|| Volume 3 || Issue 5 || May 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Secure and Effective Authentication Scheme for Distributed Mobile Cloud Computing Services

Trupti Balasaheb Farande[1], Prof. Priyanka Kedar[2]
Student, Department of Computer Science Dhole Patil College of Engineering, Pune, Maharashtra, India[1]
Assistant Professor, Department of Computer Science Dhole Patil College of Engineering, Pune, Maharashtra, India[2]

ABSTRACT: In modern societies, the number of mobile users has dramatically risen in recent years. In this paper, an efficient authentication scheme for distributed mobile cloud computing services is proposed. The proposed scheme provides security and convenience for mobile users to access multiple mobile cloud computing services from multiple service providers using only a single private key. The security strength of the proposed scheme is based on bilinear pairing cryptosystem and dynamic nonce generation. In addition, the scheme supports mutual authentication, key exchange, user anonymity, and user un traceability. From system implementation point of view, verification tables are not required for the trusted smart card generator (SCG) service and cloud computing service providers when adopting the proposed scheme. In consequence, this scheme reduces the usage of memory spaces on these corresponding service providers. In one mobile user authentication session, only the targeted cloud service provider needs to interact with the service requestor (user). The trusted SCG serves as the secure key distributor for distributed cloud service providers and mobile clients. In the proposed scheme, the trusted SCG service is not involved in individual user authentication process. With this design, our scheme reduces authentication processing time required by communication and computation between cloud service providers and traditional trusted third party service. Formal security proof and performance analyses are conducted to show that the scheme is both secure and efficient

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

I INTRODUCTION

Cloud individuals and organizations. It brings great benefits of allowing on-the-move access to the outsourced files, services simultaneously relieves file-owners from complicated local storage management and maintenance. However, some security concerns may impede users to use cloud storage. Among them, the integrity of outsourced files is considered as a main obstacle, since the users will lose physical control of their files after outsourced to a cloud storage server maintained by some cloud service provider (CSP). Thus, the file-owners may worry about whether their files have been tampered with, especially for those of importance. Considerable efforts have been made to address this issue. Among existing proposals, provable data possession (PDP) is a promising approach in proof of storage (PoS). With PDP, the file-owner only needs to retain a small amount of parameters of outsourced files and a secret key. To check whether or not the outsourced files are kept intact, the file owner or an auditor can challenge the cloud server with low communication overheads and computation costs. If some part of the file has been altered or deleted, for example, due to random hardware failures, the cloud storage server would not be able to prove the data integrity to convince the clients.

II LITERATURE SURVEY

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 not required.[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]

III EXISTING SYSTEM

In public cloud environment, most clients upload their information to Public Cloud Server (PCS) and check their remote data as integrity by Internet. When the client is an individual manager, some practical issue will happen. In the event that the supervisor is associated with being required into the business extortion, he will be taken away by the police. During the period of investigation, the supervisor will be limited to get to the system with a specific end goal to prepare for intrigue.

The managers legal business will go on during the period of investigation. When a large of data is generated, who can help him process these information? If these information 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 information for example, his secretary. But, the manager will not hope others have the ability to perform the remote data integrity checking. Public checking will bring about some risk of releasing the security. For example, the stored data volume can be detected by the malicious verifiers. When the uploaded data volume is confidential, private remote information integrity checking is necessary. Although the secretary has the ability to process and upload the information for the manager, he still cannot check the managers remote information 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.

1. In PKI, the impressive overheads come from the heavy certificate check, 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.
3. Public checking will incur some danger of leaking the privacy.
4. Less Efficiency.
5. Security level is low

IV PROPOSED SYSTEM

It depends on the research results of proxy cryptography, identity-based public key cryptography and remote information integrity checking in public cloud. In public cloud to concentrates on the identity-based proxy oriented information uploading and remote information integrity checking. By using identity-based public key cryptology, our proposed ID-PUIC protocol is proficient since the certificate administration is eliminated. ID-PUIC is a novel proxy oriented data uploading and remote data integrity checking model in public cloud. To give the formal system model and security model for ID-PUIC protocol. At that point ,based on the bilinear pairings, to designed the first concrete ID-PUIC protocol. In the random oracle model, our designed ID-PUIC convention is provably secure. Based on the original clients authorization, our protocol can understand private checking, delegated checking and public checking. To Propose an productive ID-PUIC protocol for secure information transferring and storage benefits in public clouds. Bilinear pairings system makes identity-based cryptography

functional. Our protocol is based on the bilinear pairings. To first review the bilinear pairings.

Advantages of Proposed System:

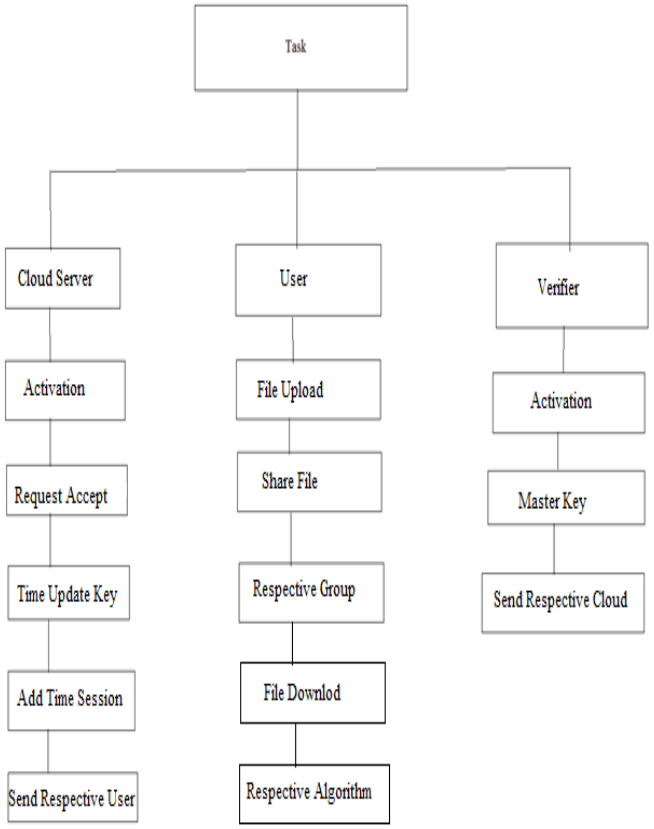
1.Compared with the previous work, our plan does not have to re-issue the entire private keys, but just need to
update a lightweight part of it at a particular entity.

2.To also specify that with the guide of Key Update, client needs not to contact with PKG in key-update, in other words, PKG is permitted to be offline after sending the revocation list to KU-CSP.

3.No secure channel or client authentication is required during key-update between client and KU-CSP.

4.To consider to realize revocable IBE with a semi-honest KU-CSP. To achieve this objective, to show a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model.

5.Finally, to give extensive experimental results to demonstrate the efficiency of our proposed construction.



V SYSTEM ARCHITECTURE

Module:

1. Original Client Module
2. Admin 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.Admin (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.

VI ALGORITHM

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

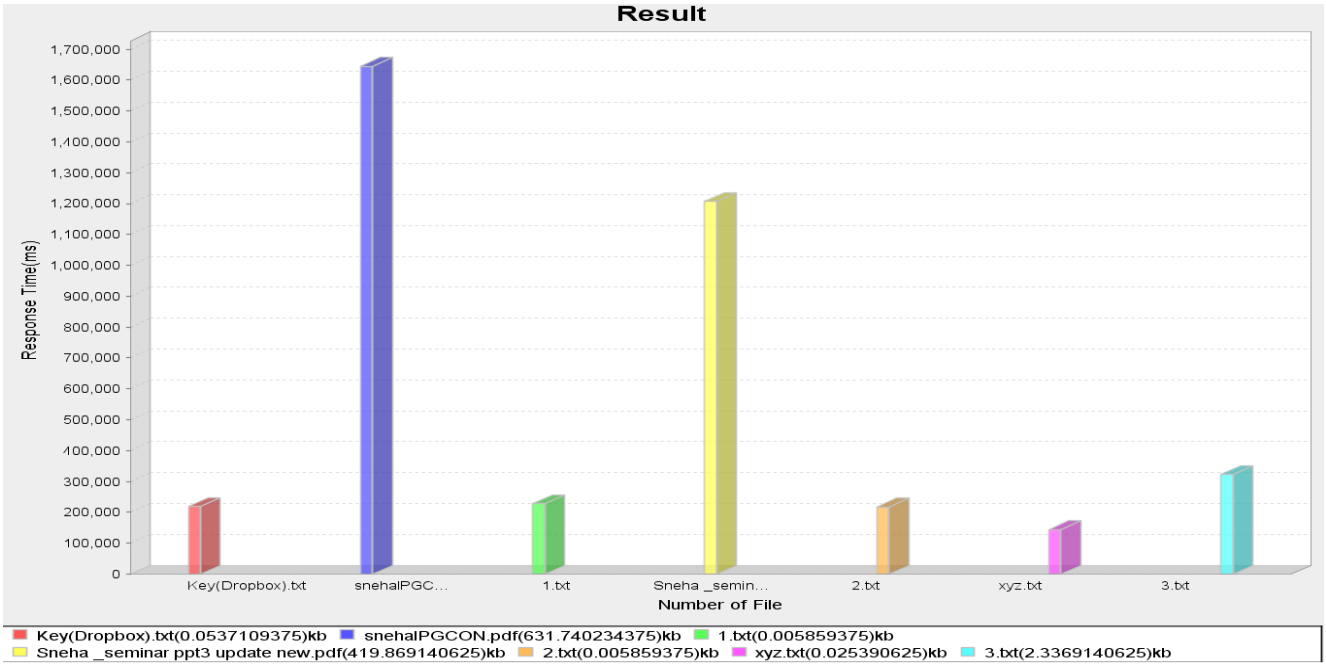
Literal type as follows,

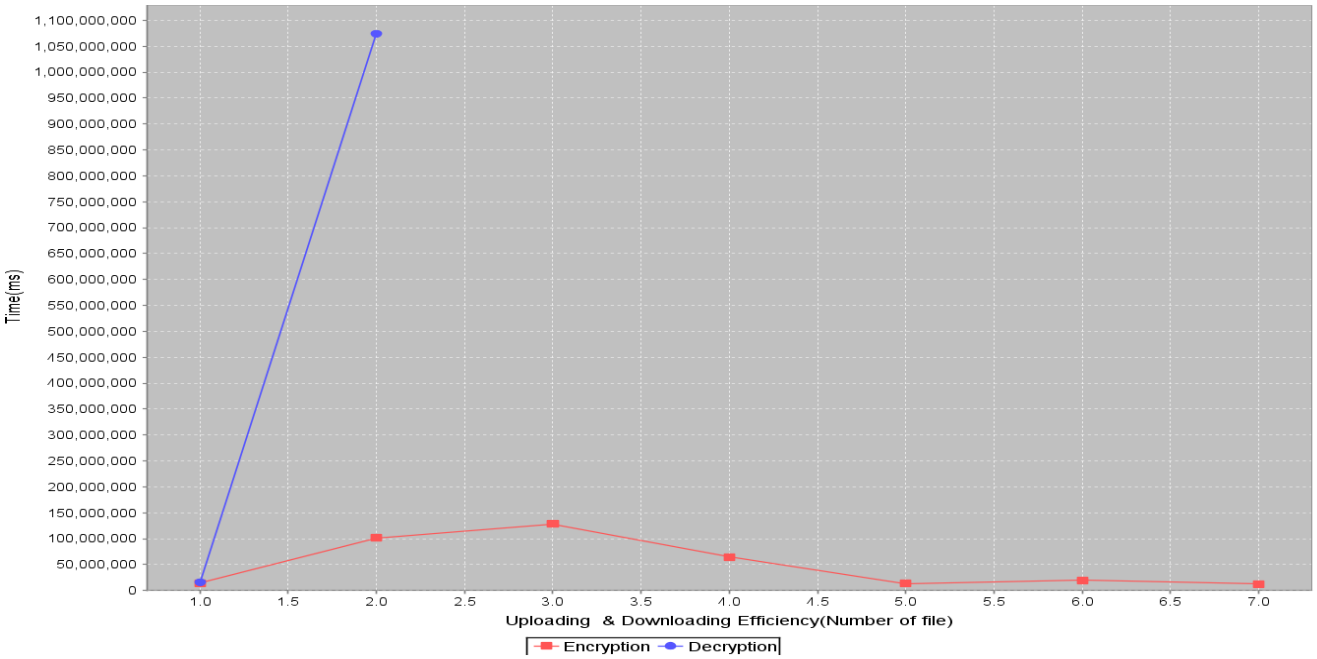
Byte cipher text, decrypted Text

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 RESULT ANALYSIS





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.

VIII CONCLUSION

Finally we can conclude that how to investigated proofs of storage in cloud in a multi-user setting. We introduced the notion of identity based data outsourcing and proposed a secure IBDO scheme. It allows the file-owner to delegate her outsourcing capability to proxies. Only the authorized proxy can process and outsource the file on behalf of the file-owner. Both the file origin and file integrity can be verified by a public auditor. The identity-based feature and the comprehensive auditing feature make our scheme

advantageous over existing PDP/PoR schemes. Security analyses and experimental results show that the proposed scheme is secure and has comparable performance as the SW scheme.

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.

[10] S. H. Islam and G. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography," *Math. Comput. Modelling*, vol. 57, no. 11, pp. 2703–2717, 2013.

[11] S. H. Islam and G. Biswas, "Dynamic ID-based remote user mutual authentication scheme with smartcard using elliptic curve cryptography," *J Electron.*, vol. 31, no. 5, pp. 473–488, 2014.

[12] C.-L. Hsu, Y.-H. Chuang, and C.-l. Kuo, "A novel remote user authentication scheme from bilinear pairings via internet," *wireless Pers. Commun.*, vol. 83, no. 1, pp. 163–174, 2015.