International Conference on Engineering & Technology (ICET-2020)

Available at: International Journal of Scientific Research and Engineering Development

RESEARCH ARTICLE OPEN ACCESS

Encrypting File Sharing and Synchronizing Using Efficient Traitor Tracing and Revocation

Mr.M.Prabhakaran[1],A.Jeevith[2],G.Krishna Prasad[3],S.Mohammed aarif[4].
[1]Assistant professor,[234]UG students.
[1234]Department of CSE,Selvam College Of Technology,Namakkal.

--************************----------------------------------

ABSTRACT:

Due to increase of cloud storage in recent years by the consumers there is a enormous popularity computer storage devices as well as in mobiles by using file syncing and sharing (FSS) services. But bring-your-own-device (BYOD) policies and greatly increasing mobile devices have in fact raised a new challenge for preventing the player/decoder abuse in the FSS service. In our approach we address the issue by using tracing and revoking traitors by using a new system model called anomaly detection and we present a new threshold cryptosystem, called Partially-ordered Hierarchical Encryption (PHE), which implements the partial-order key hierarchy, similar to role hierarchy in Hierarchical RBAC, in public-key infrastructure. Our system provides two security mechanisms which are traitor tracing and revocation to support digital forensics. The security and performance analysis shows that our construction is threshold provably secure. It consists of features like dynamic joining and revoking users, constant-size cipher texts and decryption keys, lower overloads for large-scale systems.

Keywords- Key Generation, SQL injection, anomaly detection, Pattern matching**.**

--************************----------------------------------

INTRODUCTION

In recent years, many cloud storage services, such as box, drop box, media fire, sky drive, sugar sync, have been available to small-to-medium business, and individual. these cloud based storage could be particularly attractive for consumers by providing on demand capacity, low-cost service, and long term archive. furthermore, cloud services have brought great convenience to people's lives because consumers can access applications and data from the cloud anywhere in the world and via any available device, such as personal computers, tables, and mobile phones. therefore, many more enterprises and individuals have moved their data, such as personal data and large archive system, into the cloud every day. the cloud has become a necessity to many of us for individual, enterprise, and government use.the cloud aims to reduce costs, and helps the users focus on their core business instead of being impeded by it obstacles. the main enabling technology for cloud computing is virtualization. cloud computing adopts concepts from service oriented architecture (soa) that can help the user break these problems into services that can be integrated to provide a solution.

EXISTING SYSTEM

Bring-your-own-device (BYOD) policies and an increasingly mobile devices are changing the requirements for how users want (and need) to access corporate data. The cloud storage service is generally initiated by individual users who store data and download it to sync and collaborate while working on projects. Therefore, more and more cloud-based storage platforms provide **file syncing and sharing (FSS)** services. 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 variety of endpoint devices, but also collaboratively edit file together;

File syncing: it is a new online backup mechanism for syncing data across multiple devices, such as a home computer, tablet or smart phone, as well as collaboration and working with teams.

Security is a problem that must 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 often cited as the top obstacle for cloud adoption. At first, the multi-tenant nature of the cloud is vulnerable to data leaks, threats, and malicious attacks. Therefore, it is 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 maintain the privacy and confidentiality of data for collaboration with teams. Sometimes cloud providers have access to the data stored in the cloud, and can control access to it by outside entities. When this is the case, the challenge is to maintain the confidentiality of data and limiting privileged user access to it. This can be achieved by encrypting the data before storing it in the cloud, and enforcing legal agreements and contractual obligations with the cloud service provider to ensure protection of data

DISADVANTAGES

- There is no way to distinguish assigned users because role may be assigned to multiple users who share the same secret-key.
- The secret-key derivation is not able to support functions, like revocation and traitor tracing, in digital forensics.

PROPOSED SYSTEM

We also work on a corporate FSS service with online collaboration In such work security is a major problem that must be considered for deploying a file syncing and sharing service. It is 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 maintain the privacy and confidentiality of data for collaboration with teams. To address these problems, it is necessary to design a construction for hierarchical cryptosystems, considering the new features provided by some recently proposed cryptography technologies such as HIBE, ABE, IBE etc..

We present a new FSS model for player abuse prevention and enhanced protection against unauthorized access. The proposed model uses the hierarchical role-based access control (H-RBAC) model, which is recognized for its support for simplified administration and scalability of collaboration and working with teams. Moreover, the design of this model is generic enough to support other access control policies, such as discretionary access control and multilevel security. We show such a cloud-based FSS model in the Fig. 4. This model that addresses and incorporates the afore-mentioned authorization requirements can be built using three types of components:

Anomaly detection: 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.

Tracing traitors: This 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'.

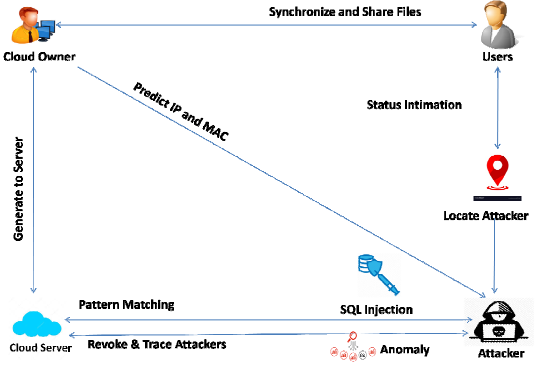
Revoking traitors: This is responsible for revoking the authority (or license) of traitors found in the previous step. The simple revocation method (e.g., the license is appeared in Blacklist) may be evaded in the way of license forgery and tampering. Taking into account the difficulty in comparing cryptographic key forgery and license forgery, the key based revocation would be a more effective and secure manner.

ADVANTAGES

- This model is generic enough to apply anomaly detection for the abnormal to trace and revoke the traitors.
- The users are organized in different groups and given decryption keys based on role hierarchy in RBAC.
- A PHE is provide, in which they can encrypt and decrypt the data by specifying the RBAC policies to meet high-security

ARCHITECTURE

Architecture Diagram



ALGORITHM

RSA ALGORITHM

ENCRYPTION

Sender A does the following

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

- Sends the cipher text c to B.

DECRYPTION

- Recipient B does the following
- Alice can recover from by using her private key exponent via computing
- $m = c^{d}(\mathrm{mod}\ n)$
- Extracts the plaintext from the integer representative m.

KEY GENERATION

- Choose two distinct prime numbers p and q.

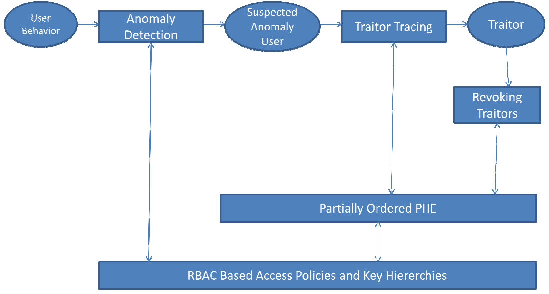
For security purposes, integer p and integer q should be chosen at random, and should be of similar bit-length.

- Compute n = pq.n is used as the modulus for both the public and private keys.
- Compute φ (n) = (p – 1) (q – 1), where φ is Euler's totient function.
- Choose an integer e such that 1 < e < φ (n) (n) and greatest common Divisor of (e, φ (n)) = 1; i.e., e and φ (n) are co-prime.
- E is released as the public key exponent.
- E having a short bit-length and small Hamming weight results in more efficient encryption.
- Determine d as:
- $d = e^{-1}\ (\mathrm{mod}\ \varphi(n))$
- ·D is the multiplicative inverse of e mod φ (n).
- This is more clearly stated as solve for d given (de) = 1 modφ(n)
- ·D is kept as the private key exponent.
- 6. By construction, d*e= 1 mod φ (n).The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret. (p, q, and φ(n) must also be kept secret because they can be used to calculate d.)

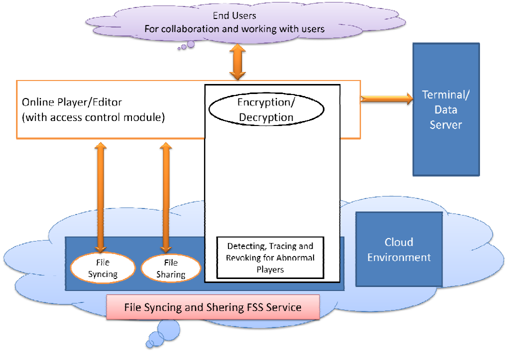
SYSTEM DESIGN

SYSTEM ARCHITECTURE DESIGN

We present a new FSS model for player abuse prevention and enhanced protection against unauthorized access. The proposed model uses the hierarchical role-based access control (H-RBAC) model, which is recognized for its support for simplified administration and scalability of collaboration and working with teams. Moreover, the design of this model is generic enough to support other access control policies, such as discretionary access control and multilevel security. We show such a cloud-based FSS model in the Fig. 4. This model that addresses and incorporates the afore-mentioned authorization requirements can be built using three types of components: **Anomaly detection:** 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. **Tracing traitors:** This 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 inthe player cannot be leaked in the tracing procedure. We call it 'black box tracing'. **Revoking traitors:** This is responsible for revoking the authority (or license) of traitors found in the previous step. The simple revocation method (e.g., the license is appeared in Blacklist) may be evaded in the way of license forgery and tampering. Taking into account the difficulty in comparing cryptographic key forgery and license forgery, the keybased revocation would be a more effective and secure manner. The above model may be developed in a non-cryptographic way, but the cryptographic technique can dramatically increase the difficulty of attackers and enhance the security of system. Therefore we will introduce a new cryptographic structure and construction into our FSS system model, as follows: **Key Hierarchy:** This is a partial-order structure in which all user's keys are organized in a hierarchy according to rolehierarchy in H-RBAC. In this way, we can use the partial order to manage these keys. **PHE Cryptosystem:** This is a new cryptosystem that enables the granting, usage tracking, and revoking of authorization. It is built on the key hierarchy described above, so that we call it the partially-ordered hierarchical encryption (PHE). In summary, two new modules are added into the existing FSS services (as shown in the dashed box of the Fig. 3): one is the monitor module for detecting, tracing, and revoking for abnormal players; another is the cryptographic module for encrypting and decrypting data. In our system model, the PHE cryptosystem might be deployed in the client side (e.g., running on the Client/Server model) or the cloud side (e.g., working on the virtual desktop in cloud) according to the requirement of practical applications. The traitor tracing and revocation mechanisms will be also realized on this model by monitoring and tracing the situation of every decoder.



We first describe a simple and general framework of file syncing and sharing service developed over the cloud computing platforms. As shown in the Fig. 3, this framework consists of three following entities: **FSS service:** provides users with the ability to remotely store their data and access the same cloud-based data. Enterprise or business class versions of FSS services provide these capabilities in a secure manner that gives IT oversight and control. **Online player/editor:** provides the ability to access this data from any location and any of their devices, including smart-phones and tablets, without having to go through a corporate VPN or firewall (shown in the middle module
in the figure). **End users:** The FSS service also provide the ability to share information with other users, both inside and outside the organization. This kind of FSS service could be built on the open-source cloud platforms, such as, OpenStack and CloudStack1, inwhich computing, networking and storage resources are integrated and managed as a unified system. These platforms provide a prefect interface with cloud service providers and tenants, but do not provide a direct interface with end users. As a more flexible and convenient way, online player/editor is developed
as the bridge between FSS service and end users. They may be built a lot of different ways, such as web service, virtual desktop, and client/server-based applications.


End Users
For collaboration and working with users
Online Player/Editor
(with access control module)
Encryption/ Decryption
Terminal/ Data Server
File Syncing
File Sharing
Detecting, Tracing and Revoking for Abnormal Players
Cloud Environment
File Syncing and Shering FSS Service

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.

FUTURE ENHANCEMENT

In our future work, we are planning to introduce a

- Comprehensive anomaly detection
- Using audit
- Pattern matching
- Risk assessment for identifying the suspected players.

REFERENCES

[1] f. r. institute, "personal data in the cloud: a global survey of consumer attitudes," http://www.fujitsu.com/downloads/ sol/fai/reports/fujitsu/personal-data-in-the-cloud.pdf, 2010.

[2] d. quick and k. r. choo, "google drive: forensic analysis of data remnants," *j. network and computer applications*, vol. 40, pp. 179– 193, 2014

[3] h. chung, j. park, s. lee, and c. kang, "digital forensic investigation of cloud storage services," *digital investigation*, vol. 9, no. 2, pp. 81–95, 2012.

[4] d. boneh and m. k. franklin, "an efficient public key traitor tracing scheme," in *crypto*, 1999, pp. 338–353.

[5] d. boneh, a. sahai, and b. waters, "fully collusion resistant traitor tracing with short ciphertexts and private keys," in *eurocrypt*, 2006, pp. 573–592.

[6] z. liu, z. cao, and d. s. wong, "traceable cp-abe: how to trace decryption devices found in the wild," *ieee trans. information forensics and security*, vol. 10, no. 1, pp. 55–68, 2015.

[7] d. boneh and m. k. franklin, “identity-based encryption fromthe weil pairing,” in *crypto*, 2001, pp. 213–229.

a. sahai and b. waters, “fuzzy identity-based encryption,” in *eurocrypt*, 2005, pp. 457–473.

[8] v. goyal, o. pandey, a. sahai, and b. waters, “attribute-based encryption for fine-grained access control of encrypted data,” in *acm conference on ccs*, 2006, pp. 89–98.

[9] r. ostrovsky, a. sahai, and b.waters, “attribute-based encryption with non-monotonic access structures,” in *acm conference on computer and communications security*, 2007, pp. 195–203.

[10] s. yamada, n. attrapadung, g. hanaoka, and n. kunihiro, “generic constructions for chosen-ciphertext secure attribute based encryption,” in *public key cryptography*, 2011, pp. 71–89.

[11] m. j. atallah, m. blanton, n. fazio, and k. b. frikken, “dynamic and efficient key management for access hierarchies,” *acm trans. inf. syst. secur.*, vol. 12, no. 3, 2009.

[12] m. blanton and k. b. frikken, “efficient multi-dimensional key management in broadcast services,” in *esorics*, 2010, pp. 424–40.

[13] d. boneh, x. boyen, and e.-j. goh, “hierarchical identity based encryption with constant size ciphertext,” in *advances in cryptology (eurocrypt’2005)*, vol. 3494 of lncs, 2005, pp. 440–456.

[14] s. berkovits, “how to broadcast a secret,” in *advances in cryptology (eurocrypt’91)*, vol. 547 of lncs. springer-verlag, 1991, pp. 536–541.

.