International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

SECURE AND EFFICIENT FILE SHARING AND SHARED OWNERSHIP IN CLOUD SYSTEMS

Preethy Roy[1], Shabiya M.I[2]

[1]M.Tech student Computer Science and Engineering
[2]Asst.Professor, Department of Computer Science and Engineering, Indira Gandhi Institute of Engineering and Technology, Nellikuzhi, Kerala, India

---

Abstract - *Cloud storage platforms promise a convenient way for users to store large amount of data and also share the data to others. Everyone can stores his or her data into cloud, That is, each file stored in the cloud is owned by a single user, who can decide whether to grant or deny any access request to that file. The individual ownership of files is not suitable for numerous cloud-based applications. In this paper designed for sharing the ownership of the files, that means if a user upload a file in to the cloud the he can share the ownership to other owners. The shared ownership of the files can be done by using the concept of commune and comrade. Suppose a user shared a file to others, so the person who receive the access request he accept the permission at this time he became the owner of the file. So owner can perform read write operation in that file. Suppose an external user can want to see the file, here introduce a novel notion of shared ownership where n users jointly own a file then each file access request must granted by a pre-arranged threshold of t owners of that files. Security one of the main concerns in data that stored in cloud. In order to provide security data outsourced after the encryption. Here the AES -128 bit algorithm used for encryption. This system provides more security to cloud systems, the performance of the of the system discussed below.*

***Key Words*: Cloud security, CPS, Commune, Comrade, shared ownership**

1 .INTRODUCTION

Cloud-assisted Cyber-Physical Systems have a wide range of applications, ranging from healthcare to smart electricity grid and military, and so on. The cloud system that provides the enormous storage space to the users, so users can stores large amount of data in to cloud. In order to provide the security on stored data the data is encrypted before it is outsourcing. In such systems, client devices can be used to access the relevant services from/via the cloud. There are large numbers of studies that focusing on the security of cloud data. The existing system is Identity-Based Encryption (IBE) scheme that can be used to facilitate secure data sharing. Thus, in this existing Identity-Based Authenticated Data Sharing (IBADS) protocol to provide data security and mutual authentication of cloud stored data in cyber-physical cloud environments. But the existing system it does not supports the concept of shared ownership.

There are large numbers of security challenges for such cloud environment, such as the following:

- Mutual Authentication: Mutual Authentication is one of the most fundamental security attributes required in cyber physical systems. Assume that the server may be dishonest or not fully trusted. In the above case, both client and server first complete the authorization process by verifying the authenticity of each other, by exchanging any confidential data over public networks.
- Anonymity: This attribute allows the hiding of the identity of the client or user.
- Password protection: Password is one of the main challenging attribute in cyber physical cloud systems specifically, the client or user generally uses low entropy password to facilitate easy memorization, and such passwords are more vulnerable to password guessing attacks.
- Data integrity and confidentiality: A secure protocol should provide a strong data integrity and confidentiality for every transmitted files across the cloud. Data integrity assures the received message has not been modified, and confidentiality ensures that only authorized users access the data.

Secure and efficient file storage and file sharing in cloud via authenticated physical devices is difficult to achieve in a cyber-physical cloud environment, because of diversity devices access the services and data. But in this existing studies that does not support sharing of ownership, that means a data owner first create a file then he or she upload the file after performing the encryption in to the cloud, also he or she share the ownership request and corresponding keyword of the file to the other authorized users. If an authorized get the ownership request, then he accept the ownership request, now he is owner of that file. The decrypted file can be opened by using the keyword. After receiving the file the user can performs the read and write operation in to that file.. Only the shared users can view the file, other authorized users cannot see the file. Suppose an external user can want to see the file, here introduce a novel notion of shared ownership where n users jointly own a file then each file access request must granted by a pre-arranged threshold of t owners of that files.

1.1 Objective

The proposed protocol provides mutual authentication, and essential features such as client registration, login, mutual authentication, password renewal. The protocol also ensures user anonymity.

- Once the physical devices are authenticated, the next phase is secure end-to-end communication.
- The data encrypted based on AES algorithm, so it provides more security than other encryption algorithm.
- The proposed system that supports the shared ownership concept, so many authorized users can access the file.
- If there are n users owned a file then each file request access is granted by a predefined threshold of t owners, here the value of threshold is set as (n+1)/2. Here n is the number of file owners.
- The proposed protocol that reduce the communication and computational cost than other systems.:

1.2 Scope

The Proposed system is designed for supporting shared ownership in cloud based applications and collabrations.

2. RELATEDWORK

There have been a number of studies that are focusing on the security of CPS in recent years [1], [2], [3]. For example, in 2012, Rajkumar [4] presented a number of technical researches and challenges associated with CPS. Then later the Rajhans et al. [5] proposed an architectural framework for CPS, using structural and semantic mappings to assure consistency of cloud data. Shortly there after, a modular design method was developed by Demirel et al.[6] to optimize packet forwarding policies and control commands for secure data transmissions More recently, in 2017, Shu et al. [7] proposed an architecture for CPS for complex industrial applications.

2.1 CYBER-PHYSICAL CLOUD COMPUTING ARCHITECTURE

Cloud computing architecture refers to the components and sub components that required for cloud computing. These components are typically consist of a front end platform (fat client, thin client, mobile device), back end platforms (servers, storage), a cloud based delivery, and a network (Internet, Intranet, Inter cloud). By using these components make up the cloud computing architecture.

One such architecture is illustrated in Figure 2.1, where the mobile device is used to denote the client device. The mobile device is connects to the mobile network by using base stations such as base transceiver station, access point, or satellite. When a mobile user requests for some tasks to be processed on that data, information (e.g., identity and location) is handover to the central processors connected to the servers for processing the tasks.

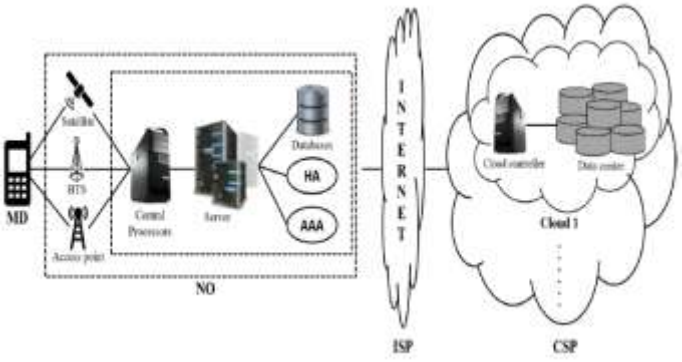

Fig 2.1 Architecture of Cyber Physical System

Despite the popularity of cloud computing and its variants, security is one of the main concerns. The Identity-based encryption (IBE) scheme is a potential cryptographic solutions that is used to facilitate secure data sharing across various systems. Thus, in this paper IBE, construct an identity-based authentic data sharing (IBADS) protocol to provide data security and sharing in cyber-physical cloud environments. For the rest of the paper, mobile devices are considered as the client devices as such devices generally have more computational and storage capabilities compared to other Internet-of-Things (IoT) devices.

Formal structure of IBE scheme consists of four independent algorithms, i.e., Setup, Extract, Encrypt and Decrypt:

- Setup: This algorithm Setup takes a security parameter k as input, and generates params, known to all users, and MSK, only known to the PKG.
- Extract: This algorithm Extract takes user identity ID, params and MSK as inputs, and generates a private key SKID for the user ID.
- Encrypt: This algorithm Encrypt takes params, a message M and recipient's identity ID as inputs, and produces a cipher text CT.
- Decrypt: This algorithm Decrypt takes CT and SKID as inputs, and produces either M.

Thus in this existing system proposes a lightweight identity-based authenticated data sharing protocol to provide secure data sharing among the geographically dispersed physical devices . But the existing system doesn't support the shared ownership in cloud.it designed for sharing the message between the data owner and the data consumer.it doesn't provide any access privileges to the data consumer. In order to provide the concept of shared

ownership it uses 2 concepts namely commune and comrade.

3. PROPOSED WORK

In this paper designed for sharing the ownership of the files, that means if a user upload a file in to the cloud the he can share the ownership to other owners. The shared ownership of the files can be done by using the concept of commune and comrade. Suppose a user shared a file to others, so the person who receive the access request he accept the permission at this time he became the owner of the file. So owner can perform read write operation in that file. Suppose an external user can want to see the file, here introduce a novel notion of shared ownership where n users jointly own a file then each file access request must granted by a pre-arranged threshold of t owners of that files. Security one of the main concerns in data that stored in cloud. In order to provide security data outsourced after the encryption. Here the AES -128 bit algorithm used for encryption. Commune, this concept used for secure file dispersal and collusion-resistant secret sharing to ensure that all access grants in the cloud require the support of an agreed threshold of owners. While Comrade is used to reach consensus on access control decision.

3.1 OVERVIEW OF COMMUNE

Before describing Commune, consider the following observations:

- Observation 1: In Commune's files cannot be stored on a single user account.

Following the discussion regarding the centralized enforcement, a single user must not be charged with making unilateral grant and deny decisions. Otherwise, the user may abuse his rights and take access control decisions. The solution is where a file is encrypted and the cipher text is stored on a single account, allows that account holder to, unilaterally deny read access to the cipher text. If the cipher text cannot be read, any mechanism to distribute or recover the encryption key is of no help. Then argue, therefore, that Commune cannot use a centralized repository owned by a single user because the repository owner can unilaterally grant or deny access to the files stored there in. Our alternative is to use a "shared repository", which is an abstraction built on top of the owners" personal accounts on S.

- Observation 2. Commune cannot support in-place writing.

If Commune were to allow in-place writing, then users who are granted write access could overwrite a file with "garbage". This would equate to granting users the right to unilaterally delete the file, thus nullifying our efforts to prevent such scenarios. A standard alternative to in-place writing is to introduce "copy-on-write" mechanisms where by a new file is created upon each file write operation.

- Observation 3. Commune cannot prevent users from disseminating a file or a key through an out-of-band channel.

3.2 OVERVIEW OF COMRADE

The main idea behind Comrade is that a setting a threshold value can instantiate a trusted third party that can evaluate user credentials against owners access policies in a trustworthy manner. Differently from Commune, however, Comrade needs the cloud to be "shared-ownership aware" and enforce the policies defined by the smart contract. To perform an action a on file F in Comrade, user Ui proceeds as follows. Ui issues a standard access request to the cloud storage. The owner contract also manages the users. Users can join the system by sending a request to the owner contract.

4. CONCLUSION

Cloud-assisted cyber-physical systems have broad applications, ranging from healthcare to smart electricity grid to military, and so on. The cloud promises a convenient way for users can store files and also share files and effortlessly engage in collaborations, it still retains the notion of individual file ownership. That is, each file stored in the cloud is owned by a single user, so the only single user can unilaterally decide whether to grant or deny any access request to that file. However, the individual ownership is not suitable for numerous cloud-based applications. Secure and efficient file storage and sharing via authenticated physical devices remain challenging in a cyber-physical cloud environment, because of diversity of devices used to access the services and data. In contrast to individual ownership, here introduce a novel notion of shared ownership.it supports the following concept, where n users jointly own a file and each file access request must be granted by a pre-arranged threshold of t owners. It uses AES cryptographic algorithm for encrypting the data. The proposed system provides more security and efficiency.

REFERENCES

[1] Qiang Liu, Jiafu Wan, and Keliang Zhou. Cloud manufacturing service system for industrial-cluster-oriented application. 15(3):373–380, 2014.

[2] Daqiang Zhang, Jiafu Wan, Qiang Liu, Xin Guan, and Xuedong Liang. A taxonomy of agent technologies for ubiquitous computing environments. KSII Transactions on Internet and Information Systems (TIIS), 6(2):547–565, 2012.

[3] Jiafu Wan, Hehua Yan, Di Li, Keliang Zhou, and Lu Zeng. Cyberphysical systems for optimal energy management scheme of autonomous electric vehicle. The Computer Journal, 56(8):947–956, 2013.

[4] Ragunathan Rajkumar. A cyber–physical future. Proceedings of the IEEE, 100(Special Centennial Issue):1309–1312, 2012.

[5] Akshay Rajhans, Ajinkya Bhave, Ivan Ruchkin, Bruce H Krogh, David Garlan, Andre Platzer, and Bradley Schmerl. Supporting heterogeneity in ´ cyber-physical systems architectures. IEEE Transactions on Automatic Control, 59(12):3178–3193, 2014.

[6] Burak Demirel, Zhenhua Zou, Pablo Soldati, and Mikael Johansson. Modular design of jointly optimal controllers and forwarding policies for wireless control. IEEE Transactions on Automatic Control, 59(12):3252– 3265, 2014.

[7] Zhaogang Shu, Jiafu Wan, Daqiang Zhang, and Di Li. Cloud-integrated cyber-physical systems for complex industrial applications. Mobile Networks and Applications, 21(5):865–878, 2016.

[8] Catherine Wise, Carsten Friedrich, Surya Nepal, Shiping Chen, and Richard O Sinnott. Cloud docs: Secure scalable document sharing on public clouds. In 2015 IEEE 8th International Conference on Cloud Computing, pages 532–539. IEEE, 2015.

[9] Deng-Guo Feng, Min Zhang, Yan Zhang, and Zhen Xu. Study on cloud computing security. Journal of software, 22(1):71–83, 2011.

[10] Tsz Hon Yuen, Ye Zhang, Siu Ming Yiu, and Joseph K Liu. Identitybased encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks. In European Symposium on Research in Computer Security, pages 130–147. Springer, 2014