SECURED WAY TO MANAGE VARIOUS ATTACKS IN CLOUD

[1] J.K. Periasamy, [2] Deepa.M, [3] Manibharathi.R, [4] Hemavathi.M

[1]Associate Professor, Department of CSE, Sri SaiRam Engineering College, Chennai. [2,3,4] Department of CSE, Sri SaiRam Engineering College, Chennai.

ABSTRACT

Cipher text-Policy Attribute-Based Encryption (CPABE) may be an effective solution to guarantee the confidentiality of data and provide fine-grained access control here. In a CP-ABE based cloud storage system, for example, organizations (e.g., a university such as the University of Texas at San Antonio) and individuals (e.g., students, faculty members and visiting scholars of the university) can first specify access policy over attributes of a potential cloud user. Authorized cloud users then are granted access credentials (i.e., decryption keys) corresponding to their attribute sets (e.g., student role, faculty member role, or visitor role), which can be used to obtain access to the outsourced data. As a robust one-to-many encryption mechanism, CP-ABE offers a reliable method to protect data stored in cloud, but also enables fine-grained access control over the data.

INTRODUCTION

Data owners will store their data in public cloud along with encryption and particular set of attributes to access control on the cloud data. While uploading the data into public cloud they will assign some attribute set to their data. If any authorized cloud user wants to download their data they should enter that particular attribute set to perform further actions on data owner's data. A cloud user wants to register their details under cloud organization to access the data owner's data. Users want to submit their details as attributes along with their designation. Based on the user details Semi-Trusted Authority generates decryption keys to get control on owner's data. An user can perform a lot of operations over the cloud data. If the user wants to read the cloud data he needs to be entering some read related attributes, and if he wants to write the data he needs to be entering write related attributes. Foe each and every action user in an organization would be verified with their unique attribute set. These attributes would be shared by the admins to the authorized users in cloud organization. These attributes will be stored in the policy files in a cloud. If any user leaks their unique decryption key to the any malicious user data owners wants to trace by sending audit request to auditor and auditor will process the data owners request and concludes that who is the guilty.

SCOPE OF THE PROJECT

The scope of our project is to prevent security breach from outside attackers as well as inside attackers. Here we use CP-ABE, which is suitable for data access control in cloud storage systems, because it gives the data owners a direct control on access policies. This is the first CP-ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Data owners are not involved in the key generation.

EXISTING SYSTEM

In existing system the CP-ABE may help us prevent security breach from outside attackers. But when an insider of the organization is suspected to commit the "crimes" related to the redistribution of decryption rights and the circulation of user information in plain format for illicit financial gains, how could we conclusively determine that the insider is guilty? Is it also possible for us to revoke the compromised access privileges? In addition to the above questions, we have one more which is related to key generation authority. A cloud user's access credential (i.e., decryption key) is usually issued by a semi-trusted authority based on the attributes the user possesses. How could we guarantee that this particular authority will not (re)distribute the generated access credentials to others.

DISADVANTAGE

- Security breach is prevented only from outside attackers.

- Data owners act as a fully trusted central authority.

PROPOSED SYSTEM

In this work, we have addressed the challenge of credential leakage in CPABE based cloud storage system by designing an accountable authority and revocable Crypt Cloud which supports white-box traceability and auditing (referred to as Crypt Cloud+). This is the first CP-ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, Crypt Cloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority.

ADVANTAGE

- Supports White box traceability and auditing.

- Prevents security breach from outside as well as inside attackers.

CP-ABE PROVIDES

- Backward Security : The revoked user cannot decrypt the new cipher texts that require the revoked attributes to decrypt.

- Forward Security :The newly joined user can also decrypt the previously published cipher texts that are encrypted if it has sufficient attributes.

FRAME WORK OF OUR SYSTEM:

List of Modules:

- Organization profile creation & Key Generation
- Data Owners File Upload
- File Permission &amp; Policy File Creation
- Tracing who is guilty

1.Organization profile creation & Key Generation

User has an initial level Registration Process at the web end. The users provide their own personal information for this process. The server in turn stores the information in its database. Now the Accountable STA (semi-trusted Authority) generates decryption keys to the users based on their Attributes Set (e.g. name, mail-id, contact number etc..,). User gets the provenance to access the Organization data after getting decryption keys from Accountable STA.

2.Data Owners File Upload

In this module data owners create their accounts under the public cloud and upload their data into public cloud. While uploading the files into public cloud data owners will encrypt their data using RSA Encryption algorithm and generates public key and secret key. And also generates one unique file access permission key for the users under the organization to access their data.

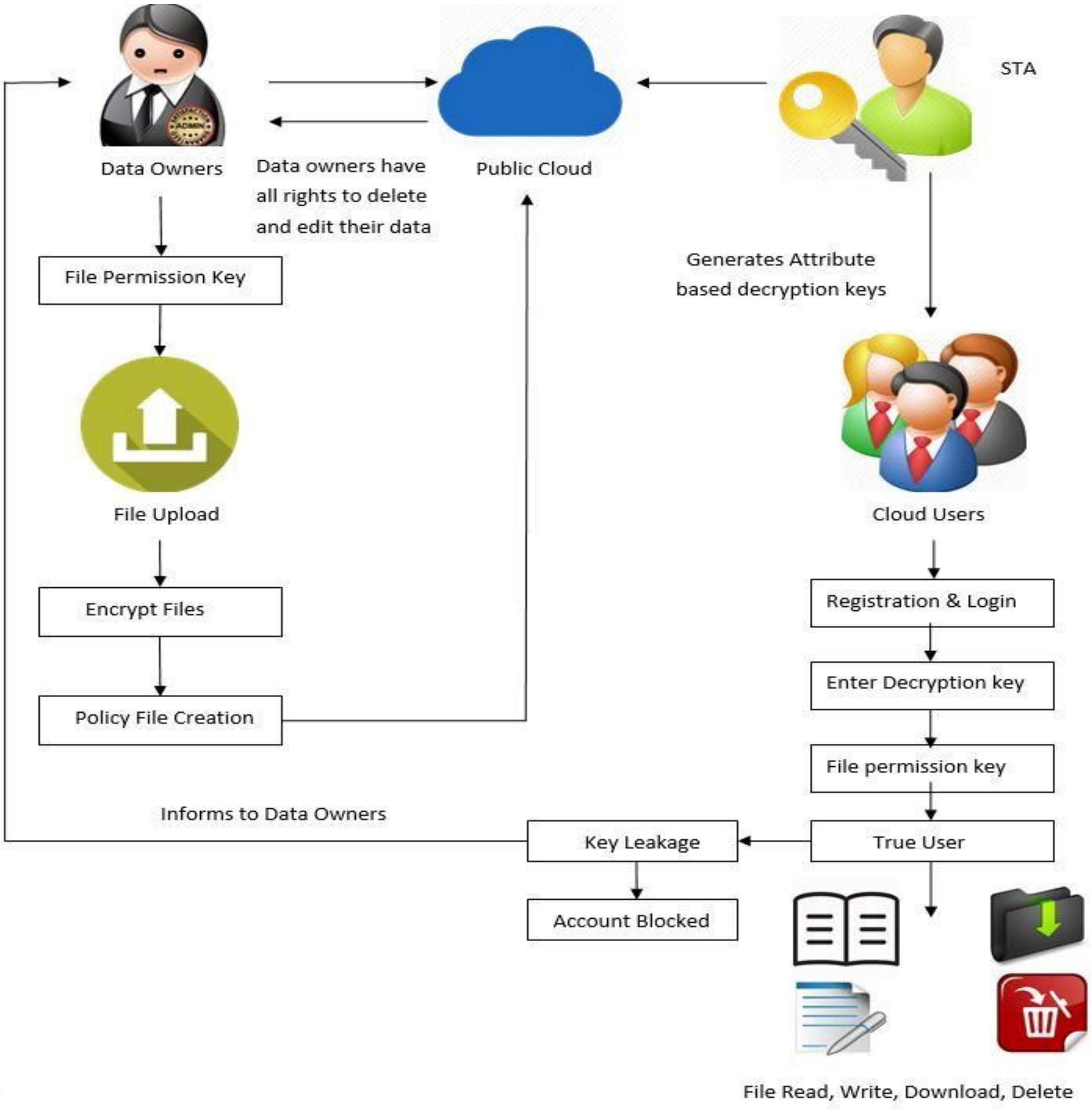
3.File Permission & Policy File Creation

Different data owners will generate different file permission keys to their files and issues those keys to users under the organization to access their files. And also generates policy files to their data that who can access their data. Policy File will split the key for read the file, write the file, download the file and delete the file.

4.Tracing who is guilty

Authorized DUs are able to access (e.g. read, write, download, delete and decrypt) the outsourced data. Here file permission keys are issued to the employees in the organization based on their experience and position. Senior Employees have all the permission to access the files (read, write, delete, & download). Fresher's only having the permission to read the files. Some Employees have the permission to read and write.

ARCHITECTURE DIAGARAM



|

CP-ABE PROVIDES

- Backward Security : The revoked user cannot decrypt the new cipher texts that require the revoked attributes to decrypt.
- Forward Security :The newly joined user can also decrypt the previously published cipher texts that are encrypted if it has sufficient attributes.

ALGORITHMS USED:

- KEY GENERATION →DIFFIE HELLMAN KEY EXCHANGE ALGORITHM
- FILE POLICY SELECTION ALGORITHM →HMAC ALGORITHM
- ENCRYPTION ALGORITHM→RSA ALGORITHM

SYSTEM REQUIREMENTS

Software Requirements

- Windows 7 and above
- JDK 1.7
- J2EE
- Tomcat 7.0
- MySQL

Hardware Requirements

▶ Hard Disk	:	80GB and Above
▶ RAM	:	4GB and Above
▶ Processor	:	P IV and Above

CONCLUSION

Thus , the proposed scheme achieves the security properties of forward security and backward security and can also withstand key exposure. Here, we have addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable Crypt Cloud which supports white-box traceability and auditing .

REFERENCES

- D. He, S. Zeadally, N. Kumar, and J.-H. Lee, “Anonymous authentication for wireless body area networks with provable security,” *IEEE Syst. J.*, 2016, doi:10.1109/JSYST.2016.2544805.

- Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records FUFU DENG1 , YALI WANG1 , LI PENG 1 , HU XIONG 1,2, JI GENG1 , AND ZHIGUANG QIN1 , [Member, IEEE].

- JIN LI, QIONG HUANG, XIAOFENG CHEN, SHERMAN SM CHOW, DUNCAN S WONG, DONGQING XIE – “ Multi-authority ciphertext-policy attribute-based encryption with accountability” - ACM, 2011.

- J. HONG, K. XUE, AND W. LI, “Security analysis of attribute revocation in multiauthority data access control for cloud storage systems,” IEEE Trans. Inf. Forens. Security, vol. 10, no. 6, pp. 1315–1317, Jun. 2015.
- J. CHEN AND H. MA, “Efficient decentralized attribute-based access control for cloud storage with user revocation,” in Proc. 2014 IEEE Int. Conf. Commun., 2014, pp. 3782–3787. [14]
- K.Yang and X. Jia, “Expressive, efficient, and revocable data access control for multi-authority cloud storage,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, Jul. 2014.
- Rahul Reddy Nadikattu, "FUNDAMENTAL APPLICATIONS OF MACHINE LEARNING ACROSS THE GLOBE", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.31-40, January 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133453.pdf
- R.R. Nadikattu. 2017. ARTIFICIAL INTELLIGENCE IN CARDIAC MANAGEMENT. International Journal of Creative Research Thoughts, Volume 5, Issue 3, 930-938.
- Sikender Mohsienuddin Mohammad, "DEVOPS AUTOMATION AND AGILE METHODOLOGY ", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 3, pp.946-949, August-2017, Available at :http://www.ijcrt.org/papers/IJCRT1133441.pdf
- Sikender Mohsienuddin Mohammad, "IMPROVE SOFTWARE QUALITY THROUGH PRACTICING DEVOPS AUTOMATION", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 1, pp.251-256, March 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133482.pdf