ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Enhanced ID-PUIC Protocol for Cloud Data Integrity Checking By Proxy

Hyma Sireesha Vasamsetty [1], Dr.P.Venkateswara Rao [2]

P.G. Student, Department of Computer Science, Adikavi Nannaya University, Rajamahendravaram, AP, India[1]

Associate Professor, Department of Computer Science, Adikavi Nannaya University, Rajamahendravaram, AP, India[2]

ABSTRACT: Many customers might want to store their information on cloud service providers (CSPs) along with the quick improvement of distributed computing. New security issues have to be unravelled with a specific end goal to help more customers process their information openly cloud. At the point when the customer is confined to get to key updated cloud service providers, designate its intermediary to process his information and transfer them. Then again, remote information honesty checking is additionally a vital security issue out in the open distributed storage. It makes the customers check whether their outsourced information is kept in place without downloading the entire information. Main thing is that computation and communication costs are higher than previous revocable IBE schemes. The other security issue is lack of scalability in the sense that the key updated provider must keep a secret value for each user. From the security issues, in this project propose new revocable identity-based encryption schema for data uploading and remote data integrity checking model in identity-based public key cryptography. For security analysis, we demonstrate that the proposed scheme is semantically secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. ID-PUIC convention is likewise effective and adaptable. In light of the unique customer's approval, the proposed ID-PUIC convention can understand private remote information erectness checking, assigned remote information erectness checking, and open remote information honor checking.

KEYWORDS: public key cryptography, Remote data integrity checking.

I. INTRODUCTION

In broad public 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 changes as far as privacy, erectness, accessibility of information and administration. Remote information integrity checking is a primitive which can be utilized to persuade the cloud customers that their information is kept in place. In some uncommon cases, the information owner might be limited to get the people in general cloud server, the information proprietor will appoint the assignment of information handling and transfer to the outsider for instance to the intermediary. On the opposite side, the remote information respectability checking convention must be effective keeping in mind the end goal to make it appropriate for limit constrained end devices. Along these lines, in view of identity-based public cryptography and intermediary open key cryptography, we used about ID-PUIC convention.

II. LITERATURE SURVEY

1. An IBE plot that fundamentally enhances key-refresh effectiveness in favour of the confided in gathering (from direct to logarithmic in the quantity of clients), while remaining productive for the clients. Our plan expands on the thoughts of the Fuzzy IBE primitive and paired tree information structure, and is provably secure.
2. Another adaptable RIBE conspire with decoding key presentation strength by joining Lewko and Waters' character based encryption plot and finish sub tree technique, and turn out to be semantically secure utilizing double framework encryption philosophy. Contrasted with existing versatile and semantically secure RIBE

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

plans, our proposed RIBE plan is more proficient in term of cipher text size, open parameters size and unscrambling cost at cost of somewhat looser security reduction.

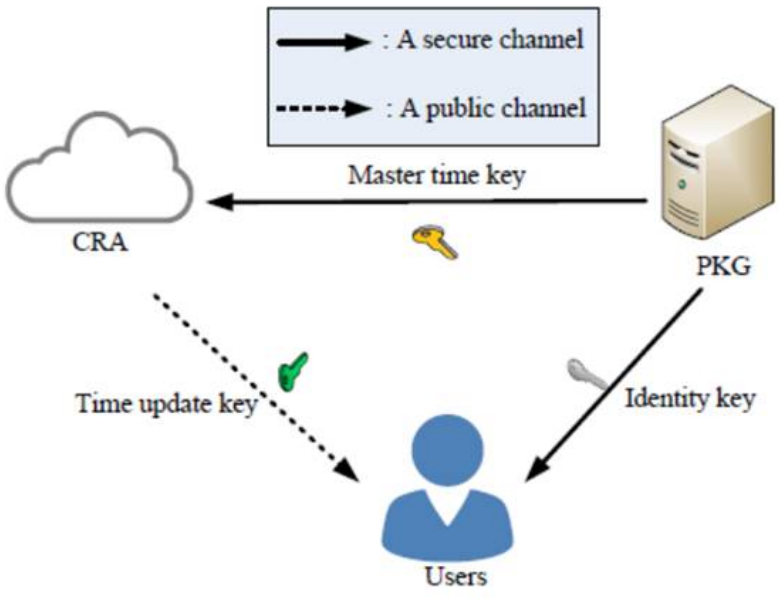
III. PROBLEM DEFINITION

In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management. When the manager delegates some entities to perform 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. PDP model and proof of retrievability (POR) scheme are not support the end devices may be mobile and limited in computation and storage.

IV. PROPOSED APPROACH

In public cloud, this project focuses on the identity-based proctor-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 proctor-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, public checking.

V. SYSTEM ARCHITECTURE



ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

VI. PROPOSED METHODOLOGY

A. *Client*

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

B. *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. *Key generation center*

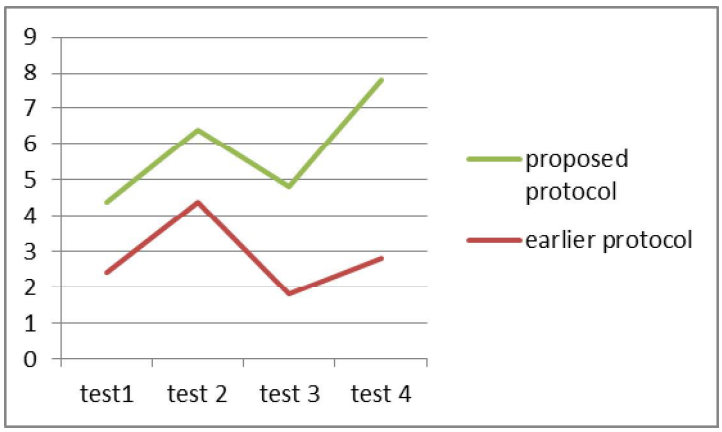
An entity, when receiving an identity, it generates the private key which corresponds to the received identity.

VII. ALGORITHM

A. *Enhanced ID-PUIC Protocol*

Input: MSKEY, PUBKEY, PRIVKEY, FID, FTAG, CLIENTID
Step 1: Initialize the system with owner, public cloud server and key generator center.
Step 2: Public and private key as well as master secret key is maintained by KGC.
Step 3: KGC generates private key which is given to client for public cloud interaction between end user and owner.
Step 4: Client generates warrant and signature pair by using KGC for authentication to public cloud.
Step 5: KGC generates private key to client by using its own private key.
Step 6: Client uploads a file with ECC-128bit algorithm with file blocks along with secrete key.
Step 7: KGC generates file tag pair uploaded to public cloud server.
Step 8: Hash generation and tag generation queries are maintained by client that is used to challenge the public cloud server for integrity checking.
Step 9: While downloading data from public cloud by the client is authorized by PKG.
Step 10: After authorization client can decrypt the file.

VIII. EXPERIMENTAL RESULT



ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

The simulation results are generated in java language.Finally the proposed protocol shows efficient performance in terms of security and communication as well as computation overhead compared to earlier protocol.

IX. CONCLUSION & FUTURE WORK

The enhanced ID-PUIC protocol is provably secure and efficient by using the formal security proof and efficiency analysis. On the other hand, the proposed Enhanced 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.in future if any adopt storage space reduction as well as implement reduplication technique to minimize storage space and bandwidth.

REFERENCES

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, "Achieving efficient cloud searchservices: multi-keyword ranked search over encrypted cloud data supportingparallel 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 provabledata auditing in public cloud storage," Journal of Internet Technology,vol. 16, no. 2, pp. 317-323, 2015.
[3] M.Mambo, K. Usuda, E. Okamoto, "Proxy signature for delegatingsigning operation", CCS 1996, pp. 48C57, 1996.
[4] E. Yoon, Y. Choi, C. Kim, "New ID-based proxy signature scheme withmessage recovery", Grid and Pervasive Computing, LNCS 7861, pp.945-951, 2013.
[5] B.Chen, H. Yeh, "Secure proxy signature schemes from the weilpairing", Journal of Supercomputing, vol. 65, no. 2, pp. 496-506, 2013.
[6] X. Liu, J. Ma, J. Xiong, T. Zhang, Q. Li, "Personal health recordsintegrity verification using attribute based proxy signature in cloudcomputing", Internet and Distributed Computing Systems, LNCS 8223,pp. 238-251, 2013.
[7] H.Guo, Z. Zhang, J. Zhang, "Proxy re-encryption with unforgeable reencryptionkeys", Cryptology and Network Security, LNCS 8813, pp.20-33, 2014.
[8] E.Kirshanova, "Proxy re-encryption from lattices", PKC 2014, LNCS8383, pp. 77-94, 2014.

[9] P.Xu, H. Chen, D. Zou, H. Jin, "Fine-grained and heterogeneous proxyre-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, "Re-encryptionverifiability: how to detect malicious activities of a proxyin 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 andefficient provable data possession", SecureComm 2008, 2008.
[13] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, R. Tamassia, "Dynamicprovable data possession", CCS'09, pp. 213-222, 2009.[14] E. Esiner, A. K¨upc¸ ¨u, ¨O¨Ozkasap, "Analysis and optimization onFlexDPDP: 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 protocolin cloud storage", Algorithms and Architectures for Parallel Processing,LNCS 8631, pp. 611-617, 2
014.
[16]. Muthukumar S, Dr.Krishnan .N, Pasupathi.P, Deepa. S, "Analysis of Image Inpainting Techniques with Exemplar, Poisson, Successive Elimination and 8 Pixel Neighborhood Methods", International Journal of Computer Applications (0975 – 8887), Volume 9, No.11, 2010