

D-Manager

KishoreJ¹, Nethaji N², Vimalchand V³ and C.Radhakrishnan⁴

¹Kongunadu College of Engineering and Technology/ CSE, Trichy, Tamilnadu, India
Email: kishoremaddy56@gmail.com

²⁻³ Kongunadu College of Engineering and Technology/ CSE, Trichy, Tamilnadu, India
Email: nethaji3377@gmail.com, vimal98lucas@gmail.com

⁴ Kongunadu College of Engineering and Technology/ AP -CSE, Trichy, Tamilnadu, India
Email: radhamayil@gmail.com

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.

Index Terms— File Syncing and Sharing, Partially-ordered Hierarchical Encryption.

I. 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.

Characteristics

Agility

It is for organizations may be improved, as cloud computing may increase user's flexibility with re-provisioning, adding, or expanding technological infrastructure resources.

Location Independence

It enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). Infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect to it from anywhere.

Maintenance

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places (e.g., different work locations, while travelling, etc.).

Performance

Performance is monitored by IT experts from the service provider, and consistent and loosely coupled architectures are constructed using web service as the system interface.

Reliability

Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

Scalability

Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, OS and cloud providers), without users having to engineer for peak loads.

Service Models

Infrastructure as a Service (IaaS)

Infrastructure as a service(IaaS) refers to online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. 3

Platform as a Service (PaaS)

In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming-language execution environment, Database and web server. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

Deployment models

Private cloud : Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, hosted either internally or externally.

Public cloud : A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free.

Hybrid cloud: Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models.

II. EXISTING SYSTEMS

Bring-your-own-device (BYOD) policies and 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.

III. PROPOSED WORK

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.1. 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.

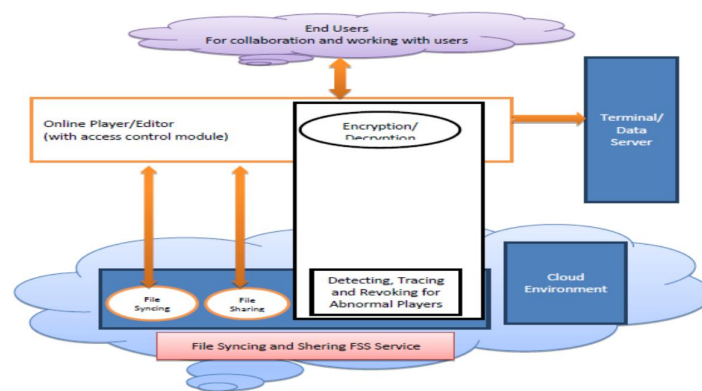


Fig 1. System Architecture

IV. IMPLEMENTATION ALGORITHM

A. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a subset of the Rijndael cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.

For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

B. 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 decrypt the cipher text and output the plaintext M.
5. The data holder conducts this process to gain the plaintext of stored data at CSP.

C. Output: Encrypted and Decrypted File.

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
$$m = c \pmod{n}$$
- 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.
$$\text{Compute } \phi(n) = (p-1)(q-1), \text{ where } \phi \text{ is Euler's totient function.}$$
- Choose an integer e such that $1 < e < \phi(n)$ and greatest common Divisor of (e, $\phi(n)$) = 1; i.e., e and $\phi(n)$ are co-prime.
- E having a short bit-length and small Hamming weight results in more efficient encryption.
$$\text{Determine } d \text{ as: } d = e^{-1} \pmod{\phi(n)}$$
- D is the multiplicative inverse of e mod $\phi(n)$.
- This is more clearly stated as solve for d given $(de) = 1 \pmod{\phi(n)}$
- D is kept as the private key exponent.

V. CONCLUSIONS

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.

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*, pp. 338–353, 1999.
- [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 from the weil pairing," in *crypto*, pp. 213–229, 2001.
- [8] A. Sahai and b. Waters, "fuzzy identity-based encryption," in *eurocrypt*, pp. 457–473, 2005.
- [9] 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*, pp. 89–98, 2006.
- [10] R. Ostrovsky, A. Sahai, and B. Waters, "attribute-based encryption with non-monotonic access structures," in *acm conference on computer and communications security*, pp. 195–203, 2007.
- [11] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "generic constructions for chosen-ciphertext secure attribute based encryption," in *public key cryptography*, pp. 71–89, 2011.
- [12] 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.
- [13] M. Blanton and k. B. Frikken, "efficient multi-dimensional key management in broadcast services," in *esorics*, pp. 424–440, 2010.
- [14] 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*, pp. 440–456, 2005.
- [15] S. Berkovits, "how to broadcast a secret," in *advances in cryptology (eurocrypt'91)*, vol. 547 of *lncs*. Springer-verlag, pp. 536–541, 1991.
- [16] A. Fiat and m. Naor, "broadcast encryption," in *advances in cryptology (crypto'93)*, vol. 773 of *lncs*. Springer-verlag, pp. 480–491, 1994.
- [17] D. Padmini Bai and P. Preethi, "Security Enhancement of Health Information Exchange Based on Cloud Computing System", *International Journal of Scientific Engineering and Research*, pp. 79-82, Volume 4 Issue 10, October 2016.
- [18] Yogapriya, J., Saravanabhavan, C., Asokan, R., Vennila, I., Preethi, P., Nithya, B. 2018. A Study of Image Retrieval System Based on Feature Extraction, Selection, Classification and Similarity Measurements. *Journal of Medical Imaging and Health Informatics*, 8(3), 479-484.
- [19] Saravanan Kumarasamy and Dr.R.Asokan An Efficient Detection Mechanism for Distributed Denial of Service (DDoS) Attack. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, Vol.1, No.5, December 2011.
- [20] Thillaiarasu, N. and ChenturPandian, S., 2017. A novel scheme for safeguarding confidentiality in public clouds for service uses of cloud computing. *Cluster Computing*, pp.1-10.
- [21] Dr.Raghavendran P.S., Dr.Asokan R., Vishnupriya M., Enhancing the security against Flooding Attack in MANET for Medical Application, *Asian Journal of Research in Social Sciences and Humanities*, Vol. 6, Issue 6, 2016.
- [22] R.Pavithra, Dr.R.Asokan, K.Baskar, Improving Privacy And Dynamic Updation Using Ranked Search Over Outsourced Cloud Data, *International Research Journal of Engineering and Technology (IRJET)*, Volume: 03 Issue: 10, Oct-2016.
- [23] Saravanan, K; Asokan, R; Venkatachalam, K., Neuro- Fuzzy Based Clustering of Distributed Denial of Service (DDoS) Attack Detection Mechanism, *International Information Institute (Tokyo). Information; Koganei Vol. 16, Iss. 11, (Nov 2013)*.
- [24] Vellingiri, J.; Balambigai, S.; Saravanan, K.; Asokan, R., Secure Real Time Web Based Electrocardiogram Monitoring System for Improved Healthcare, *Journal of Medical Imaging and Health Informatics*, Volume 6, Number 3, June 2016, pp. 774-778(5).
- [25] M. Bhuvaneshwari, Dr. J. Yogapriya, Decentralized, Energy-Efficient, Low Latency and Less Homogeneous Settings based Workload Management in Enterprise Clouds, *International Journal of Scientific Engineering and Research (IJSER)*, Volume 4 Issue 10, October 2016.