International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

AWS Cloud Based Data Integrity Checking and Identity-Based Proxy-Oriented Data Management

KORIBILLI JAYAPRAKASH NAIDU 1, V. SRINIVASA RAO

1Student,Dept Of CSE , Dadi institute of Engg & Tech,Anakapalli,vizag dist.

2 Associate Professor Dept Of CSE , Dadi institute of Engg & Tech,Anakapalli,vizag dist.

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 (AWS-C DIC). We give the formal definition, system model, and security model. Then, a concrete AWS-CDIC protocol is designed using the bilinear pairings. The proposed AWS-CDIC protocol is provably secure based on the hardness of computational Diffie–Hellman problem. Our AWS-CDIC protocol is also efficient and flexible. Based on the original client's authorization, the proposed AWS-CDIC protocol can realize private remote data integrity checking, delegated remote data integrity checking, and public remote data integrity checking.

I. INTRODUCTION

Cloud Computing [1] is serving the wide range of computing and research communities in the everyday growing researches. It helps in making the resources available to everyone who virtually increases the storage space, processor speed, memory and

the applications stored. Cloud computing provides three kinds of services, most commonly used is software as a service. Cloud computing has a huge number of advantages and benefits: a) reduces the high investment on the hardware's by providing the virtual availability of all the hardware's needed. b) Maintenance of the cloud contents is left to the cloud servers by transferring the overhead to the cloud server's. c) Your data is available whenever you needed to use it, no need to take your computers with you always. However the most useful cloud computing also has some of the drawbacks which is hard to digest.one of most important problem to worry with cloud servers are the security and the availability of your data. The data stored in cloud are stored in the third party servers where in the access over the data you stored is preserved with cloud servers. Where in the cloud servers can miss use the data you stored. There is no guarantee for the data you stored as the data can be lost or damaged and the cloud servers do not take any responsibility for the data stored. Your data may become temporarily un available in case of cloud failures.in case of data shift to untrusted clouds or the user your personal information leaked to the third party. Preserving the privacy of the data stored by the user into the public clouds are always need to be secured and made available to the user at all times whenever he needed with zero damage. Remote data integrity protocols helps in maintaining the data security [4] by using key protection and the data labeling based on the keys. The user data should be necessarily made available to the user when he wants to access it. In our design we make use of security and the performance concepts. We allow the user to upload his file to the cloud servers where in the data is stored with the primary level protection with a key generation with a digital signature by using the SHA1 and SHA2 algorithms which is better used than the md5 encryption. The file uploaded by the user can be verified before he download's the file ensuring the data preserved and the data security which we made it possible by the use of zero knowledge check.by making use of the file signature generating servers. We could able to reduce the overheads and

the traffic over the networks by selecting the server with the less traffic and making the data available to user as early as he can The contribution of this paper is summarized as bellow

. • Identity based keys are generated using the third party auditor where in the remote data integrity checks are used. Based on which the keys are generated for an identity that's the id level.

• We provided the detailed security proofs of the protocols including sounding of privacy with SHA1 and SHA2 with the key level encryption

• File signature generating servers are used along with the cloud servers to controlling the traffic over the network.

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 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. 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, identity-based proxy-oriented data uploading and remote data integrity checking is more attractive. Thus, it will be very necessary to study the ID-PUIC protocol.

B. Related Work

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 cryp-tography 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 identity-based 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 from the Weil pairing [5]. By combining the proxy cryptography with encryption technique, some proxy re-encryption schemes are proposed. Liu *et al.* formalize and construct the attribute-based proxy signature [6]. 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 [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]–[16]. Following Ateniese *et al.*'s pioneering

work, many remote data integrity checking models and protocols have been proposed [17]–[19]. In 2008, proof of retrievability (POR) scheme was proposed by Shacham *et al.* [20]. 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 [21]–[26]. 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 indispens-able [27]–[30]. By using cloud storage, the clients can access the remote data with independent geographical locations. The end devices may be mobile 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.

C. Contributions

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.

D. Paper Organization

The paper is organized below. The formal system model and security model of ID-PUIC protocol are given in Section II. The concrete protocol, performance analysis and prototype implementation are presented in Section III. Section IV ana-lyzes the proposed ID-PUIC protocol's security. The proposed protocol is provably secure. At the end of the paper, the conclusion is given in Section V.

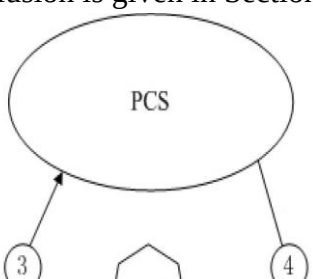

Fig. 1. Architecture of our ID-DPDP protocol.

III.Modules

Original Client

- Public Cloud Server
- Proxy
- KGC

MODULE DESCRIPTIONS:

ORIGINAL CLIENT:

Original Client is an Entity, Who is going to act as an upload the massive data into the public cloud server (PCS) by the delegated proxy, and the main purpose is integrity checking of massive data will be through the remote control. For the Data uploading and Downloading client have to follow the following Process steps:

- Client can view the cloud files and also make the downloading.
- Client has to upload the file with some requested attributes with encryption key.
- Then client has to make the request to the TPA and PROXY to accept the download request and request for the secret key which will be given by the TPA.
- After receiving the secret key client can make the downloading file.

PUBLIC CLOUD SERVER:

PCS is an entity which is maintained by the cloud service provider. PCS is the significant cloud storage space and computation resource to maintain the client's massive data.

PCS can view the all the client's details and upload some file which is useful for the client and make the storage for the client uploaded files.

PROXY

Proxy is 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 $m\omega$ which

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 22
November 2018

is signed and issued by *Original Client*, it can process and upload the original client's data; otherwise, it cannot perform the procedure.

Simply say means: without the Knowledge of Proxy's authentication and verification and acceptance of proxy client cannot download the file which is uploaded by the Client.

KGC

KGC (Key Generation Center): an entity, when receiving an identity, it generates the private key which corresponds to the received identity.

Generated Secret key is send to the client who is make the request for the secret key via mail id which is given by the Client.

IV.Results And Discussions

IV.Conclusion

This paper proposes the novel security idea of ID-PUIC out in the open cloud. The paper formalizes ID-PUIC's framework model and security display. At that point, the principal solid ID-PUIC convention is outlined by utilizing the bilinear pairings system. The solid ID-PUIC convention is provably secure and productive by utilizing the formal security confirmation and effectiveness examination. Then again, the proposed ID-PUIC convention can likewise acknowledge private remote

information honesty checking, assigned remote information respectability checking and open remote information uprightness checking in light of the first customer's approval.

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.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. G. Ateniese *et al.*, "Provable data possession at untrusted stores," in *Proc. CCS*, 2007, pp. 598–609.

[9] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proc. SecureComm*, 2008, Art. ID 9.

[10] C. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. CCS*, 2009, pp. 213–222.

[11] E. Esiner, A. Küpçü, and Ö. Özkasap, "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.

[12] 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, Germany: Springer-Verlag, 2014, pp. 611–617.

[13] H. Wang, "Proxy provable data possession in public clouds," *IEEE Trans. Services Comput.*, vol. 6, no. 4, pp. 551–559, Oct./Dec. 2013.

[14] H. Wang, "Identity-based distributed provable data possession in multi-cloud storage," *IEEE Trans. Services Comput.*, vol. 8, no. 2, pp. 328–340, Mar./Apr. 2015.

Author's Profile

KORIBILLI JAYAPRAKASH NAIDU

pursuring M.Tech in Computer Science and Engineering from Dadi institute of Engg & Tech Anakapalli,vizag dist affiliated to the Jawaharlal Nehru Technological University, Kakinada respectively.

naidukoribillin@gmail.com

V. SRINIVASA RAO

Working As Associative Professor Dadi institute of Engg & Tech Anakapalli,vizag dist.
srini.vegi@gmail.com