The access key is one which allows accessing the cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, october 2015

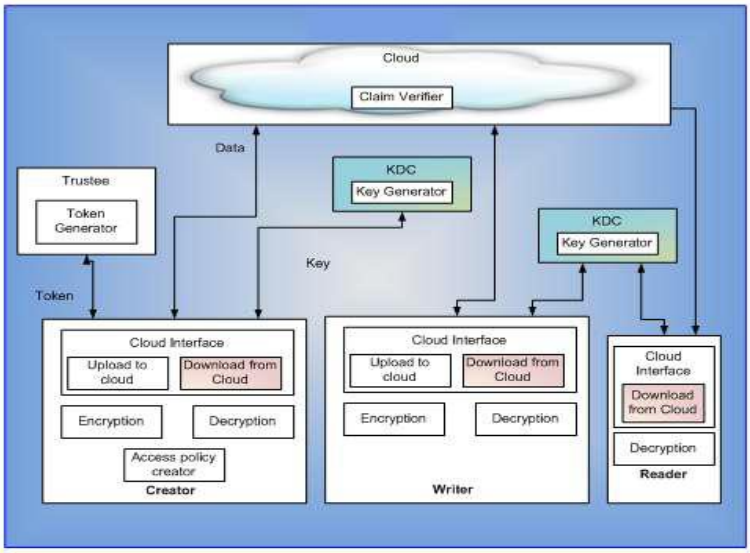

Figure 1: System Modules

- *File Upload :*

To upload a file initially user requests to the key manager for the public key. This key will be generated according to the policy associated with the file. For the different polices public key may differ and vice versa. Then user generates the private key by using user credentials. After that file is encrypted with the help of public and private key.

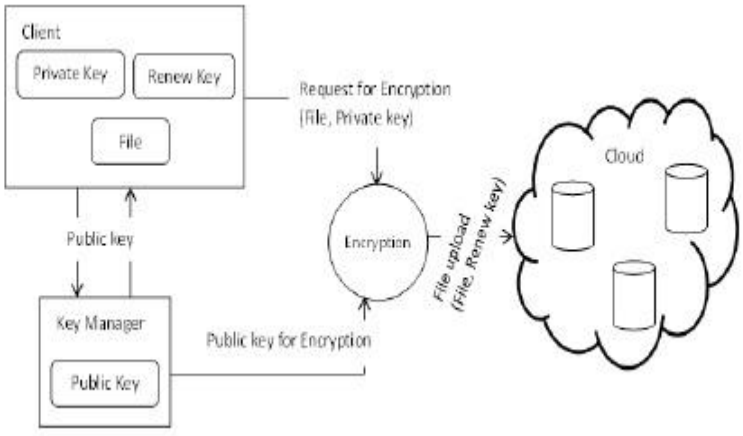

Figure 2: File uploading

- *File Download :*

One can download the file from the cloud after the authentication process. User requests the public key to the key manager as public key is maintained by the key manager. The authenticated users can get the public key. Then one can decrypt the file using public key and private key. During the downloading cloud authenticates the user but the cloud doest have any attribute or details of the users.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, october 2015

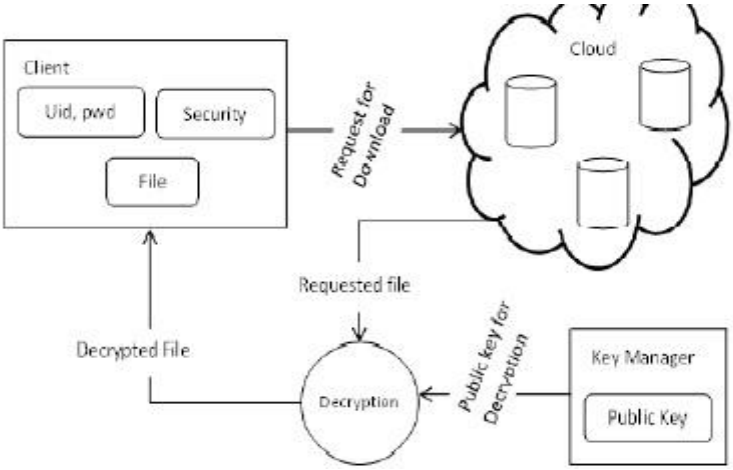

Figure 3: File download

IV. RESULTS

Cloud is the virtual storage where user can store the data or information. This data may be sensitive so user must ensure about the security of the cloud. For this user must sure that only authorized users can access the data. Security of data and privacy of the users must be preserved by the cloud. User may permit access to another user by granting access permission according to the choice. Result analysis can be done according to the authentication scheme, access permission and decentralized environment.

Scheme	Authentication
Attribute based Data sharing with Attribute revocation	No Authentication
Decentralizing Attribute based encryption	No Authentication
Securing Personal health records in cloud computing	No Authentication
Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems	Authentication
Proposed scheme	Authentication

Table 1: Comparison between different systems

Users	Read	Read / Write
Velansiya	05	07
Shreeyash	15	03
Snehal	00	23
Dhanashree	09	21

Table 2: Comparison between granting the access i.e. read or read/write

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, october 2015

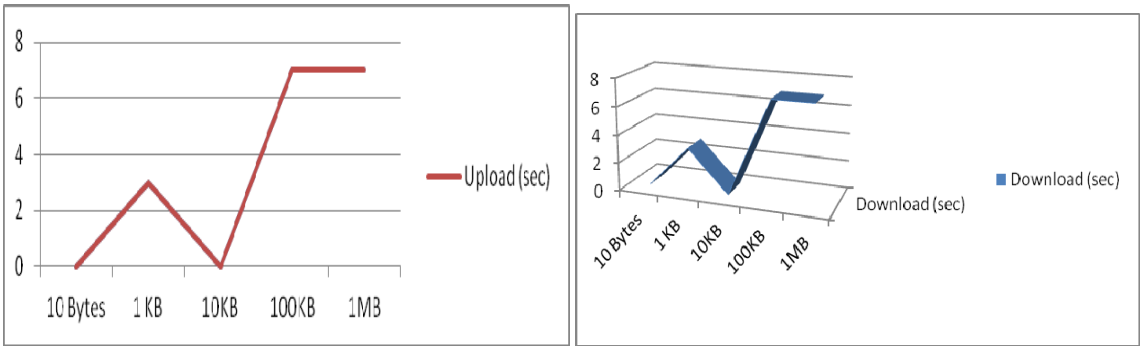

Figure 4: Graph showing time required time for the uploading and downloading the file on cloud

V. CONCLUSION AND FUTURE WORK

We have presented Suburbanized Access Control with Unsinged Affirmation of Data Stored in Cloud, which provides user revocation and prevents reply attacks. More security is assured while uploading and downloading the file to the cloud s it uses the standard Encryption / Decryption techniques. The cloud does not know the identity of the user but verifies the user credentials. Key distribution is in decentralized way. The cloud knows the access polices this can be a limitation in future work can be done to hide attributes and access policies of the users.

REFERENCES

1. S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc.IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556- 563, 2012
2. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
3. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.
4. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.
5. G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.
6. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008
7. Pooja R. Vyawhare et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2441-2447
8. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.
9. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010

BIOGRAPHY

Raghvendra V. Kulakarani is pursing Master of Engineering in Computer Engineering from MGM's College of Engineering & Technology, Kamothe, Navi Mumbai, India. He received Bachelor of Engineering in Information & Technology degree in 2013 from Sant Gadage Baba Amravati University, Amravati, MS, India. His research interests are computer networks, cloud computing etc.

Sachin Chavan is Assistant Professor in the computer Engineering Department, MGM's college of engineering & Technology, Mumbai University. He receives Master of Engineering (ME) in 2010 from Mumbai University,Mumbai, MS, India. His research interests are computer networks, Data Mining, Web mining etc.