ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Efficient Data Uploading Scheme with Proxy-Identity Based Data Integrity Management over Cloud Server

Ronnarit Kamlangjai [1], Dr. Reeja S. R [2]

M.Tech, Department of Computer Science and Information Technology, Dayananda Sagar University, Bangalore, India

Associate Professor, Department of Computer Science and Engineering, Dayananda Sagar University, Bangalore, India

ABSTRACT: An ever increasing number of customers might want to store their information to PCS [Public cloud servers] alongside the quick improvement of cloud computing. New security issues must be illuminated keeping in mind the end goal to help more customers process their information openly cloud. At the point when the customer is limited to get to PCS, he will assign its intermediary to process his information and transfer them. Then again, remote information respectability checking is additionally a vital security issue out in the open cloud storage. It makes the customers check whether their outsourced information is kept in place without downloading the entire information. From the security issues, we propose a novel intermediary situated information transferring and remote information respectability checking model in character based open key cryptography: IDPUIC (identity-based proxy-oriented data uploading and remote data integrity checking in public cloud). We give the formal definition, framework model and security demonstrates. At that point, a solid ID-PUIC convention is outlined by utilizing the bilinear pairings. The proposed ID-PUIC convention is provably secure in view of the hardness of CDH (Computational Diffie-Hellman) issue. Our ID-PUIC convention is likewise effective and adaptable. In view of the first customer's approval, the proposed ID-PUIC convention can understand private remote information trustworthiness checking, appointed remote information uprightness checking and open remote information honesty checking.

KEYWORDS: Data Integrity, Proxy, Public Cloud, PCS, IDPUIC, Computational Diffie-Hellman, Data Security.

I. INTRODUCTION

Alongside the quick advancement of registering and correspondence strategy, a lot of information is produced. This huge information needs more solid calculation asset and more prominent storage room. In the course of the most recent years, cloud computing fulfills the application necessities and becomes rapidly. Basically, it takes the information handling as an administration, for example, stockpiling, figuring, information security, and so forth. By utilizing the general population cloud stage, the customers are eased of the weight for capacity administration, all-inclusive information access with free geological areas, and so on.

Consequently, an ever increasing number of customers might want to store and process their information by utilizing the remote cloud computing framework. Out in the open cloud computing, the customers store their gigantic information in the remote open cloud servers. Since the put away information is outside of the control of the customers, it involves the security chances as far as secrecy, respectability and accessibility of information and administration.

Remote information honesty checking is a primitive which can be utilized to persuade the cloud customers that their information is kept in place. In some extraordinary cases, the information proprietor might be confined to get to the general population cloud server, the information proprietor will designate the errand of information handling and transferring to the outsider, for instance the intermediary. On the opposite side, the remote information honesty checking convention must be proficient keeping in mind the end goal to make it reasonable for limit constrained end

DOI: 10.15680/IJIRCCE.2017. 0504274

gadgets. Hence, in light of character based open cryptography and intermediary open key cryptography, we will think about ID-PUIC convention.

II. SYSTEM INSPIRATION

In broad daylight cloud condition, most customers transfer their information to PCS and check their remote information's trustworthiness by Internet. At the point when the customer is an individual supervisor, some reasonable issues will happen. In the event that the administrator is associated with being required into the business misrepresentation, he will be taken away by the police. Amid the time of examination, the administrator will be limited to get to the system with a specific end goal to make preparations for arrangement.

The administrator's lawful business will continue amid the time of examination. At the point when an extensive of information is created, who can help him handle these information? On the off chance that this information can't be handled without a moment to spare, the administrator will confront the loose of monetary intrigue. Keeping in mind the end goal to keep the case happening, the chief needs to designate the intermediary to process its information, for instance, his secretary. Be that as it may, the director won't trust others can play out the remote information honesty checking.

Open checking will acquire some peril of releasing the security. For instance, the put away information volume can be distinguished by the vindictive verifiers. At the point when the transferred information volume is classified, private remote information respectability checking is essential. In spite of the fact that the secretary can handle and transfer the information for the supervisor, regardless he can't check the director's remote information respectability unless he is designated by the chief. We call the secretary as the intermediary of the supervisor. In PKI (open key foundation), remote information trustworthiness checking convention will play out the authentication administration.

At the point when the chief delegates a few substances to play out the remote information uprightness checking, it will acquire impressive overheads since the verifier will check the declaration when it checks the remote information respectability. In PKI, the impressive overheads originated from the substantial authentication check, endorsements era, conveyance, renouncement, recharges, and so on. Out in the open cloud computing, the end gadgets may have low calculation limit, for example, cell phone, iPad, and so on. Personality based open key cryptography can dispense with the confused authentication administration. So as to expand the proficiency, identity based intermediary arranged information transferring and remote information uprightness checking is more appealing. In this way, it will be exceptionally important to concentrate the ID-PUIC convention.

III. PROPOSED METHODOLOGY

In broad thinking cloud, this paper concentrates on the character based intermediary arranged information transferring and remote information trustworthiness checking. By utilizing character based open key cryptology, our proposed ID-PUIC convention is proficient since the endorsement administration is dispensed with. ID-PUIC is a novel intermediary situated information transferring and remote information uprightness checking model in broad daylight cloud. We give the formal framework model and security show for ID-PUIC convention. At that point, in light of the bilinear pairings, we composed the main solid ID-PUIC convention. In the arbitrary prophet show, our planned ID-PUIC convention is provably secure. In focus of the first customer's approval, our convention can understand private checking, assigned checking and open checking.

IV. LITERATURE SURVEY

There exist various security issues in the cloud computing. This paper depends on the examination consequences of intermediary cryptography, personality based open key cryptography and remote information honesty checking in broad daylight cloud. Now and again, the cryptographic operation will be assigned to the outsider, for instance intermediary. Hence, we need to utilize the intermediary cryptography. Intermediary cryptography is an imperative cryptography primitive. In 1996, Mambo et al. proposed the idea of the intermediary cryptosystem. At the point when the bilinear pairings are brought into the personality based cryptography, identity based cryptography winds up noticeably productive and down to earth.

Since character based cryptography turns out to be more effective in light of the fact that it maintains a strategic distance from of the authentication administration, an ever increasing number of specialists are able to study personality based intermediary cryptography. In 2013, Yoon et al. proposed an ID-based intermediary signature conspire with message recuperation. Chen et al. proposed an intermediary signature plot and an edge intermediary signature conspire from the Weil blending.

By joining the intermediary cryptography with encryption procedure, some intermediary re-encryption plans are proposed. Liu et al. formalize and develop the quality based intermediary signature. Guo et al. displayed a non-intelligent CPA (chosen-plaintext assault)- secure intermediary re-encryption plot, which is impervious to arrangement assaults in manufacturing re-encryption keys. Numerous other solid intermediary re-encryption plans and their applications are likewise proposed.

Out in the open cloud, remote information uprightness checking is an essential security issue. Since the customers' gigantic information is outside of their control, the customers' information might be undermined by the pernicious cloud server paying little heed to deliberately or unexpectedly. So as to address the novel security issue, some productive models are exhibited. In 2007, Ateniese et al. proposed provable information ownership (PDP) worldview. In PDP show, the checker can check the remote information trustworthiness without recovering or downloading the entire information. PDP is a probabilistic evidence of remote information uprightness checking by examining arbitrary arrangement of squares from the general population cloud server, which radically lessens I/O costs.

The checker can play out the remote information trustworthiness checking by keeping up little metadata. From that point forward, some unique PDP model and conventions are composed. Taking after Ateniese et al's. Spearheading work, numerous remote information honesty checking models and conventions have been proposed. In 2008, proof of irretrievability (POR) plan was proposed by Shacham et al. POR is a more grounded model which makes the checker checks the remote information uprightness as well as recovers the remote information.

Numerous POR plans have been proposed. On a few cases, the customer may assign the remote information respectability checking undertaking to the outsider. In cloud computing, the outsider reviewing is essential.

By utilizing cloud storage, the customers can get to the remote information with autonomous land areas. The end gadgets might be versatile and constrained in calculation and capacity. In this way, productive and secure ID-PUIC convention is more appropriate for cloud customers outfitted with versatile end gadgets. From the part of the remote information uprightness checker, all the remote information trustworthiness registering conventions are ordered with two classes: private remote information honesty checking and open remote information respectability checking. In the reaction checking period of private remote information uprightness checking, some private data is irreplaceable.

In actuality, private data is not required in the reaction checking of open remote information uprightness checking. Exceptionally, when the private data is appointed to the outsider, the outsider can likewise play out the remote information uprightness checking. For this situation, it is additionally called assigned checking.

IV. SYSTEM MODEL

In this description, we give the system model and security model of ID-PUIC protocol. An ID-PUIC protocol consists of four different entities which are described below:

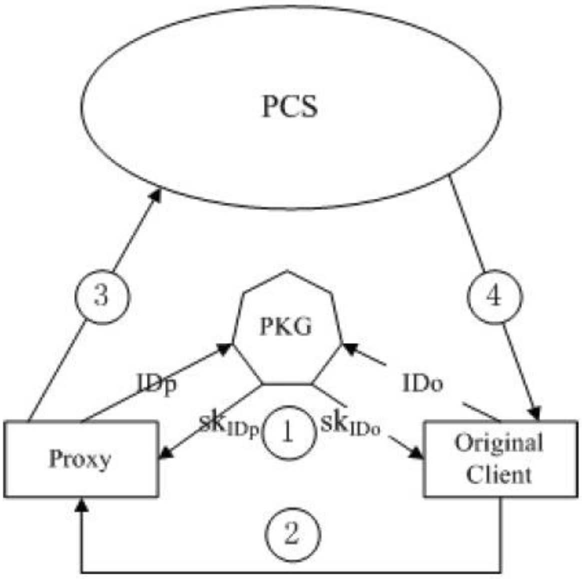

Fig.1. System Architecture Diagram

(a) Original Client: an entity, which has massive data to be uploaded to PCS by the delegated proxy, can perform the remote data integrity checking.
(b) 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.
(c) 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! which is signed and issued by Original-Client, it can process and upload the original client's data; otherwise, it cannot perform the procedure.
(d) PKG (Private Key Generation): an entity, when receiving an identity, it generates the private key which corresponds to the received identity.

In our proposed ID-PUIC protocol, Original Client will interact with PCS to check the remote data integrity. Thus, we give the the definition of interactive proof system. Then, we give the formal definition and security model of ID-PUIC protocol.

V. CONCLUSION

Spurred by the application needs, this paper proposes the novel security idea of ID-PUIC openly cloud. The paper formalizes ID-PUIC's framework model and security show. At that point, the primary solid ID-PUIC convention is composed by utilizing the bilinear pairings procedure. The solid ID-PUIC convention is provably secure and effective by utilizing the formal security confirmation and proficiency investigation. Then again, the proposed ID-PUIC convention can likewise acknowledge private remote information honesty checking, assigned remote information trustworthiness checking and open remote information uprightness checking in light of the first customer's approval.

DOI: 10.15680/IJIRCCE.2017. 0504274

REFERENCES

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

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

[3] T. Ma, J. Zhou, M. Tang, Y. Tian, Al-dhelaan A., Al-rodhaan M., L. Sungyoung, "Social network and tag sources based augmenting collaborative recommender system", *IEICE Transactions on Information and Systems*, vol. E98-D, no.4, pp. 902-910, 2015.

[4] E. Yoon, Y. Choi, C. Kim, "New ID-based proxy signature scheme with message recovery", Grid and Pervasive Computing, LNCS 7861, pp. 945-951, 2013.

[5] B. Chen, H. Yeh, "Secure proxy signature schemes from the weil pairing", Journal of Supercomputing, vol. 65, no. 2, pp. 496-506, 2013.

[6] X. Liu, J. Ma, J. Xiong, T. Zhang, Q. Li, "Personal health records integrity verification using attribute based proxy signature in cloud computing", Internet and Distributed Computing Systems, LNCS 8223, pp. 238-251, 2013.

[7] H. Guo, Z. Zhang, J. Zhang, "Proxy re-encryption with unforgeable reencryption keys", Cryptology and Network Security, LNCS 8813, pp. 20-33, 2014.

[8] E. Kirshanova, "Proxy re-encryption from lattices", PKC 2014, LNCS 8383, pp. 77-94, 2014.

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

[10] S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, K. Matsuura, "Reencryption verifiability: how to detect malicious activities of a proxy in proxy re-encryption", CT-RSA 2015, LNCS 9048, pp. 410-428, 2015.

[11] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, "Provable data possession at untrusted stores", *CCS'07*, pp. 598-609, 2007.

[12] G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable and efficient provable data possession", *SecureComm 2008*, 2008.

[13] C. C. Erway, A. Kupcu, C. Papamanthou, R. Tamassia, "Dynamic provable data possession", *CCS'09*, pp. 213-222, 2009.

[14] E. Esiner, A. Kupcu, O Ozkasap, "Analysis and optimization on FlexDPDP: a practical solution for dynamic provable data possession", *Intelligent Cloud Computing*, LNCS 8993, pp. 65-83, 2014.

[15] E. Zhou, Z. Li, "An improved remote data possession checking protocol in cloud storage", *Algorithms and Architectures for Parallel Processing*, LNCS 8631, pp. 611-617, 2014.

[16] H. Wang, "Proxy provable data possession in public clouds," *IEEE Transactions on Services Computing*, vol. 6, no. 4, pp. 551-559, 2013.

[17] H. Wang, "Identity-based distributed provable data possession in multi-cloud storage", *IEEE Transactions on Services Computing*, vol. 8, no. 2, pp. 328-340, 2015.

[18] H. Wang, Q. Wu, B. Qin, J. Domingo-Ferrer, "FRR: Fair remote retrieval of outsourced private medical records in electronic health networks", *Journal of Biomedical Informatics*, vol. 50, pp. 226-233, 2014.

[19] H. Wang, "Anonymous multi-receiver remote data retrieval for pay-tv in public clouds", *IET Information Security*, vol. 9, no. 2, pp. 108-118, 2015.

[20] H. Shacham, B. Waters, "Compact proofs of retrievability", *ASIACRYPT 2008*, LNCS 5350, pp. 90-107, 2008.

BIOGRAPHY

Mr. Ronnarit Kamlangjai, Studying M.Tech., Department of Computer Science and Information Technology in Dayananda Sagar University, Bangalore, India.

Dr. Reeja S. R, Working as an Associate Professor, Department of Computer Science and Engineering in Dayananda Sagar University, Bangalore, India.

DOI: 10.15680/IJIRCCE.2017. 0504274