International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

ATTRIBUTE BASED DATA MANAGEMENT IN CRYPT CLOUD

I.Veni[1], H.Rupini[2], G.Vidhya[3] – Guided By D.Jayakumar[4]

[1,2,3]Student(B.E), CSE Department, R.M.D Engineering College, Kavaraipettai, Chennai-601 206, Tamil Nadu, India

---

ABSTRACT -*The main aim of this project is to provide integrity of an organization data which is in public cloud. The data will be stored inside the public cloud along with encryption and particular set of attributes to access control on the cloud data. The secure cloud storage is an emerging cloud service that is used to protect the confidentiality. Thus 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. whenever a detail to be uploaded in the cloud, is used to access the data owners data. Users must 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. This produces flexible data access for cloud users whose data is out of physical control. Cipher text Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques that may be leveraged to secure the guarantee of the service. 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. For each and every action of the user, it will be verified by the 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*.

Keywords: *traceability, ciphertext policy attribute based encryption.*

1. Introduction

The cloud computing may involve in the vulnerability to confidentiality of the data and the privacy of the cloud users. Here is the challenge only on the authorized users can access the data which is outsourced to the cloud. There is a solution to this is we need to encrypt the data prior while uploading to the cloud thus limits to the further processing and sharing. This is because first we need to download the encrypted data and then if so we don't' have any local copies of the data we need re-encrypt the data which desirable in the context of the cloud computing. Thus Ciphertext policy attribute based encryption is the solution that is users to provide the confidentiality of data and flexibility of data. Authorised cloud users are granted access credentials corresponding to their attribute sets which can be used to obtain the outsourced data. This CP-ABE is used to protect the data in the cloud and enables the access control over the data that is uploaded. Generally in an existing CP-ABE system it fails to consider whether if there is misusing of credentials or not. Thus to solve this we ensure some decryption policies to be involved hence only the attributes which satisfies the decryption policy of the credential can only be able to access the data that is stored in public cloud. So the leakage of the sensitivity content in the cloud could result in the range of the consequences of the cloud. Thus this CP-ABE can help us to prevent the security breach from the 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 student information in plain format for illicit financial gains, how could we conclusively determine that the insider. 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. To overcome this credential misuse, we propose Crypt Cloud+, an accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing. This is the solution to secure fine-grained access control over encrypted data in cloud .If the decryption is leaked to any malicious user data owners trace by sending audit request to auditor and auditor will process the data owners request and concludes that who is guilty.

2. LITERATURE REVIEW

Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data model: They built a whole new crypto-system during this research for the fine-grained exchange of cryptographic data which is often referred to as Key- Policy Attribute-Based Encryption (KP-ABE)[10]. In this cipher-texts, sets of attributes are labelled , and private keys are related to access structures that control which cipher-texts a user can decrypt to. Private user keys may house a group member in the corresponding access tree for each leaf in the key. They also developed new techniques for applying control of fine grained exposure. The information is processed on the server in an encrypted manner of their strategies, though various users are also allowed to decrypt specific pieces of information under the protection policies. . They noticed that previous CP-ABE schemes may either help only very restricted access mechanisms or only provide a protection signal inside the default community model (rather than accepted theoretical expectation of variety).A user will be able to decrypt if and as long as his attributes

satisfy the cipher text's policy. A user would log into the server then the server would decide what data the user is permitted to access. That improves health. Their design may help access structures that were described as their nodes by a restricted size access tree with threshold gates. The disadvantages faced during this research were that the Ciphertext Policy Attribute Dependent Encryption (CPABE)of this scheme was either able to endorse only very restricted access systems, or had protection evidence only within the default community model. Managing a dynamic access control strategy utilizing conventional, theoretically complicated, public key encryption schemes.

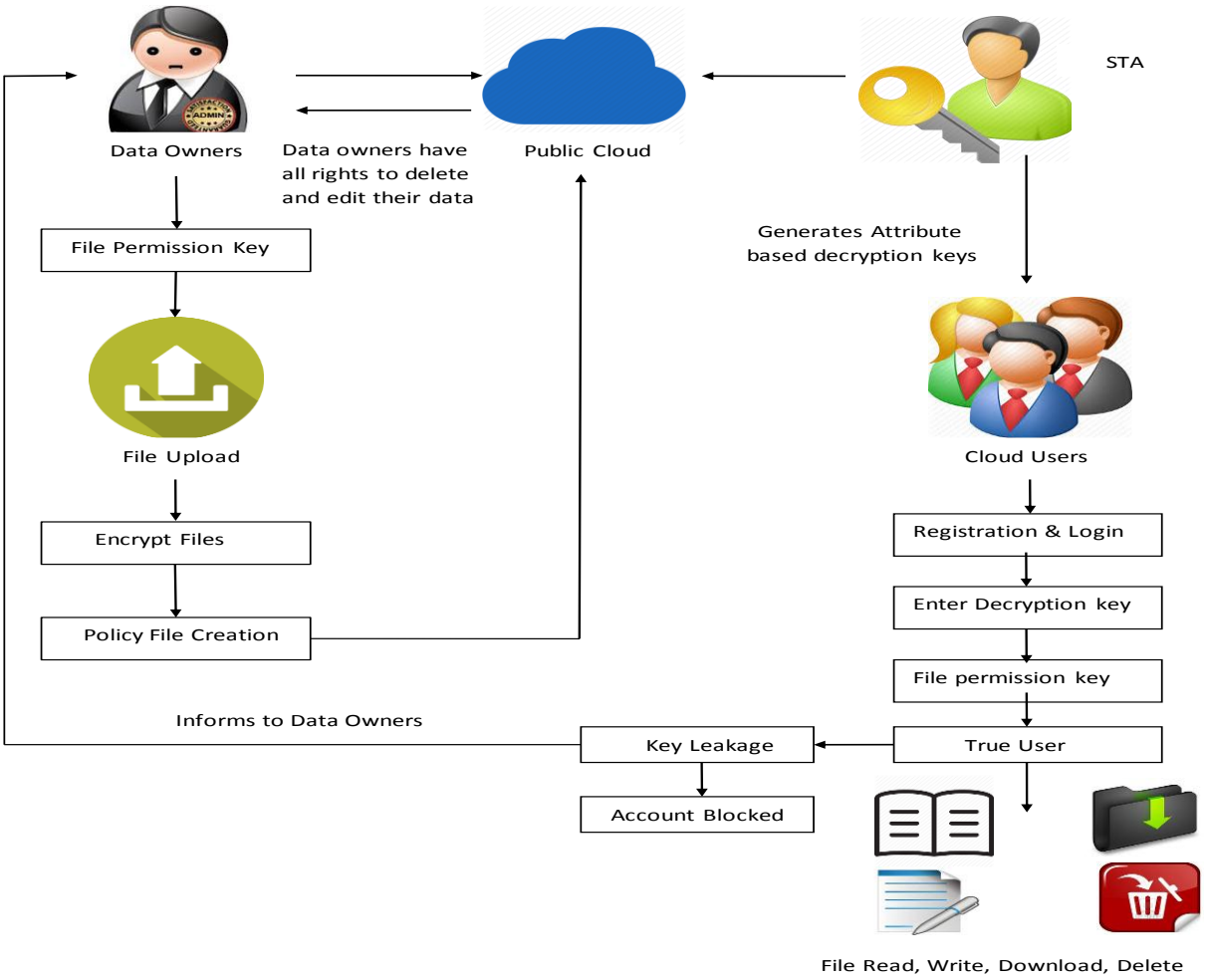
3. EXISTING SYSTEM

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.

4. PROPOSED SYSTEM

In this work, 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 (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.

5. ARCHITECTURE



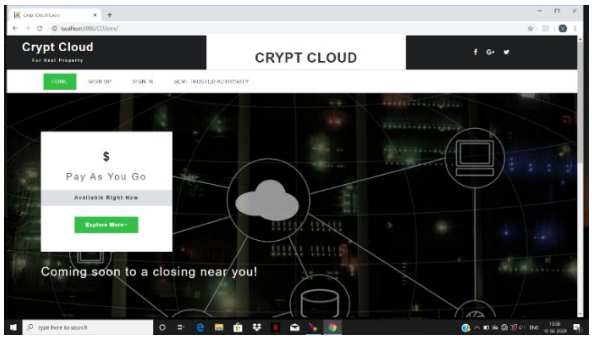
6. MODULES

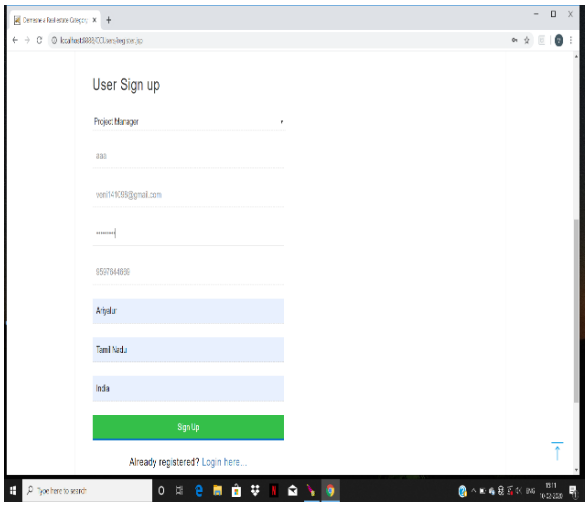
- Organization profile creation & Key Generation
- Data Owners File Upload
- File Permission & Policy File Creation
- Tracing who is guilty

MODULE DESCRIPTION:

6.1. 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.



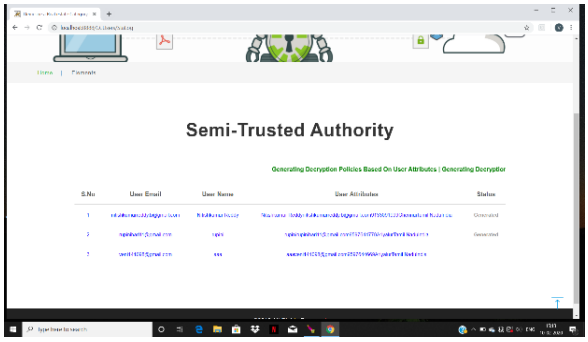


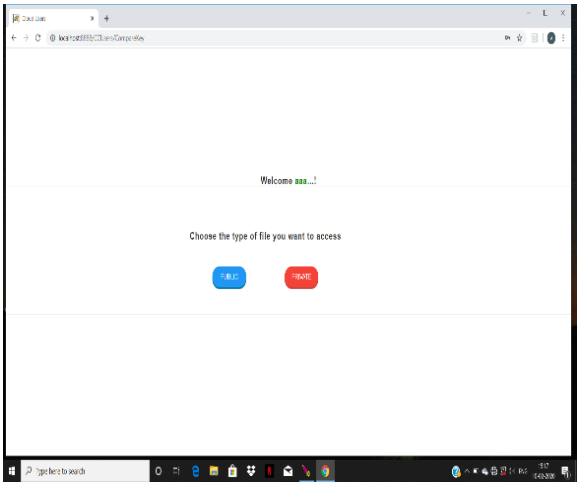
6.2. Data Owners File Upload

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. Once transferring information to public cloud account owners and also creates a special software access authorization key for people inside the enterprise to access data.

6.3. 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.

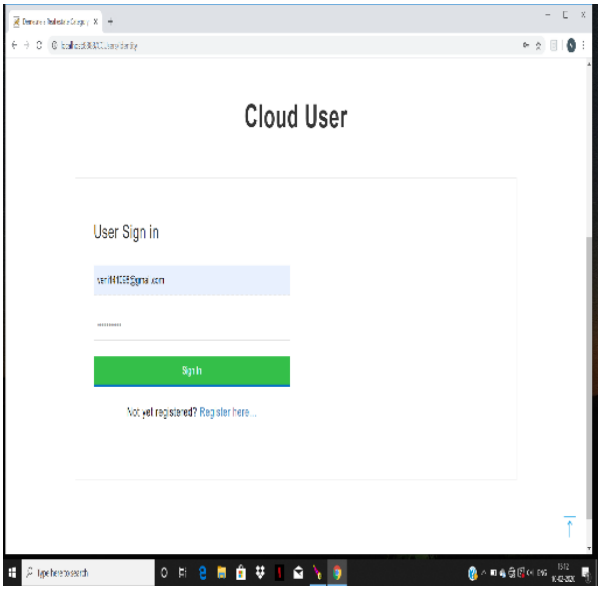


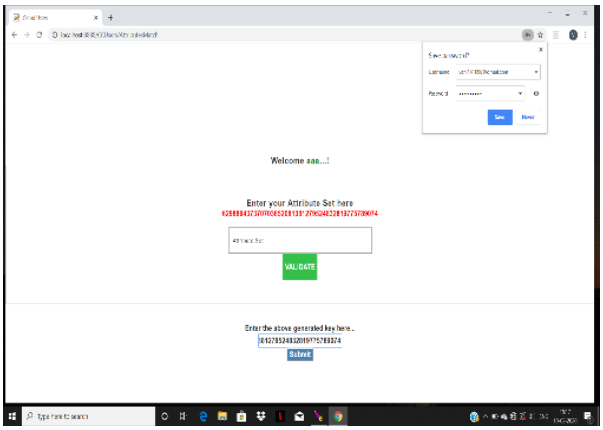


6.4. Tracing who is guilty

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. And some employees have all the permissions except delete the data. If any Senior Employee leaks or shares their secret permission keys to their junior employees they will request to download or delete the Data Owners Data. While entering the key system will generate attribute set for their role in background validate that the user has all rights to access the data. If the attributes set is not matched to the Data Owners policy files

they will be claimed as guilty. If we ask them we will find who leaked the key to the junior employees.





Several Workers are required to read and write. And some employees are permitted everything but to remove the details. When a senior employee spills or exchanges with their junior workers their hidden access keys, they may threaten to view or remove the Software Owners. While entering the password for the re-encryption method, a series of attributes for their position in the context validation would produce that the consumer has all rights to access the info. If the collections of attributes are not aligned with the control files of the Data Owners they will be found guilty. If we question them we'll find out who has released the key to the junior workers.

7. CONCLUSION

In this paper we have proposed a system in which we can able to find the malicious or the guilty users who is trying to access our organization details thus we could able to decrypt the data that is involved so that it could identified by the decryption attribute set that is by the encryption that is involved. Thus, AU is assumed to be fully trusted in Crypt cloud+. However, in practice, it may not be the case .Is there any way to reduce trust from AU? Intuitively ,one method is to employ multiple AU's. This is similar to the technique used in threshold schemes. But it will require additional communication and deployment cost and meanwhile, the problem of collusion among AUs remains. Another potential approach is to employ secure multi-party computation in the presence of malicious adversaries. How-ever, the efficiency is also a bottleneck. Designing efficient multi-party computation and decentralizing trust among AUs (while maintaining the same level of security and efficiency) is also a part of our future work.

8. REFERENCES

[1] Qi Jing, Athanasios V.Vasilakos , JiafuWan, Jingwei Lu, and Qiu . Security of the internet of things: perspectives and challenges. Wireless Networks, 20(8):2481–2501, 2014.

[2] Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki,Takashima and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Advances in Cryptology–EUROCRYPT 2010, pages62–91. Springer, 2010.

[3] Jiaqiang Liu, Yong Li, Huandong Wang, Depeng Jin, Li Su,Lieguang Zeng, and Thanos Vasilakos. Leveraging software-defined networking for security policy enforcement. Inf. Sci., 327:288–299, 2016.

[4] Qiang Liu, Hao Zhang, Jiafu Wan, and Xin Chen. An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing internet of things. IEEE Access, 5:7001–7011, 2017.

[5] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Junqing Gong, and Jie Chen. Traceable cp-abe with short ciphertexts: How to catch people selling decryption devices on ebay efficiently. In Computer Security-ESORICS 2016, pages 551–569. Springer, 2016.

[6] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma,and Lifei Wei. Auditable -time outsourced attribute-based encryption for access control in cloud computing. IEEE Transactions of Information Forensics and Security, 13(1):94–105, 2018.

[7] Hu Xiong, Kim-Kwang Raymond Choo, and Athanasios V Vasi-

9. AUTHOR PROFILE

I.Veni is a student currently studying fourth year B.E (CSE) in R.M.D Engineering College, Chennai, Tamil Nadu, India. Her areas of interest include Computer Networks, Operating Systems and Software Engineering.

H. Rupini is a student currently studying fourth year B.E (CSE) in R.M.D Engineering College Chennai, Tamil Nadu, India. Her areas of interest include Software Engineering, Object Oriented Analysis and Design and Web Designing.

G. Vidhya is a student currently studying fourth year B.E (CSE) in R.M.D Engineering College, Chennai, Tamil Nadu, India. Her areas of interest include Data Structures, Software Engineering, Web Designing and Object Oriented Analysis and Design.

Mr. D. Jayakumar B.E, M.E., is working as an Associate Professor in R.M.D Engineering College, Chennai, Tamil Nadu. He has 16 years of experience in teaching Computer Science. His fields of interest include Operating System and Mobile Computing.