INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING

ISSN: 2320-1363

Enhancing Reliability and Scalability in Dynamic Group System Using Three Level Security Mechanisms

A.Sarika*1, Smt.J.Raghaveni*2

M.Tech Student, Dept of CSE, S.R.K.R Engineering college, Bhimavaram, AP, India.

Assistant Professor, Dept of CSE, S.R.K.R Engineering college, Bhimavaram, AP, India.

ABSTRACT:

Cloud computing is an emerging computing paradigm. It provides an economically efficient solution for sharing data in groups. There is a lot of research being made to find out the issues over cloud service providers. Existing solutions apply cryptographic methods for identification of authentication users over un-trusted cloud servers. Cryptographic methods are not support well.

To resolve previous methods issues here we are introducing three level security mechanisms. It resolves previous methods of all issues. Through this method we can enhance improved reliability and scalability and performance.

KEYWORDS: Three level security mechanism, reliability, scalability, dynamic group system, one time password, image authentication.

I.INTRODUCTION

All local data management systems are migrating to cloud servers to store large amount of sensitive or personal information. Users want to enjoy with high quality services and save significant investments with cloud servers.

By using encryption and group signature concept cloud user can access and share the data securely. It does not provide efficient security. We observed many issues like low scalability and reliability.

In this paper we can enhance with addition of new features like one time passwords and image authentication. After adding new features with MONA automatically all issues are resolved efficiently. All users are gets improved reliability and scalability and efficient results information.

II.RELATED WORK:

In this section system presenting different methods, those are solving different problems related to cloud security.

Storage systems and individual storage devices themselves become networked, causal attacks may chance to disturb under traversing time over un-trusted public network. This is the challenge, primary purpose to add data security. To protect data traditional techniques are not sufficient. Store data with long network is a misleading analogy. Same data is access by the multiple users. We have to update the data frequently.

Secure storage solutions require the creators of data to trust the storage servers and control at accessing stage. Most of systems allow single users and few members are allowed to share the files by using passwords. One of the existing system handle to store encrypted data and key distribution in a decentralized manner. Encryption techniques support for security features. These security features efficiently support for detection and prevention. This new system controls leakage attacks but have some more limitations. Integrity results are not received by the users.

After some days some concepts are design with group signatures. Group signature scheme allows any member of group to sign messages. Group signature works as a identity. It control anonymous unauthorized access and also support for efficient membership revocation. Using RSA generates only short signatures only. This signature concept is not support that much efficient.

After some days again signature creation starts with Diffie-Hellman assumption with bilinear groups. Linear encryption scheme is more secure with perfect decisions. This gives semantically secure solution. Different categories of revocation mechanisms are designed here. All revocation mechanism is added to our systems. Revocation mechanism verifies each and every signer information. Group signature must satisfy different security properties like correctness, anonymity, scalability and efficiency.

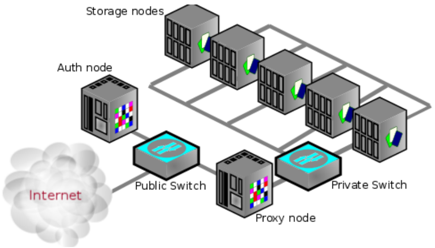


Fig1: Cloud data Storage Architecture

Again for storage systems designs one time passwords. It provides stronger security after addition for previous secure systems. Number of levels security also increases efficiently in our implementation process.

ISSN: 2320-1363

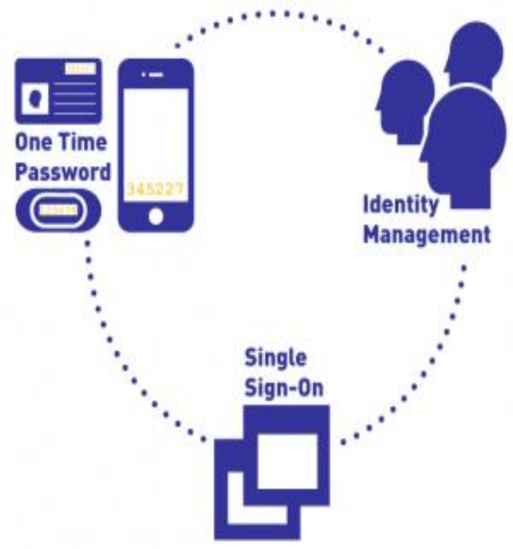


Fig2: one time passwords

Through from above analysis we can observe that how to securely shared files in multiple owners for dynamic groups. Identity privacy provides trusted services. Finally here some limitations are available. We can overcome those in this current paper.

III.PROBLEM STATEMENT

In literature survey this paper have seen many methods for protective data sharing in cloud computing. Almost all methods are failed to achieve efficient as well as secure method for data sharing in groups. Here we afford the best solutions for previous methods problems. This new method presents the design of reliable and efficient secure data sharing scheme. We can add extra features like image based authentication and one time password for previous dynamic group system. This method resolves all previous existing methods drawbacks and increases reliability and scalability.

IV.PROPOSED METHODOLOGY

The major operation of the paper is to solve the challenges and issues of above methods. Here we propose to provide reliable, scalable and secure multi owner data sharing scheme in cloud environment. Main implementation steps are

1. Provide enhanced security for dynamic group system integrates image based authentication and one time passwords.

2. Analyze the security results with rigorous proof and one time passwords.

3. One time passwords are more popular, it's provide stronger security across all number of machines.

4. After addition of one time passwords number of levels security is increase.

5. After adding additional features automatically improve scalability and reliability results.

ISSN: 2320-1363

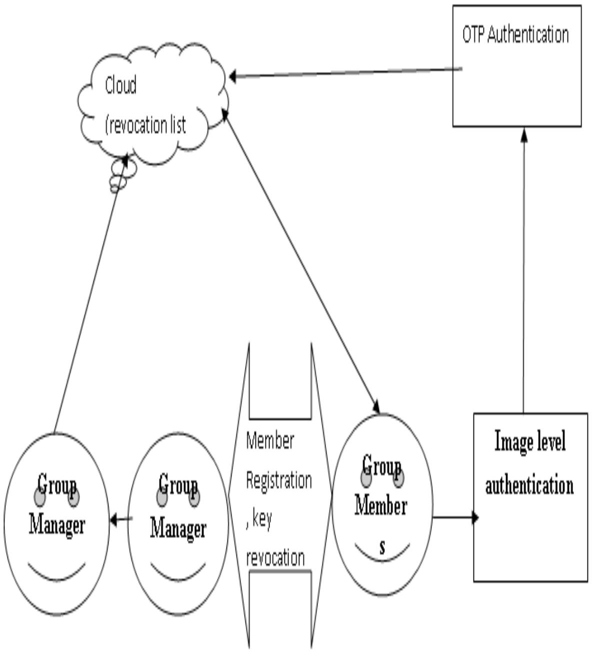


Fig3: proposed system architecture

System Model contains different users. Those are group members, group manager and cloud. Group manager have all different users of registration and key distribution information. Collect all distributed key list of information and create revocation list. Complete revocation list store into cloud. Here we design different levels of security in our implementation. Those numbers of levels are

1. Text level authentication
2. Image level authentication
3. OTP passwords authentication

Level1: security provides first with text based passwords.

Level2: next we can continue with image based authentication, its control different kinds of attacks like brute force etc,.

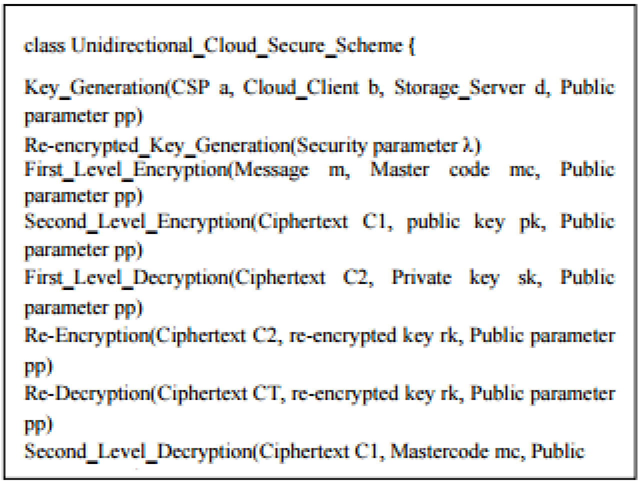
Level3: the above two passwords procedures are ok then we can go for OTP.

V.SYSTEM SETUP

System setups have different number of steps. Those steps are described below

1. User registration
2. User revocation
3. File upload
4. File download
5. File delete

VI.MULTI LEVEL SECURITY ALGORITHM



```
class Unidirectional_Cloud_Secure_Scheme {
Key_Generation(CSP a, Cloud_Client b, Storage_Server d, Public parameter pp)
Re-encrypted_Key_Generation(Security parameter λ)
First_Level_Encryption(Message m, Master code mc, Public parameter pp)
Second_Level_Encryption(Ciphertext C1, public key pk, Public parameter pp)
First_Level_Decryption(Ciphertext C2, Private key sk, Public parameter pp)
Re-Encryption(Ciphertext C2, re-encrypted key rk, Public parameter pp)
Re-Decryption(Ciphertext CT, re-encrypted key rk, Public parameter pp)
Second_Level_Decryption(Ciphertext C1, Mastercode mc, Public
```

ISSN: 2320-1363

Fig4: Multi level security algorithm pseudo code

VII.EXPERIMENTAL RESULTS AND DISCUSSION

Integrated Features Mona Support under efficiently for new user joining and revocation. Image authentication and one time password features are control more number of un-authentication user's compare to normal Mona.

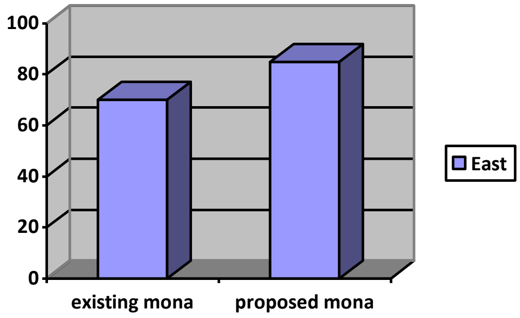


Fig5: Performance graph

Graph represents detection of authentication users relate to existing and proposed system.

VIII.CONCLUSION AND FUTURE WORK

This paper controls the failures of group manager under sharing of data and access of data. These benefits we got it with the help of three level security mechanisms. New security system control different kinds of attacks also. It provides efficient facilities with less and cost effective way. It supports efficient user revocation through revocation list. This study provides efficient security solutions compare to previous system.

In future some more levels we can add then its possible enhance the security for cloud data storages.

IX.REFERENCES

[1] Sunita R. Patil , Sandeep Kadam, RS-MONA: Reliable and Scalable Secure Method to Store and Share Secrete Data for Groups in Cloud, International Journal of Computer Applications (0975 – 8887) Volume 102– No.3, September 2014, PAGE NO:1-5.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[6] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and

Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
[7] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.
[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.
[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.
[11] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.
[12] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.
[13] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.
[14] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.
[15] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.