Attribute based Data Management in Crypt-Cloud

Teja Rajashekar.B[1], Yukta Chaudhary.P[2], Pamuganipalli Divya[3] , Ms.Logeshwari[4]

[1]Student, Dept. of Computer Science & Engineering, SRM IST., Tamil Nadu, India
[2]Student, Dept. of Computer Science & Engineering, SRM IST., Tamil Nadu, India
[3]Student, Dept. of Computer Science & Engineering, SRM IST., Tamil Nadu, India
[4]Assistant Professor, Dept. of Computer Science & Engineering, SRM IST., Tamil Nadu, India

---***---

Abstract - *Digital file computing and backup services are valuable to businesses and institutions of all kinds. Data management in the cloud is rising as an alternative to data management using traditional on premises software systems. However like different cloud computing technologies, cloud data management can introduce challenges like information security associated with storing sensitive business information outside the company's firewall. In this paper, we tend to propose a system that involves attribute based data management in crypt cloud. At the site end the individual has an initial level authentication procedure that is processed inside the database of the website. Now the accountable Semi-Trusted Authority produces decryption keys dependent on their collection of characteristics for the members of the organization. The encryption of the files uploaded into the general public cloud is completed by the data owner using RSA encryption algorithmic program which generates a unique file access permission key for the users to access the information within the cloud. The outsourced details may be accessed by registered data users (e.g., read, compose, print, erase, and decrypt). Based on their expertise and role entered in their registered records, file permission keys are given here to the users. Senior staff have any right to access the data (read, write, remove, and download). Fresher's have just the authorization to search the files. If any senior worker leaks or shares their secret permission keys to their junior workers, the system will generate an attribute set for their role in the background confirming that the user has every right to access the information when entering the password for re-encryption. Unless the collection of attributes is not aligned to the regulation files of the data owners they would be charged as guilty. The proposed scheme achieves confidentiality and user access privileges.*

***Key Words*: data, cloud, management, encryption, insert.**

1. INTRODUCTION

BACKGROUND:- In the simplest form, digital infrastructure takes resources ("internet technology") and transfers them behind the boundaries of an organization. In earlier times, most of the companies used to depend on the in-house servers for storing their growing collection of files and online data; but today rather than buying on-premise storage resources and managing them, resources are bought on-demand within the cloud. In the past, most companies used to rely on in-house servers to store their growing collection of files and online data; but today, rather than buying and managing onsite storage resources, resources are being purchased on demand in the cloud. The concerns we face so far in cloud computing are cyber threats, interference by the authorities, lack of standardization and outages. Therefore, protection of data files until they are placed in cloud computing facilities is an important way to solve much of those issues. The next big move is to hold electronic data on cloud servers, as it requires unrestricted access. Another benefit when it comes to keeping all knowledge inside the cloud is that it guarantees simplicity and that the data is therefore readily available from everywhere in the world. Cloud platforms have been developed to be the most suitable choice for digitally storing data electronically. Crypto cloud storage is a new platform for sharing computer resources which protects privacy and data protection. Well, cryptocloud computing in a cloud environment ensures information security and integrity throughout the entire procedure. The security management of cloud computing can even be carried out by authorizing the signatures of each element involved.

OUR CONTRIBUTION :- In crypt-cloud we build a far richer kind of attribute-based data management framework. In our construction the authorized users are going to be ready to access the outsourced data with the assistance of two keys. First being the decryption key and second being the file permission key. Here the decryption key and the file permission key are generated with the assistance of RSA and AES encryption algorithm. Data owner or admin will generate different file permission keys to their files and issue those keys to users who have access to their files under the same organization. They will also generate policy files about who can access their data. Regulation Software breaks the key for reading, publishing, uploading, and removing the text. The customer has an initial stage of registration phase at the electronic end of our program. During this method, users are expected to have their personal details that is saved in their database by the server. The semi-trusted authority further produces the decryption keys dependent on the collection of attributes contained in the database. In addition we offer a tracking system which can trace a user if he/she intends to use the file permission key for wrong usage.

2. LITERATURE REVIEW

2.1 PAPER A

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 labeled, 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. This essentially reduces the need to focus on the database system to avoid unwanted disclosure to data and would improve the scheme's capacity for encryption and decryption in terms to calculation time, cipher text and private key duration. The disadvantage of encrypting data is that it severely limits users' flexibility to share their encrypted data selectively at a fine grained level[10]. On top of this, it is not even feasible to understand an access management involving monotonous permission trees when utilizing the interface hierarchies.

2.2 PAPER B

Bounded Cipher-text Policy Attribute Based Encryption:

They introduced the primary construction of an encryption scheme based on the ciphertext-policy attribute which consisted of providing a security proof based on a standard number theoretical assumption and supporting advanced access structures[4]. Their design may help access structures that were described as their nodes by a restricted size access tree with threshold gates. At the time of system setup, the bound on the dimensions of the access trees is chosen and is represented by a tuple (d, num) where d represents the utmost depth of the access tree, and number represents the utmost number of children each non-leaf node of the tree could have. They emphasize that the encryptor will dynamically select any access tree that satisfies these upper limits on the distance. The security proof is based on the assumption of the standard Decisional Bilinear Diffie-Hellman (BDH). 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 (CP-ABE)[4] 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.

2.3 PAPER C

Cryptography based secure file system:

It notes that cryptography not only complements certain security measures of UCC transformations but also enforces safe applications [13]. Several systems for applying security are evaluated according to health, reliability and consumer convenience. But there's the problem of the cryptographic keys being generated and securely distributed. If only users know the cryptographic keys, in period of reorganization and recovery of errors there is a need for strong cooperation between the DBA and users.

2.4 PAPER D

Cryptographically Enforced Data Access Control in Personal Health Record Systems:

This program offers numerous value-added functionality such as accessing health-related records, safe sharing and monitoring of health care providers with that information[12]. For health information management settings, a cloud-assisted PHR program maximizes the probability that PHR applications can interoperate with other programs. Many owners or patients are available for personal health record (PHR) program, but the current data access control systems are largely configured for single authority / owner situations, proposing a totally new patient-centered data access control scheme named Revocable Multi Authority Collection Dependent Encryption (R- MA- ASBE). Now this new scheme inherits the power of consistency, scalability and fine-grained patient-centered data access which the previous schemes ignored. But the problem is that the patients will miss their physical connection to their cloud-served health data[12]. Plus, components that do not seem to be correlated with the revoked feature may not be changed. In addition, each patient will encrypt their personal health record (PHR) data before uploading it to the cloud because patients may lose their physical connection to their cloud-served health records. However, in MA-ABE scheme the attribute revocation was not implemented in a single authority situation.

2.5 PAPER E

Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud:

It proposes delegation-aware encryption strategy to delegate the cloud to amend policy data and, second, Crypt-DAC also proposes an flexible onion encryption strategy to delegate file data to the cloud[8].During the file's life cycle being modified, encrypted or decrypted, the security layers are constantly through again and again before a predefined limit is achieved. This approach suggests delayed de-onion encryption technique to regularly update the file's symmetric key list and eliminate bounded layers of encryption over it by writing operations. It also proposes delegating the cloud to update the policy data while using a delegation-aware encryption strategy in a privacy conserving way. Through utilizing an adaptive onion encryption technique, the expensive re-encryption of file data at the hand of the user was avoided. Apart from that a slow de-onion encryption technique was implemented to prevent overhead reading of the text. The theoretical review and even the performance evaluation reveal that Crypt-DAC achieves higher output orders of magnitude in access revocations while maintaining equal protection properties under the honest yet curious danger model relative to previous schemes[1] -[4]. The challenges faced in this is that it limits the flexibility of users to make changes in the data in the absence of the admin.

3. BACKGROUND AND ASSUMPTIONS

3.1 System Model

We find a case where businesses agree to outsource data computing to a private cloud service (e.g., Alicloud, Microsoft Azure). Our network model includes four categories of entities: a distributed domain, a computer controller, a significant number of the organization's staff and a semi-trusted authority. The data administrator is responsible for the file permission key, file upload, encryption of files and policy file. The policy file includes information regulating access policies for the data stored in the cloud. The semi-trusted authority generates the decryption key for the employees of the organisation. By creating and distributing cryptographic keys used to encrypt files, it assigns / revokes access permissions. Employees can download any file data from the cloud, but they are only permitted to decrypt and view certain files in compliance with their delegated permissions in the policy file based on the user 's name.We did not find concerns around data deduplication. We always presume that both parties interact via pairly protected channels (for example, SSL / TLS tunnels).

3.2 Threat Model

In this model, we see the administrator as being truthful. Users / employees can try out their access permissions to access the file details. If an employee spills or transfers their hidden authorization keys to the other employee then a series of attributes for their position in the context will be created when entering the credentials for the re-encryption program to verify that the consumer has all privileges to access the data. If the collection of attributes is not aligned to the regulation files of the data owner they would be found to be responsible. And further action can be taken against them.

3.3 Security Goals

They plan to include protections for anonymity and user rights for file data management in the cloud depending on the attributes. Confidentiality: Our device stores cloud encryption data but never shows cloud decryption keys. It preserves the details in the system from secrecy.

User access control privileges: Our program uses cryptography to implement access control and enable users to access client data from the policy server according to their access permissions.

3.4 Attribute Based Access Control

We develop and evaluate the program depending on the characteristics of the organisation's workers. The model defines permission management using abstraction: employee assignment explains the access permissions associated with a particular work task, employees are delegated to the positions associated with their job responsibilities, and the employee shall have access to the files deposited where they are given a label that requires access to the information held in the cloud.

3.5 Cryptographic Tools

Symmetric / Asymmetric cryptography: we use symmetric-key encryption schemes (GenSym, EncSym, DecSym)and public-key encryption schemes(GenPub, EncPub, DecPub).

4. DESIGN DETAILS

The device owner transfers information to the cloud through this program, then encrypts the device by utilizing RSA encryption. The administrator grants classification system permissions by the allocation of device keys depending on the data contained in the policy log.Next we define the various activities of the machine. There are four styles of operations inside the system: building profiles and producing main, uploading data, making data and building tuples, and tracking the culprit.

4.1 Profile Creation & Key Generation

The employee has the web-end of an initial level registration process. For this phase the employee offers his personal details. The Inturn server holds the data in its database. Now the Accountable STA produces decryption keys for workers dependent on their collection of attributes (e.g. email, mail-id, phone number, etc.). User gets the provenance to unlock data from the Company after having obtained Responsible STA decryption keys.

4.2 File Upload

File owners build their accounts under the public cloud in this section, and upload their file into the public cloud. Once transferring information to public cloud account owners, their account must be authenticated using the RSA Encryption method that produces public key and secret key and also creates a special software access authorization key for people inside the enterprise to access data.

4.3 File Permission & Tuple Creation

Specific data owners can create separate file authorization keys for their files and give certain keys to the organization's workers to access their files. And it also creates policy files that can link their data to all that can.

Rule Data breaks the system read document, reads the data, saves the system and deletes the file.

4.4 Tracing Who Is Guilty

D. Authorised users/employees will be able to access (e.g. read, write, download, delete and decrypt) the outsourced data depending upon their attributes. There file access keys are given to the organization's workers depending on their background and status with regard to their reported records. Senior workers are allowed to view all the data (read, write, erase, and download). Fresher's are enabled just to read the files. 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.

5. SECURITY ANALYSIS

We evaluate device security utilizing the access control expressiveness method referred to as appsensitive access control evaluation (ACE)[22]. Evaluation of access control is a formalized statistical method that assesses how effectively an idealized access control system executes a nominee access control system. Under ACE we prove the device is right and stable. In particular, we demonstrate that the device fulfills all three properties specified in ACE which are correctness, protection and preservation. At a high point, precision and protection guarantee that an area for implementation can not decide how it communicates with the idealized structure via inputs , outputs and intermediate states. The two assets guarantee right framework. Preservation guarantees authorization is granted in the idealized RBAC0 scheme if and only if its mapping is granted in the program. This property assures a secure system. Since our system inherits the design of [23], our evidence is similar to that of [23].

6. SYSTEM EVALUATION

We name the two revocation schemes introduced in [23] as immediate re-encoding and delayed reencoding. We often call the scheme of revocation introduced in [24] as homomorphic re-encryption. We i n t roduce Crypto+++-based cryptographic schemes[26]. Every cryptographic algorithm has its own strengths and weaknesses. We pick the cryptographic algorithm based on the application's requirements which will be used. From the results of the experiment and the contrast, the blowfish algorithm is a good option for time and memory according to the parameters of guessing attacks and the features needed, because it reports the shortest period of all algorithms. This often uses the least volume of ram storage. Since the key priority of the systems is data security and privacy, AES algorithm may also be chosen. If the application's requirement is network bandwidth, the best choice is the DES. We should find that AES and blowfish algorithms are used to prevent the application from guessing attacks and it can be implemented in addition to all internet protocols based on IPv4 and IPv6 and the tests reported in this paper showing that all algorithms and groups are working well with specific execution time and memory use.

6.1 Security Testing

Security monitoring helps to validate the mechanisms of security installed into a device well, in effect shielding it against excessive intrusion. The device stability must be checked for frontal attack invulnerability, as well as for rear attack invulnerability. The tester places the position of an person, who wants to infiltrate the framework during defense.

6.2 User Acceptance Testing

User acceptance of the system is a key factor in any system's success. The program under review is checked for consumer adoption by remaining in regular touch with prospective systems and users while they evolve and make improvements as appropriate. This is done with the following points in mind.

- Creation of computer inputs.
- Layout of the escape panels.

7. FUTURE SCOPE

We did not find concerns around data deduplication. Safe deduplication technique [25] may be used here if needed.

8. CONCLUSION

Thus we provide honesty and protection of the data of an entity which is deposited by the aid of this paper in a public cloud. We introduced Crypt-DAC-an attribute-based data management framework that offers functional cryptographic implementation of complex access control inside a cloud service that is theoretically untrusted. Using four modules the machine achieves its objectives. In specific, we suggest delegating the cloud to amend policy details in a way that protects privacy and using a delegation aware encryption technique. Using an adaptive AES encryption and RSA encryption technique, we recommend to prevent expensive re-encryption of file data at the administrator level. The theoretical study, and thus the output evaluation, reveals that Crypt-DAC achieves higher efficiency orders of magnitude in access revocations while maintaining equal protection properties under the honest yet suspicious vulnerability model relative to previous systems.

ACKNOWLEDGEMENT

It is our pleasure to convey our heartfelt gratitude to our project guide Ms. Logeshwari and our project coordinators, Dr. G. Paavai Anand and Mr. H. Anwar Basha for their useful feedback, skillful direction, motivation, full-hearted cooperation and constructive criticism during our project period. We convey our heartfelt thanks to our Head of Department Dr. S.Prasanna Devi for motivating and empowering us to pose the project in our department premises on the subject of "Attribute Based data management In Crypt-Cloud" for partial fulfillment of the requirements leading to the awarding of B-Tech. We take this opportunity to thank all of our faculty members, Dean, Dr. K.Duraivelu and Management who supported our project directly or indirectly. Last but not least, we express our appreciation to our friends for their support and cooperation.

REFERENCES

1. J. Bethencourt, A. Sahai, and B. Waters, Ciphertext - policy attribute based encryption, in IEEE S&P, 2007.

2. X. Wang, Y. Qi, and Z. Wang, Design and Implementation of SecPod: A Framework for Virtualisation -based Security Systems, IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 1, 2019.
3. J. Ren, Y. Qi, Y. Dai, X. Wang, and Y. Shi, AppSec: A Safe Execution Environment for Security Sensitive Applications, in ACM VEE, 2015.
4. V. Goyal, A. Jain, O. Pandey, and A. Sahai, Bounded ciphertext policy attribute based encryption, in ICALP, 2008.
5. E.Shen, E.Shi, and B.Waters: Predicate privacy in encryption systems, in TCC, 2009.
6. J. R. Lorch, B. Parno, J. W. Mickens, M. Raykova, and J. Schiffman, Shroud: Ensuring Private Access to Large-Scale Data in the Data Center, in USENIX FAST, 2013.
7. A. Sahai, and B. Waters: Fuzzy identity-based encryption, in EURO- CRYPT, 2005.
8. Saiyu Qi, Yuanqing Zheng: Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud, in IEEE Transactions on Dependable and Secure Computing, 20019.
9. Prerna, Parul Agrawal : Cryptography Based Security for Cloud Computing System, in IJARCS Research paper, 2017.
10. Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data
11. Mikhail J. Atallah, Keith B. Frikken, and Marina Blanton: Dynamic and Efficient Key Management for Access Hierarchies
12. Dr. Ragesh G. K., Dr. K. Baskaran : Cryptographically Enforced Data Access Control in Personal Health Record Systems, in RAEREST , 2016.
13. E. Gudes. : The Design of a Cryptography Based Secure File System, in IEEE Transactions on Software Engineering, 1980.
14. www.cs.ucdavis.edu
15. Assured Way to Manage Various Controls in Cloud, International Journal of Recent Technology and Engineering, 2019.
16. www.cs.ucla.edu
17. www.cs.cmu.edu
18. www.ijarcs.info
19. www.milesweb.com
20. L. Ibraimi, Cryptographically enforced distributed data access control, Ph.D. dissertation, University of Twente, 2011.
21. S. Muller and S. Katzenbeisser : Hiding the policy in cryptographic access control, in stm, 2011.
22. T. L. Hinrichs, D. Martinoia, W. C. Garrison III, A. J. Lee, A. Panebianco, and L. Zuck, Application-sensitive access control evaluation using parameterized expressiveness, in CSF, 2013.
23. W. C. Garrison III, A. Shull, S. Myers, and, A.J. Lee, On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud, in IEEE S&P, 2016.
24. F. Wang, J. Mickens, N. Zeldovich and V. Vaikuntanathan, Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Clouds, in NSDI, 2016.
25. T. Jiang, X. Chen, Q. Wu, J. Ma, W. Susilo, and W. Lou, Secure and Efficient Cloud Data Deduplication With Randomized Tag, IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, 2017.
26. https://www.cryptopp.com/