Identity Based Proxy System Using Data Uploading and Integrity Check in Cloud

S. B. Phatangare[1], Prof. S.K.Sonkar[2]
[1, 2] Department of Computer Engineering
[1, 2] AVCOE, Sangamner, Savitribai Phule Pune University,Pune India.

Abstract- *More clients might want to store their information to public cloud servers along with the rapid improvement of cloud computing. New security issues must be solved in order to help more clients process their information in the public cloud. At the point when the clients is limited to get to PCS, he will delegate its proxy too process his information and transfer them. Then again, remote information integrating checking is also an important security issue in public cloud storage. It makes the clients check whether their outsourced information is kept in place without downloading whole information. From the security issues, To propose a novel proxy oriented information uploading and remote information integrating checking model in character based public key cryptography: ID-PUIC (identity - based proxy oriented data uploading and remote data integrating checking in public cloud). Typically, System model and Security model. At that point, a concrete ID-PUIC protocol is designed by using the bilinear pairings. The proposed ID-PUIC protocol is provably secure in based on the hardness of CDH (computational Diffie-Hellman) issue. Our ID-PUIC protocol is likewise effective and adaptable. In view of the first customer's approval, the proposed ID-PUIC protocol can understand private remote information integrating checking, designated remote information integrating checking and public remote information honesty checking.*

Keywords- cloud computing, Identity-based cryptography, Proxy public key cryptography, Remote data integrity checking.

I. INTRODUCTION

Identity -based public key system (ID-PKS) is an attractive alternative for public key cryptography. ID-PKS setting eliminates the demands of public key infrastructure (PKI) and certificate organization in customary public key settings. An ID-PKS setting comprises of clients and a trusted third party (i.e. private key generator, PKG). The PKG is dependable to create every clients private key by utilizing the related ID data (e.g. e-mail address, name or social security number). In this way, no certificate and PKI are required in the related cryptographic system under ID-PKS settings. ID-based encryption (IBE) allows a sender to encrypt message straight forwardly by using a recipients ID without checking the approval of public key certificate. As need be, the recipient utilizes the private key respective with her/his ID to decrypt such cipher text. A public key setting needs to give client revocation approach, the earlier problem on the best way to revoke misbehaving/compromised users in an IDPKS setting is actually raised. The conventional public key settings to certificate revocation list (CRL) is a well-known revocation approach. CRL approach, if a party gets a public key and its related authentication, first approves them and then looks upward the CRL to guarantee that the public key has not been revoked. In this procedure requires the online help under PKI so that it will incur communication bottleneck. To improve the execution several efficient revocation system for traditional public key settings have been well examined for PKI. The researchers also pay attention to the renouncement issue of ID-PKS settings. A few revocable IBE plans have been proposed with respect to the revocation mechanisms in ID-PKS settings. 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.

II. RELATED WORK

Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, Motivated to get to the large scale processing assets and economic savings. To ensure information protection, the sensitive information should be encrypted by the information owner before outsourcing, which makes the traditional and productive plaintext keyword search procedure pointless. So how to plan a productive, in the two parts of exactness and proficiency, searchable encryption scheme over encrypted cloud information is very challenging task. To propose a reasonable, proficient, and adaptable searchable encryption scheme which

supports both multi-keyword ranked search and parallel search. To support multi-keyword search and result significance positioning, to receive Vector Space Model (VSM) to construct the searchable file to accomplish precise list items. To enhance search productivity, outline a tree-based record structure which supports parallel search to exploit the intense processing limit and assets of the cloud server. With our planned parallel search algorithm, the search productivity is well improved. To propose two secure searchable encryption plans to meet different protection requirements in two threat models. Extensive experiments on this present reality dataset approve our investigation and show that our proposed solution is very efficient and effective in supporting multi-keyword ranked parallel search.[1]

Y. Ren, J. Shen, J. Wang, J. Han, S. Lee,Cloud storageis presently a hot research topic in data technology. In cloud storage, date security properties such as information classification, respectability and accessibility turn out to be increasingly critical in numerous business applications. Recently, many provable data possession (PDP) plans are proposed to secure information respectability. It needs to appoint the remote information possession checking undertaking to some proxy. These PDP schemes are not secure since the proxy stores some state data in distributed storage servers. To propose an proficient common verifiable provable data possession scheme, which uses Diffie-Hellman shared key to develop the homomorphic authenticator. Specifically, the verifier in our scheme is stateless and free of the cloud storage benefit. It is significant that the introduced scheme is very productive compared with the previous PDP scheme, since the bilinear operation is notrequired.[2]

M. Mambo, K. Usuda, E. Okamoto A proxy signature scheme permits an entity to delegate its marking rights to another. These schemes have been proposed for use in various applications, especially in distributed computing. Before our work showed up, no exact definitions or demonstrated secure scheme had been given. To formalize a thought of security for proxy signature scheme and present provably-secure schemes. The break down the security of the notable assignment by-certificate scheme and show that after some slight but important modification, the subsequent scheme is secure, expecting the basic standard signature scheme is secure. Then demonstrate that work of total signature schemes grants transfer speed and computational savings. To analyses the proxy signature scheme of Kim, Park and Won, which offers essential execution benefits. A propose adjustments to this scheme which preserve its proficiency and yield an proxy signature plot that is provably secure in the arbitrary prophet demonstrate, under the discrete-logarithm assumption.[3]

E. Yoon, Y. Choi, C. Kim, The proposed an ID-based proxy signature scheme with message recuperation. To show that their plan is helpless against the forgery attack, and an adversary can produce a legitimate proxy signature for any message with knowing a past substantial proxy signature. What's more, there is a security defect in their confirmation. A propose an enhanced scheme that cures the shortcoming of their scheme and the enhanced scheme can be demonstrated existentially un-forgeable-adaptively picked message and ID attack accepting the computational Diffie-Hellman issue is hard.[4]

B. Chen, H. Yeh,[5] An intermediary signature plan is a technique which permits a unique endorser to delegate his marking power to an assigned individual, called an intermediary underwriter. Up to now, the vast majority of intermediary mark plans depend on the discrete logarithm issue. In this paper, The propose an intermediary signature plot and an edge intermediary signature conspire from the Weil matching, furthermore give a security evidence.[5]

Kirshanova Motivated to get proxy re-encryption (PRE) was presented by Blaze, Bleumer and Strauss [Euro crypt '98]. Basically, PRE permits a semi- trusted intermediary to change a cipher text encoded under one key into an encryption of the same plaintext under another key, without uncovering the fundamental plain- text. From that point forward, intriguing applications have been investigated, and numerous developments in different settings have been proposed. In 2007, Canetti and Honhenberger [CCS '07] characterized a more grounded thought CCA-security and build a bi-directional PRE plot. Later on, a few work considered CCA-secure PRE in view of bilinear gathering suppositions. Recently, Kirshanova [PKC '14] proposed the principal single-bounce CCA1-secure PRE conspire in light of learning with mistakes (LWE) supposition. In this work, we first bring up an inconspicuous however genuine error in the security verification of the work by Kirshanova. This revives the bearing of grid based CCA1-secure developments, even in the single hop setting. At that point we propose another LWE-based single-bounce CCA1-secure PRE conspire. At long last, A extend development to bolster multi-bounce re-encryptions for various levels of security under various settings.

III. PROBLEM DEFINITION

"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.."

IV. SYSTEM ARCHITECTURE

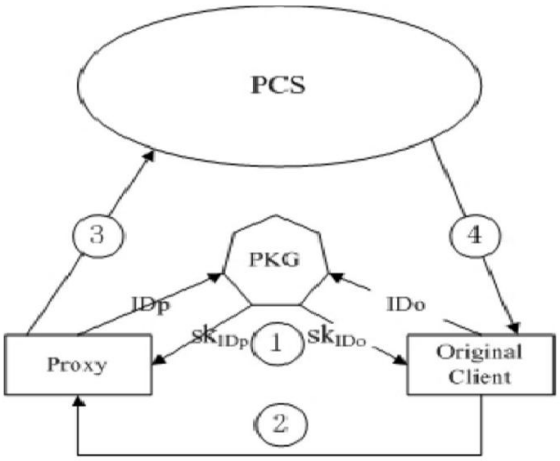

Figure 1. System Architecture

Module:

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

Module Description:

1. Original Client:

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

2. PCS (Public Cloud Server):

An entity which is managed by cloud service provider, has huge storage space and calculation resource to maintain the clients information.

3. Proxy:

An Entity, which is authorized to process the Original Clients information and exchange them, is chosen and authorized by Original Client. When Proxy satisfies the warrant which is signed and issued by Original Client, it can handle and transfer the original clients information; otherwise, it cannot perform the method.

4. KGC (Key Generation Center):

An entity, when receiving a personality, it creates the private key which corresponds to the received identity.

V. MATHEMATICAL MODEL

a) Uploading file:

U (Z) = {u1; u2; u3::::::un}
F(Z) = {f1; f2; f3::::::fn}
S(Z) = {s1; s2; s3::::::sn}
MAC(Z) = {m1;m2;m3::::mn}
D(Z) = {d1; d2; d3::::::dn}
Where
U (Z): Total number of users
F (Z): Total number of files
S (Z): Total number of secret key
MAC (Z): Master key
D (Z): Total data
U(Z) [F(Z) : S(Z) [MAC(Z)

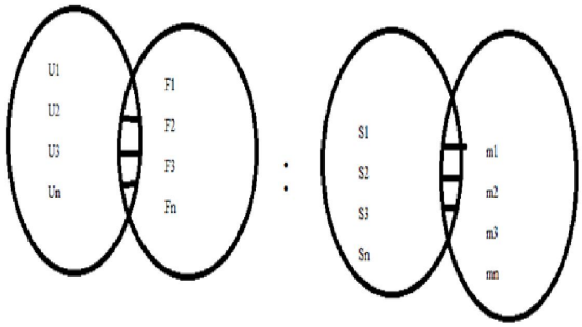

Figure 2.

Above diagram indicate that every file store on remote location with help of dynamic scheme in as per paper.Every file having secret key, public key whatever.

b) Downloading Files :

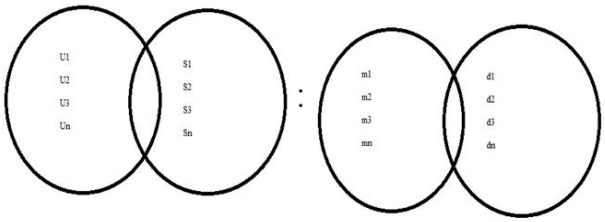

Figure 3.

Above diagram indicate that every file download on remote location with help of dynamic scheme in as per paper.

VI. ALGORITHMS

The AES and DES algorithm are used for encryption and decryption.

Encryption:

Encryption means convert plain text into cipher text. AES algorithm for encryptions as follows.

Input:

Encryption object as follows,
1. Encrytedstring = NULL
2. Secret key=key

Literal type as follows,
Byte plaintext, encrypted Text

Output:

1. START
2. Init = (ENCRYPT MODE, key)
3. Plaintext = UNICODE FORMAT/input message
4. EncryptedText - do Final (plaintext)
5. EncryptedString = Base64.encodeBase64 (encrypted Text)
6. Return encrypted String.

Decryption:

Decryptions are used to decrypt the message. Convert the cipher text into plain text .

Input:

Decryption object as follows,
Decrypted String = NULL
Secret Key =key
Literal type as follows,
Byte cipher text, decrypted Text

Output:

1. START
2. Init - (DECRYPT MODE, key)
3. Ciphertext - UNICODE FORMAT
4. DecryptedText - do Final(ciphertext)
5. DecryptedString -Base64.encodeBase64 (decrypted Text)
6. Return decrypted String

VII. EXPERIMENTAL SETUP

In this the Structure consist of technologies like JAVA , HTML , CSS , Java script. For back end MySql is used. Hence before investigational set up Software like Eclipse, Tomcat is predictable to be installed on server. User must have basic windows Family, good browser to view the results. Supervised Dataset or Un-Supervised dataset is used for testing in MySQL is tested.

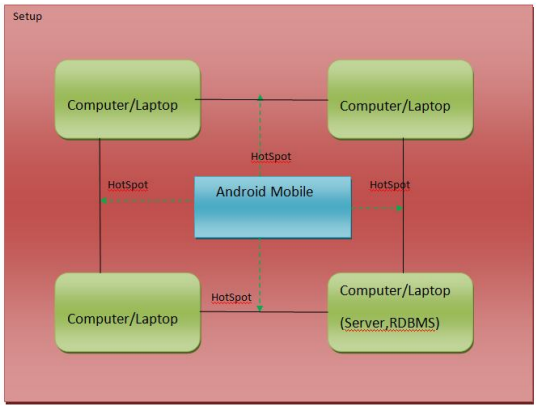

Figure 4.

VIII. RESULT TABLE AND DISCUSSION

Table 1. Result Table

Sr. No.	Existing System(DCG)	Proposed System(DCG)
1	0.45	0.78

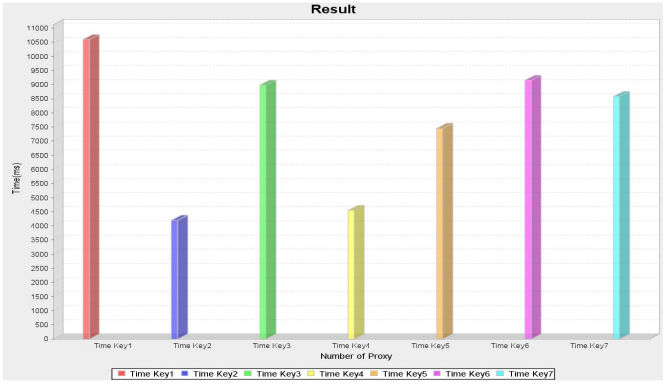

Figure 5. Time Update Key

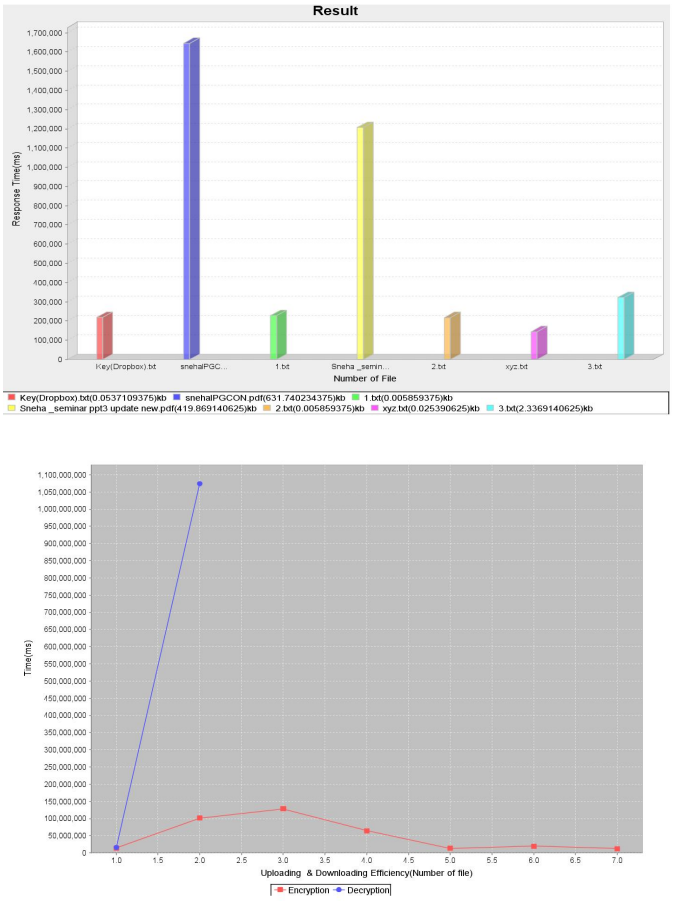

Figure 7. Upload &Download File

Figure shows the upload and download number of file encryption and decryption in time. The number of files [text,pdf..etc] are upload the file efficiency.

Number of proxy key generate the time key.

Above figure shows Revocation efficiency of the system as well as Un-Revocation Process. Two assumptions are made in using DCG and its related measures.

1. Highly Revoke User are more useful when appearing earlier in a Black result list (have higher Revoke).
2. Highly Revocation Process are more useful than marginally Un-Revoke Process, which are in turn more useful than Un-Revocation.
3. DCG originates from an earlier, more primitive, measure called Cumulative Gain.

IX. CONCLUSION

Finally conclude that how to securely put remote data. To proposes the novel security idea of ID-PUIC in public cloud. The paper formalizes ID-PUICs system model and security model. The first concrete ID-PUIC protocol is designed by using the bilinear pairings method. The concrete ID-PUIC protocol is provably secure and efficient by utilizing the formal security evidence and efficiency analysis.

ACKNOWLEDGMENT

It gives me an immense pleasure to express my sincere and heartiest gratitude towards my guide Prof. S.K.Sonkar for his guidance, encouragement, moral support and affection during the course of my work. I am especially appreciative of his willingness to listen and guide me to find the best Solution, regardless of the challenge. This work is also the outcome of the blessing guidance and support of my parents and family members and friends. I am also thankful to all who have contributed indirectly and materially in words and deeds for completion of this work.

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] 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] M. Mambo, K. Usuda, E. Okamoto, Proxy signature for delegating signing operation, CCS 1996, pp. 48C57, 1996.

[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 well 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 un-forgeable re-encryption 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.

BIOGRAPHIES

Miss. S. B. Phatangare is Pursuing Master in Engineering from Amrutwahini College of Engineering Sangamner. Received BE degree from University of Pune. His interested Areas are Cloud Computing, Data mining, Computer Network.

Prof. S. K. Sonkar is Assistant Professor in Amrutvahini College of Engineering, Sangamner. He is PhD Pursuing from university of Pune. His Research interests includes Cloud Computing, Network security, Data Mining.