ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

Proxy – Oriented Data Uploading and Remote Data Reliability Checking in Multi Cloud

S.SARANYA [1], V.MATHESWARAN [2]

1. P.G. Student, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India

2. Assistant Professor, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India

ABSTRACT:

More and more clients would like to store their data to public cloud servers (PCSs) along with the rapid development of cloud computing. New security problems have to be solved in order to help more clients process their data in public cloud. When the client is restricted to access PCS, he will delegate its proxy to process his data and upload them. On the other hand, remote data integrity checking is also an important security problem in public cloud storage. It makes the clients check whether their outsourced data are kept intact without downloading the whole data. From the security problems, we propose a novel proxy-oriented data uploading and remote data integrity checking model in identity-based public key cryptography: identity-based proxy-oriented data uploading and remote data integrity checking in public cloud (ID-PUIC). We give the formal definition, system model, and security model. Then, a concrete ID-PUIC protocol is designed using the bilinear pairings. The proposed ID-PUIC protocol is provably secure based on the hardness of computational Diffie–Hellman problem. Our ID-PUIC protocol is also efficient and flexible. Based on the original client's authorization, the proposed ID-PUIC protocol can realize private remote data integrity checking, delegated remote data integrity checking, and public remote data integrity checking.

1. INTRODUCTION

Along with the rapid development of computing and communication technique, a great deal of data are generated. These massive data needs more strong computation resource and greater storage space. Over the last years, cloud computing satisfies the application requirements and grows very quickly. Essentially, it takes the data processing as a service, such as storage, computing, data security, etc. By using the public cloud platform, the clients are relieved of the burden for storage management, universal data access with independent geographical locations, etc. Thus, more and more clients would like to store and process their data by using the remote cloud computing system. In public cloud computing, the clients store their massive data in the remote public cloud servers. Since the stored data is outside of the control of the clients, it entails the security risks in terms of confidentiality, integrity and availability of data and service. Remote data integrity checking is a primitive which can be used to convince the cloud clients that their data are kept intact. In some special cases, the data owner may be restricted to access the public cloud server, the data owner will delegate the task of data processing and uploading to the third party, for example the proxy. On the other side, the remote data integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices. Thus, based on identity-based public cryptography and proxy public key cryptography, we will study ID-PUIC protocol.

A. Motivation

In public cloud environment, most clients upload their data to PCS and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen. If the manager is suspected of being involved into the commercial fraud, he will be taken away by the police. During the period of investigation, the manager will be restricted to access the network in order to guard against collusion. But, the manager's legal business will go on during the period of investigation. When a large of data is generated, who can help him process these data? If these data cannot be processed just in time, the manager will face the lose of economic interest. In order to prevent the case happening, the manager has to delegate the proxy to process its data, for example, his secretary. But, the manager will not hope others have the ability to perform the remote data integrity checking. Public checking will incur some danger of leaking the privacy. For example, the stored data volume can be detected by the malicious verifiers. When the uploaded data volume is confidential, private remote data integrity checking is necessary. Although the secretary has the ability to process and upload the data for the manager, he still cannot check the manager's remote data integrity unless he is delegated by the manager. We call the secretary as the proxy of the manager.

In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management. When the manager delegates some entities to perform the remote data integrity checking, it will incur considerable overheads since the verifier will check the certificate when it checks the remote data integrity. In PKI, the considerable overheads come from the heavy certificate verification, certificates generation, delivery, revocation, renewals, etc. In public cloud computing, the end devices may have low computation capacity, such as mobile phone, ipad, etc. Identity-based public key cryptography can eliminate the complicated certificate management. In order to increase the efficiency, identitybased proxy-oriented data uploading and remote data integrity checking is more attractive. Thus, it will be very necessary to study the ID-PUIC protocol.

In public cloud, this paper focuses on the identity-based proxy-oriented data uploading and remote data integrity checking. By using identity-based public key cryptology, our proposed ID-PUIC protocol is efficient since the certificate management is eliminated. ID-PUIC is a novel proxy-oriented data uploading and remote data integrity checking model in public cloud. We give the formal system model and security model for ID-PUIC protocol. Then, based on the bilinear pairings, we designed the first concrete ID-PUIC protocol. In the random oracle model, our designed ID-PUIC protocol is provably secure. Based on the original client's authorization, our protocol can realize private checking, delegated checking and public checking.

2. RELATED WORKS

There exist many different security problems in the cloud computing [1], [2]. This paper is based on the research results of proxy cryptography, identity-based public key cryptography and remote data integrity checking in public cloud. In some cases, the cryptographic operation will be delegated to the third party, for example proxy. Thus, we have to use the proxy cryptography. Proxy cryptography is a very important cryptography primitive. In 1996, Mambo et al. proposed the notion of the proxy cryptosystem [3]. When the bilinear pairings are brought into the identity-based cryptography, identity-based cryptography becomes efficient and practical. Since identitybased cryptography becomes more efficient because it avoids of the certificate management, more and more experts are apt to study identity-based proxy cryptography.

In 2013, Yoon et al. proposed an ID-based proxy signature scheme with message recovery [4]. Chen et al. proposed a proxy signature scheme and a threshold proxy signature scheme signature scheme from the Weil pairing [5]. By combining the proxy cryptography with encryption technique, some proxy re-encryption schemes are proposed. [6] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC).. Guo et al. presented a non-interactive CPA (chosen-plaintext attack)-secure proxy re-encryption scheme, which is resistant to collusion attacks in forging re-encryption keys [7]. Many other concrete proxy re-encryption schemes and their applications are also proposed [8]–[10].

In public cloud, remote data integrity checking is an important security problem. Since the clients' massive data is outside of their control, the clients' data may be corrupted by the malicious cloud server regardless of intentionally or unintentionally. In order to address the novel security problem, some efficient models are presented. In 2007, Ateniese et al. proposed provable data possession (PDP) paradigm.

In PDP model, the checker can check the remote data integrity without retrieving or downloading the whole data. PDP is a probabilistic proof of remote data integrity checking by sampling random set of blocks from the public cloud server, which drastically reduces I/O costs. The checker can perform the remote data integrity checking by maintaining small metadata. After that, some dynamic PDP model and protocols are designed. Following Ateniese et al.'s pioneering work, many remote data integrity checking models and protocols have been proposed. In 2008, proof of retrievability (POR) scheme was proposed by Shacham et al. POR is a stronger model which makes the checker not only check the remote data integrity but also retrieve the remote data. Many POR schemes have been proposed. On some cases, the client may delegate the remote data integrity checking task to the third party. In cloud computing, the third party auditing is indispensable. By using cloud storage, the clients can access the remote data with independent geographical locations. The end devices may be mobile

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

and limited in computation and storage. Thus, efficient and secure ID-PUIC protocol is more suitable for cloud clients equipped with mobile end devices. From the role of the remote data integrity checker, all the remote data integrity checking protocols are classified into two categories: private remote data integrity checking and public remote data integrity checking. In the response checking phase of private remote data integrity checking, some private information is indispensable. On the contrary, private information is not required in the response checking of public remote data integrity checking. Specially, when the private information is delegated to the third party, the third party can also perform the remote data integrity checking. In this case, it is also called delegated checking.

2.1 EXISTING SYSTEM

In public cloud environment, most clients upload their data to PCS and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen. If the manager is suspected of being involved into the commercial fraud, he will be taken away by the police. During the period of investigation, the manager will be restricted to access the network in order to guard against collusion. But, the manager's legal business will go on during the period of investigation. If these data cannot be processed just in time, the manager will face the lose of economic interest. In order to prevent the case happening, the manager has to delegate the proxy to process its data, for example, his secretary. But, the manager will not hope others have the ability to perform the remote data integrity checking. Public checking will incur some danger of leaking the privacy. For example, the stored data volume can be detected by the malicious verifiers. When the uploaded data volume is confidential, private remote data integrity checking is necessary. Although the secretary has the ability to process and upload the data for the manager, he still cannot check the manager's remote data integrity unless he is delegated by the manager. Here the secretary is called as the proxy of the manager. . In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management. When the manager delegates some entities to perform the remote data integrity checking, it will incur considerable overheads since the verifier will check the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

certificate when it checks the remote data integrity.

2.1.1 Disadvantages of Existing System:

- Public checking will incur some danger of leaking the privacy.
- Less Efficiency.
- Security level is low
- In PKI, the considerable overheads come from the heavy certificate verification, certificates generation, delivery, revocation, renewals, etc.
- In public cloud computing, the end devices may have low computation capacity, such as mobile phone, ipad, etc.

2.2 PROPOSED SYSTEM

The proposed system is based on the research results of proxy cryptography, identity-based public key cryptography and remote data integrity checking in public cloud. In public cloud, it focuses on the identity-based proxy-oriented data uploading and remote data integrity checking. By using identity-based public key cryptology, our proposed ID-PUIC protocol is efficient since the certificate management is eliminated. ID-PUIC is a novel proxy-oriented data uploading and remote data integrity checking model in public cloud. It gives the formal system model and security model for ID-PUIC protocol. Then, based on the bilinear pairings, the first concrete ID-PUIC protocol has been designed.

In the random oracle model, designed ID-PUIC protocol is provably secure. Based on the original client's authorization, this protocol can realize private checking, delegated checking and public checking. An efficient ID-PUIC protocol for secure data uploading and storage service in public clouds is designed.

Bilinear pairings technique makes identity-based cryptography practical. This protocol is built on the bilinear pairings.

2.2.1 Advantages of Proposed System:

- High Efficiency.
- Improved Security.
- The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis.
- On the other hand, the proposed ID-PUIC protocol can also realize private remote data integrity checking, delegated remote data integrity checking and public

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

remote data integrity checking based on the original client's authorization.

- Decrease the Overhead

3. SYSTEM DESCRIPTION

Advances in networking and computing technologies have prompted many organizations to outsource their storage needs on demand. This new economic and computing paradigm is commonly referred to as cloud storage. It brings appealing benefits including relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, Software, and personnel maintenances, etc. However, there are barriers that hinder migration to the cloud. One of the main barriers is that, due to lack of physical control over the outsourced data, a cloud user may worry about whether her data are kept as expected. If the cloud user is a company, apart from the risk of remote malicious attacks on the cloud, the traditional concerns posed by malicious company insiders are now supplemented by the even more hazardous threat of malicious outsiders who are given the power of insiders. Convincing cloud users that their data are intact is especially vital when users are companies. Remote data possession checking (RDPC) is a primitive designed to address this issue. RDPC allows a client that has stored data at a public cloud server (PCS) to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. In order to achieve secure RDPC implementations, Ateniese et al. proposed a provable data possession (PDP) paradigm and designed two provably-secure PDP3 schemes based on the difficulty of large integer factoring. They refined the original paradigm and proposed a dynamic PDP scheme in but their proposal does not support the insert operation. In order to solve this problem, Erway et al. proposed a full-dynamic PDP scheme by employing an authenticated flip table. Following Ateniese et al.'s pioneering work, researchers devoted great efforts to RDPC with extended models and new protocols. One of the variations is the proof of retrievability (POR), in which a

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

data storage server cannot only prove to a verifier that he is actually storing all of a client's data, but also it can prove that the users can retrieve them at any time. This is stronger than the regular PDP notion. Shacham presented the first POR schemes with provable security. The state of the art can be found in but few POR protocols are more efficient than their PDP counterparts. The challenge is to build POR systems that are both efficient and provably secure. Note that one of benefits of cloud storage is to enable universal data access with independent geographical locations. This implies that the end devices may be mobile and limited in computation and storage. Regular RDPC protocols are more suitable for cloud users equipped with mobile end devices.

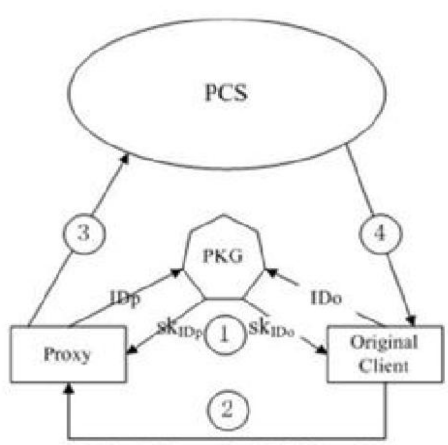

Fig.1 System Architecture

3.1 MODULE DESCRIPTION

- Original Client Module
- Public Cloud Server Module
- Proxy Module
- Key Generation Center (KGC) Module

ORIGINAL CLIENT

An entity, which has massive data to be uploaded to PCS by the delegated proxy, can perform the remote data integrity checking.

PCS (PUBLIC CLOUD SERVER)

An entity, which is managed by cloud service provider, has significant storage space and computation resource to maintain the clients' data.

PROXY

An entity, which is authorized to process the Original Client's data and upload them, is selected and authorized by Original Client. When Proxy satisfies the warrant mω which is signed and issued by Original Client, it can process and upload the original client's data; otherwise, it cannot perform the procedure.

KGC (KEY GENERATION CENTER)

An entity, when receiving an identity, it generates the private key which corresponds to the received identity.

4. CONCLUSION

Favorable solutions to ensure data privacy must employ flexible data perturbation methods that provide control over the tradeoff between the privacy guarantee and the utility of the query results. Prevent dynamic data integrity among applications hosted by different cloud systems. Proxy services are implemented to maintain the authentication and initially provide support for simple use cases, later progressing to more complex use cases. It formalizes ID-PUIC's system model and security model. Then, the first concrete ID-PUIC protocol is designed by using the bilinear pairings technique. The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis. On the other hand, the proposed ID-PUIC protocol can also realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking based on the original client's authorization.

4.1 FUTURE ENHANCEMENT

The client file has been modified to clients does not show what modification is done in client file by server, if the user need to know the modification only way to download the corresponding file. In future will show what modification is done in the client file by server to the client.

The user can view their file details such as upload files, download files. Modification files can view through accessing with the help of mobile.

REFERENCES

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. E98-B, no. 1, pp. 190–200, 2015.

[2] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.

[3] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in Proc. CCS, 1996, pp. 48–57.

[4] E.-J. Yoon, Y. Choi, and C. Kim, "New ID-based proxy signature scheme with

message recovery," in Grid and Pervasive Computing (Lecture Notes in Computer Science), vol. 7861. Berlin, Germany: Springer- Verlag, 2013, pp. 945–951.

[5] B.-C. Chen and H.-T. Yeh, "Secure proxy signature schemes from the weil pairing," J. Supercomput., vol. 65, no. 2, pp. 496–506, 2013.

[6] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[7] H. Guo, Z. Zhang, and J. Zhang, "Proxy re-encryption with unforgeable re-encryption keys," in Cryptology and Network Security (Lecture Notes in Computer Science), vol.8813. Berlin, Germany: Springer-Verlag, 2014, pp.20-33.

[8] E. Kirshanova, "Proxy re-encryption from lattices," in Public-Key Cryptography (Lecture Notes in Computer Science), vol. 8383. Berlin, Germany: Springer-Verlag, 2014, pp. 77–94.

[9] P. Xu, H. Chen, D. Zou, and H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage," Chin. Sci. Bull., vol. 59, no. 32, pp. 4201–4209, 2014.

[10] S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, and K. Matsuura, "Re-encryption verifiability: How to detect malicious activities of a proxy in proxy re-encryption," in Proc. CT-RSA Conf., vol. 9048. 2015, pp. 410–428.