Foreseeable of IP Address Allocations for Cloud Computing Platforms

Rengaraj R[1], Bhuvaneswari M[2], Raesa Tanzila S A[3], Sathya B[4]
[1]*Assistant Professor Information Technology, Saranathan College of Engineering, Trichy*
[2,3,4] *Information Technology, Saranathan College of Engineering, Trichy*

Abstract- **Due to increase of cloud storage in recent years by the consumers there's a massive popularity computer memory device in addition as in mobiles by using file syncing and sharing (FSS) services. But tremendous increasing mobile devices have of course raised a replacement challenge for preventing the decoder abuse within the FSS service. During this approach we address the problem by using tracing and revoking traitors by employing a new system model called anomaly detection and that we present a replacement threshold cryptosystem that executes the partial-order key hierarchy, the same as role hierarchy in Hierarchical RBAC. This can be also called Partially-ordered Hierarchical Encryption (PHE). Our system provides two different security mechanisms which are traitor tracing and revocation to support digital forensics. Our construction is threshold provably secure which may be known by the safety and performance analysis. It consists of distinct characteristics like revoking users, constant-size cipher texts and decryption keys, lower overloads for large-scale systems.**

Index terms- **: Cloud Computing, Anomaly detection**

1.INTRODUCTION

In recent years, many cloud storage services, like Box, Drop box, Media Fire, Sky Drive, Sugar Sync, are available to small-to-medium business, and individual. The above said cloud based storage might be particularly attractive for consumers by providing on demand capacity, low-cost service, and long run archive. Furthermore, cloud services have brought great convenience to people's lives because consumers can access applications and data from the cloud anywhere within the world and via any available device, like personal computers, tables, and mobile phones. Therefore, more enterprises and individuals have moved their data, like personal data and enormous archive system, into the cloud daily. The cloud has become a necessity to several of the individuals, enterprises, and government use.

The cloud aims to scale backcosts, and helps the users concentrate on their core business rather than being impeded by IT obstacles. Virtualization is being one amongst the most enabling technology for cloud computing. The Service Oriented Architecture (SOA) concepts are adopted in cloud computing to assist the user break these problems into services which will be integrated to produce an answer.

Agility: Improvements will be made to organisation using this, as user's flexibility with re-provisioning, adding, or expanding technological infrastructure resources will be increased by adopting cloud computing.

Location Independence: It enables users to access systems employing a browser no matter their location or which device they use (e.g., PC, mobile phone). An off-site which may be accessed via the net, called infrastructure (typically provided by a third-party), will be used to connect users from anywhere.

Maintenance: The maintenance of cloud computing platforms are easy because it's not essential to be installed on each user's computer and it can be accessed from different places irrespective of any location.

Performance: The performance of cloud computing applications is monitored by the IT experts from the service provider.

Reliability: The employment of multiple redundant sites can help in improving reliability, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

Scalability: Provisioning of resources on a fine-grained, self-service basis in near real-time, without users having to engineer for peak loads will be achieved by scalability and elasticity via dynamic ("on-demand").

2. ARCHITECTURE

In the initial stage, the cloud owner creates his login and acquire access from the provider. Next the user can get his cloud space by the approval of owner by using his login credentials. The user can store any quitego into the space for storing along with his respective public and personal key. Once the file is saved the cloud owner has the rights to synchronize and share the files. When the attacker intrudes the owner has all quite restriction methods to guard the files from the attacker. When the attacker attacks the cloud server generates the knowledge to the owner. The attack might be of any of the kinds like SQL injection, anomaly and different patterns. The owner has the potential of blocking the intruder by sorting out and blocking the MAC and IP address of the intruder. They may also revoke and trace the attackers. By sorting out different instances the owner could block them by the strategy of pattern matching.

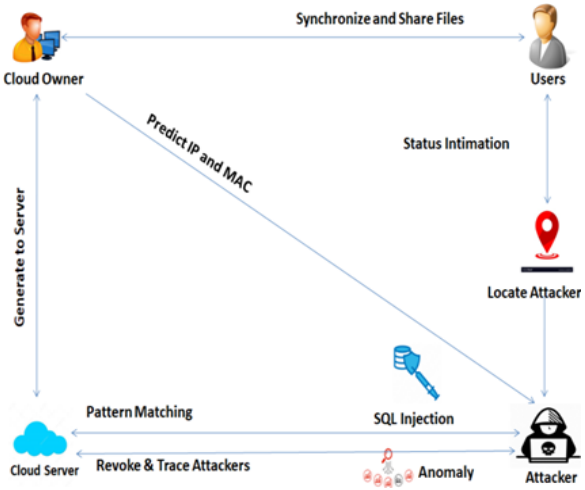


Fig 1.1 Architecture diagram

3. EXISTING SYSTEM

Bring-your-own-device (BYOD) policies and increasing mobile devices are changing the necessities for a way users want (and need) to access corporate data. The cloud storage service is mostly initiated by individual users who store data and download it to sync and collaborate while performing on projects. Therefo re,file syncing and sharing (FSS) services are provided by many cloud based platforms. These two services introduce new features for enterprise file sharing solution for online collaboration and storage:

File sharing: It allows the users to not only access files anywhere, anytime and from a spread of endpoint devices, but also collaboratively edit file together.

File syncing: It's a replacement online backup mechanism for syncing data across multiple devices, like a home computer, tablet or smart phone, as well as collaboration and dealing with teams.

Security may be a problem that has got to be considered for deploying a file syncing-and-sharing service. Several recent surveys show that 88% potential cloud consumers worry about the privacy of their data, and security is commonly cited because the top obstacle for cloud adoption. At first, the multi-tenant nature of the cloud is liable to data leaks, threats, and malicious attacks. Therefore, it's important for enterprises to have strong access control policies (such as Role-based Access Control (RBAC) or Attribute-based Access Control (ABAC)) in place to keep up the privacy and confidentiality of knowledge for collaboration with teams. Sometimes cloud providers have access to the info stored within the cloud, and can control access to that by outside entities. When this can be the case, the challenge is to keep up the confidentiality of data and limiting privileged user access to it. This could be achieved by encrypting the data before storing it within the cloud, and enforcing legal agreements and contractual obligations with the cloud service provider to ensure protection of knowledge.We work on a corporate FSS service with online collaboration. In such work security may be a major problem that has got to be considered for deploying a file syncing and sharing service. It's important for cloud providers to have strong access control policies (such as Role-based Access Control (RBAC) or Attribute-based Access Control (ABAC)) in place to keep up the privacy and confidentiality of knowledge for collaboration with teams.

4. PROPOSED SYSTEM

To address these problems, it is necessary to style a construction for hierarchical cryptosystems, considering the new features provided by some recently proposed cryptography technologies such as HIBE, ABE, IBE. We present a replacement FSS model for user abuse prevention and enhanced protection against unauthorized access. The proposed model uses the hierarchical role-based access control model, which is recognized for its support for simplified administration and scalability of collaboration and dealing with teams. Moreover, the look of this model is generic enough to support other access control policies, such as discretionary access control and multilevel security. This model that addresses and incorporates the afore-mentioned authorization requirements are often built using three sorts of components:

Anomaly Detection: This can be used for detecting abnormal players. More exactly, it is liable for monitoring deployed resources and might allocate or release them to make sure the compliance of enterprise-side existing access control system. The output of this module is a few suspected anomaly players. The suspected anomaly and their involvement within the cloud server have been monitored time to time for effective performance of the server. By doing so, the anomaly users can be identified and blocked by the cloud owner. Because the entire data has been encrypted and maintained with various security measures the prospect for attack of the user data has been reduced to the core.

Tracing Traitors: This can be liable for finding out the traitors from the suspected players recognized within the previous step. In some cases this can be simple and straightforward, but such a practice procedure sometimes leads to solution difficulties if we request that the secrets or keys stored within the player cannot be leaked in the tracing procedure.

Revoking Traitors: This can be liable for revoking the authority (or license) of traitors found in the previous step. The straightforward revocation method could also be evaded within the way of license forgery and tampering. Taking into account the issue in comparing cryptographic key forgery and license forgery, the key based revocation would be a more practical and secure manner. Whereas the owner can manage and handle the entire IP Addresses that has been added to the network so phishing networks or unauthorized IP's may be eliminated and added to the block list for the owner reference.

5. SYSTEM ARCHITECTURE

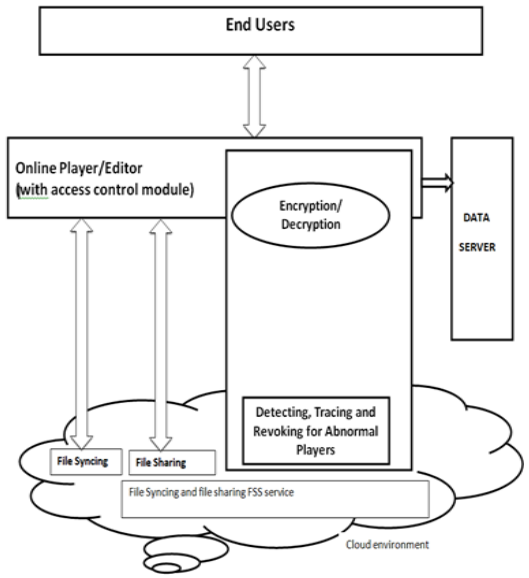


Fig 5.1 System Architecture

This model that addresses and incorporates the afore-mentioned authorization requirements may be built using three types of components:

Anomaly detection: This is can be used for detecting abnormal players. To be exact, it is liable for monitoring deployed resources and it can allocate or release them to ensure the compliance of enterprise-side existing access control system. The output of this module is a few suspected anomaly players.

Tracing traitors: This can be liable for finding out the traitors from the suspected players recognized within the previous step. In some cases this can be simple and straightforward, but such a practice procedure sometimes leads to solution difficulties if we request that the secrets or keys stored within the player cannot be leaked in the tracing procedure. We call it 'black box tracing.

Revoking traitors: This can be liable for revoking the authority (or license) of traitors found within the previous step. The simple revocation method (e.g.,

the license is appeared in Blacklist) could also be evaded in the way of license forgery and tampering. Taking under consideration the issue in comparing cryptographic key forgery and license forgery, the key based revocation would be a more practical and secure manner.

6. MODULES

6.1 Key Generation

There are three algorithms in Merkle hash tree:KeyGen, Sign and Verify. In KeyGen, a public key and a personal key is generated by each user in the group. In Sign, a user within the group is in a position to get a signature on a block and its block identifier with his/her private key and everyone the group members' public keys. A string known as block identifier is employed which will distinguish the corresponding block from others. A verifier is in a position to test whether a given block is signed by a gaggle member for Verify.

6.2 Detect Anomaly and Pattern Matching

This is used for detecting abnormal players. More exactly, it is responsible for monitoring deployed resources and might allocate or release them to ensure the compliance of enterprise-side existing access control system. The output of this module is some suspected anomaly players. Apart from the same network i.e.: the same IP Address, new users can be added by the cloud owner and the unauthorized users are blocked by the concerned cloud owner.

6.3 Traitor Tracing and Revoke Traitors

Traitor tracing is responsible for finding out the traitors from the suspected players recognized in the previous step. In some cases this is simple and straightforward, but such a practice procedure sometimes results in solution difficulties if we request that the secrets or keys stored in the player cannot be leaked in the tracing procedure. We call it 'black box tracing'.

Revoke traitors is responsible for revoking the authority (or license) of traitors found in the previous step. The simple revocation method may be evaded in the way of license forgery and tampering.

6.4 File Syncing and Sharing

File sharing allows the users to not only access files anywhere, anytime and from a variety of endpoint devices, but also collaboratively edit file together.

File syncing becomes a new online backup mechanism for syncing data across multiple devices, such as a home computer, tablet or smart phone and it also can helps in collaboration and working with teams.

6.5 Performance Evaluation

We evaluate the performances of the proposed schemes based on the factors such as bandwidth, user's storage, computation costs and the number of keys. For the sake of clarity, we list some major variables as follows: for secure key hierarchy Ψ = _C,E,K_, Our solution also provides the scalability for practical applications.

7. TECHNIQUES USED

In our system we use Advanced Encryption Standard (AES) Algorithm and RSA Algorithm

In our system we use Advanced Encryption Standard (AES) Algorithm and RSA Algorithm

7.1 ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

The U.S. National Institute of Standards and Technology (NIST) established a specification for the encryption of electronic data in 2001 called Advanced Encryption Standard (AES). AES is a subset of the Rijndael cipher. This Rijndael cipher was developed by two different Belgian cryptographers, Vincent Rijmen and Joan Daemen. Rijndael is one of the family of ciphers which has different key and block sizes.

FEATURES: The number of transformations that are to be performed on information that have been stored in an array is defined by the AES encryption algorithm. Initially, data is put into an array; and then the cipher transformations are repeated over a number of encryption rounds. The key length determines the number of rounds, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Encryption and decryption is done for security purpose. Decryption is done for downloading the file.

ALGORITHM:

Input : Uploading a File
Process :

1. After duplication check is done, the encryption and decryption process is done.
2. The encrypt algorithm takes as input data M and it is encrypted with the help of an encryption key DEK .The output of the cipher text is CT.
3. The encryption is done in order to protect the user's data at CSP with DEK.
4. The decrypt algorithm takes as input the encrypted data CT, with the help of symmetric key DEK. And it decrypts the cipher text and output the plaintext M.
5. The data holder conducts this process to gain the plaintext of stored data at CSP.
   Output : Encrypted and Decrypted File

7.2 RSA ALGORITHM
Public Key Cryptography
Public Key Cryptography also known as Asymmetrical Cryptography is one of the cryptographic system which provides encryption by using a pair of keys. One is the public key which is openly known to all the users in the system and the other is the private key which is in the knowledge of the owner alone. They are used to perform two functions namely, authentication, where the public key verifies that a holder of the paired private key sent the message, and encryption, wherein decryption of the message can be done only by the paired private key holder.

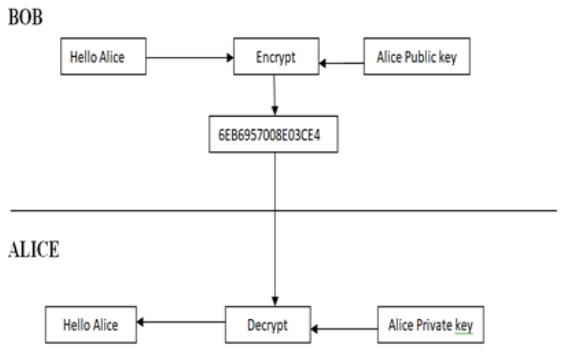


Fig 7.1 Key Generation Algorithm

ALGORITHM:
ENCRYPTION
Sender A does the subsequent

- Acquire the recipient B's public key (n, e).
- Represents the plaintext message as a positive integer m such that $0 \leq m < n$.
- Reckon the cipher text $C = m^e \pmod n$
- Sends the cipher text C to B.

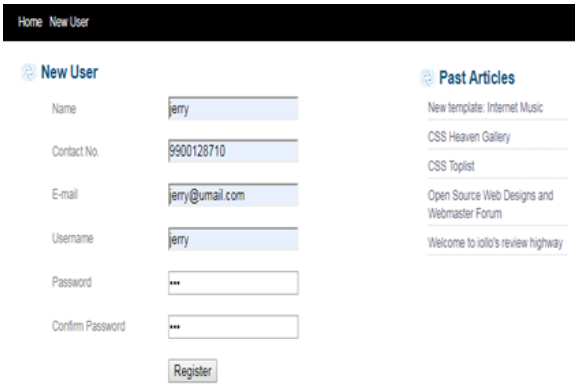
DECRYPTION
Recipient B does the subsequent

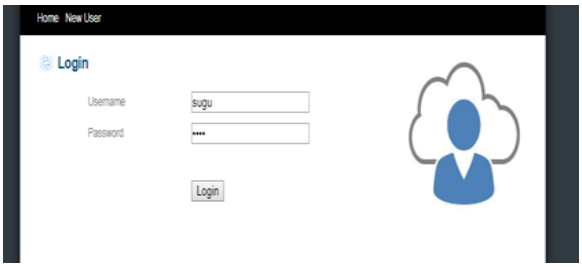
- Alice can recover from by using her private key exponent via computing $m = c^d \pmod n$
- Evoke the plaintext from the integer representative m.

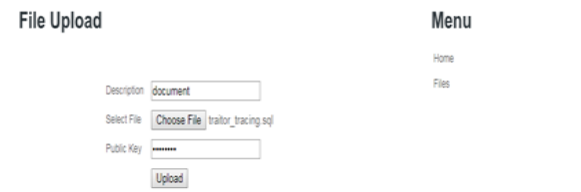
KEY GENERATION

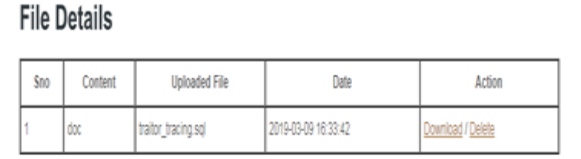
- Select distinct prime numbers p and q.
- For security purposes, integer p and integer q should be chosen at random, and should be of similar bit-length.
- Generate n = pq. 'n' is used as the modulus for both the general public and private keys.
- Reckon $\varphi(n) = (p - 1)(q - 1)$, where φ is Euler's totient function.
- Pick an integer e such that $1 < e < \varphi(n)$ and Greatest Common Divisor of $(e, \varphi(n)) = 1$; i.e., e and φ (n) are co-prime.
- E is released as the general public key exponent.
- E having a short bit-length and tiny hamming weight results in more efficient encryption.
- Determine d as: $d = e^{-1} \pmod{\varphi(n)}$
- D is the multiplicative reciprocal of e mod φ (n).
- This is more clearly stated as solve for 'd' given $(de) = 1 \bmod \varphi(n)$
- D is chosen as the private key exponent.

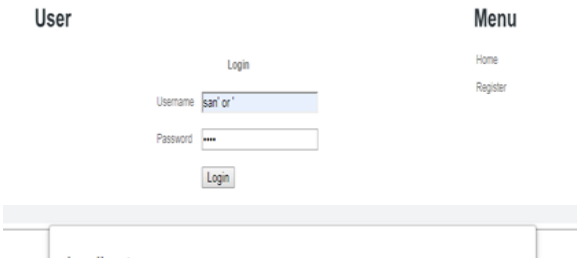
8. IMPLEMENTATION

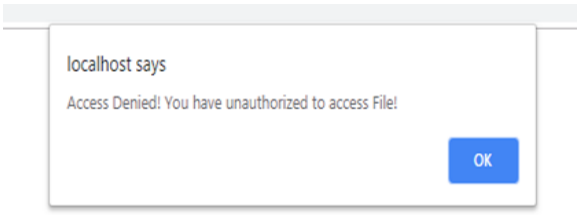


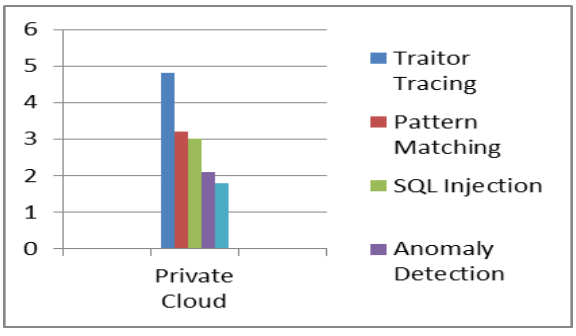












9. CONCLUSION

In this paper, we focus on protection the privacy of outsourcing data and preventing player abuse in file syncing and sharing services in the cloud. We highlight the development of a group-oriented cryptosystem with digital forensics, especially for tracing and revoking methods that can ensure the security of player/editor. Based on this cryptosystem, we present a new secure service model to provide a forensic analysis framework to guide investigations. In our future work, we are planning to introduce a comprehensive anomaly detection, using audit, pattern matching, and risk assessment, for identifying the suspected players.

10. FUTURE WORK

In our future work, we are planning to introduce a comprehensive anomaly detection using audit, attacker identification in public cloud storages, attaining the MAC ID for the every system to enhance the security measure, and also by encrypting the database or the storage that has been allotted to the every cloud user involved in the system.

REFERENCES

[1] C. Gentry, S. Halevi, and N. P. Smart, “Tile-based modular architecture for accelerating homomorphic function evaluation on FPGA”, 2016.

[2] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, “Crypt-EHRServer: Protecting Confidentiality with Attribute-Based Encryption and Encrypted Query Processing”, 2017.

[3] Anjali J. Rathod; V. S. Mahalle, “Resolve the classification problem on sescure encrypted relational data”, 2017.

[4] S. Tu, M. F. Kaashoek, S. Madden, and N. Zeldovich,“A comparative analysis of AES common modes of operation”, 2017.

[5] Sultan Almuhammadi; Ibraheem Al-Hejri,“A comparative analysis of AES common modes of operation”, 2017.

[6] Ibraheem Al-Hejri; El-Sayed M. El-Alfy, “Scalability evaluation of block cipher modes of AES standard”, 2018.