

Remote Data Identity-Based Integrity Checking and Data Uploading in Public Cloud

¹Dr. C. Bhuvaneshwari, ²S. Daisy Fatima Mary and ³N. Rajkumar,
¹Assistant Professor & Head, ^{2,3}Guest lecturer,
^{1,2,3}Government Arts and Science College, Thiruvannainallur, 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 in fact 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.

Keyword: Cloud, Clients, Diffie–Hellman, Proxy, Security

I. RELATED WORKS

Paper [1, 2] 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. Chen *et al.* proposed a proxy signature scheme and a threshold proxy signature scheme from the Weil pairing [3]. 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 [11]. 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 [12]–[15].

II. EXISTING SYSTEM

In public cloud environment, most clients upload their data to Public Cloud Server (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 loss 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.

Disadvantages of Existing System

1. In PKI, the considerable overheads come from the heavy certificate verification, certificates generation, delivery, revocation, renewals, *etc.*
2. In public cloud computing, the end devices may have low computation capacity, such as mobile phone, ipad, *etc.*

III. PROPOSED SYSTEM

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 cryptography, 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.

Advantages of Proposed System

1. The concrete ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis

IV. SYSTEM ARCHITECTURE

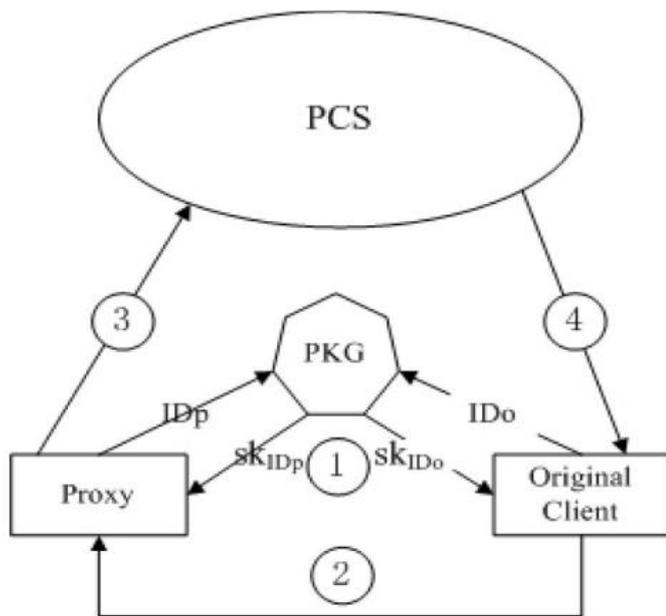


Fig. 1. Architecture of our ID-DPDP protocol.

MODULES

1. Original Client Module
2. Public Cloud Server Module
3. Proxy Module
4. Key Generation Center (KGC) Module

Module Description

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 m_0 , 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.

V. RESULT AND DISCUSSION

This paper proposes the novel security concept of ID-PUIC in public cloud and formalizes ID-PUIC's system model and security model. 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. 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.

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] X. Liu, J. Ma, J. Xiong, T. Zhang, and Q. Li, "Personal health records integrity verification using attribute based proxy signature in cloud computing," in *Internet and Distributed Computing Systems (Lecture Notes in Computer Science)*, vol. 8223. Berlin, Germany: Springer-Verlag, 2013, pp. 238–251.
- [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.
- [11] G. Ateniese et al., "Provable data possession at untrusted stores," in *Proc. CCS*, 2007, pp. 598–609.
- [12] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proc. SecureComm*, 2008, Art. ID 9.
- [13] C. C. Erway, A. K p c , C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. CCS*, 2009, pp. 213–222.
- [14] E. Esiner, A. K p c , and  .  zkasap, "Analysis and optimization on FlexDPDP: A practical solution for dynamic provable data possession," *Intelligent Cloud Computing (Lecture Notes in Computer Science)*, vol. 8993. Berlin, Germany: Springer-Verlag, 2014, pp. 65–83.
- [15] E. Zhou and Z. Li, "An improved remote data possession checking protocol in cloud storage," in *Algorithms and Architectures for Parallel Processing (Lecture Notes in Computer Science)*, vol. 8631. Berlin, 2014, pp. 611–617.
- [16] Germany: Springer-Verlag, 2014, pp. 611–617.