Undesignated And Referable Group Data Sharing In Cloud Computing

Prof. Anub Nair[1], Sneha Bhadrige[2], Pranjali Alurkar[3], Prashikha Jondhale[4], Sandhya jadhav[5], Anjali Sahajrao[6]
[1, 2, 3, 4, 5, 6] Dept of Information technology
[1, 2, 3, 4, 5, 6] Rajarshi Shahu College Of Engineering. Tathawade

Abstract*- As the cloud storage is a used widely now-a-days for sharing as well as storing of data. We are going to develop a technology which is supporting group data sharing on cloud. The main purpose behind this is to provide more security to the data. Previously, the computational overhead on revocation of user was more so as to reduce this we are implementing more user friendly platform to such users. By using this the duplication of same files are avoided. The basic behind this security technology is identity based cryptography. The unique strategy for key generation and also for encryption and decryption is used in addition to this we are going to use third party auditor to communicate in between user and cloud service provider(CSP). Both theoretical and experimental analysis demonstrate that the proposed scheme is secure and efficient for group data sharing in cloud computing.*

Keywords- Cloud storage auditing,Identity based cryptography, user revocation

I. INTRODUCTION

We construct a unique cloud storage auditing scheme for shared information supporting real economical user revocation in this paper. so as to understand economical user revocation, we come up with a unique strategy for key generation. In this design, the group's public key is replaced by the group's identity data, that remains unchanged within the whole One part remains mounted since being issued, and the other part alters with user revocation.

We also propose a unique non-public key update techniqueto support user revocation. once users are revoked from the cluster, all of the non-revoked users will update their non-public keys by this technique to form the cloud storage auditing still work, while the identity data of the cluster doesn't got to amendment. In addition, the revoked users aren't ready to transfer information and authenticators to the cloud any longer. during this approach, all of the authenticators generated before user revocation don't got to be recomputed. Therefore, the overhead of user revocation is fully freelance of the whole range of the revoked user's blocks. the group can still complete user revocation terribly expeditiously. Besides, our theme is predicated on identity-based cryptography, which eliminates the difficult certificate management in ancient PKI systems, as well as certificate generation, certificate revocation, certificate renewal, etc.

II. ALGORITHM

1) SHA-1 (Secure Hash Algorithm) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long. This is designed to be computationally infeasible to:

A) Obtain the original message , given its message digest.

B) Find two messages producing the same message digest. Each round takes 3 inputs-

- 512-bit block,
- A constant K[t] (where t= 0 to 79)

2) AES (Advanced Encryption Standard) The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES).

1. Derive the set of round keys from the cipher key
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation
6. Copy the final state array out as the encrypted data

III. PROPOSED SYSTEM

We propose a new construction of identity-based (ID-based) Remote data integrity checking protocol by making use of key-homomorphic cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication framework in PKI based Remote data integrity checking schemes. We formalize ID-based Remote data integrity checking and its security model including security against a malicious cloud server and zero knowledge privacy against a third party verifier. The proposed ID-based Remote data integrity checking protocol leaks no information of the stored data to the verifier during the Remote data integrity checking process.

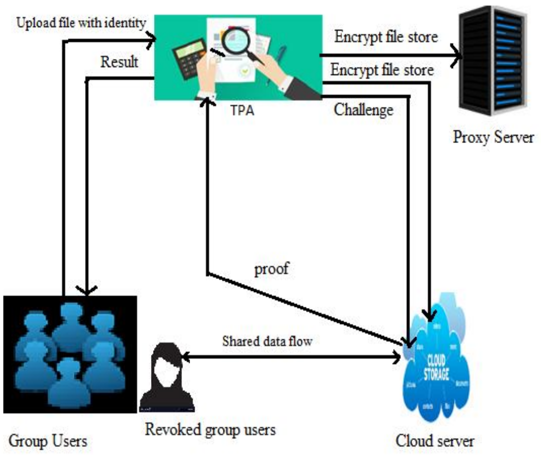
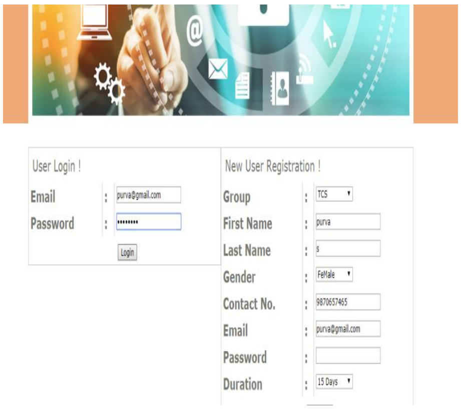


Fig.2.SystemArchitecture

IV. RESULT

1.User registration



User Login !

Email : purva@gmail.com

Password : ••••••••

New User Registration !

Group : TCS

First Name : purva

Last Name : s

Gender : FeMale

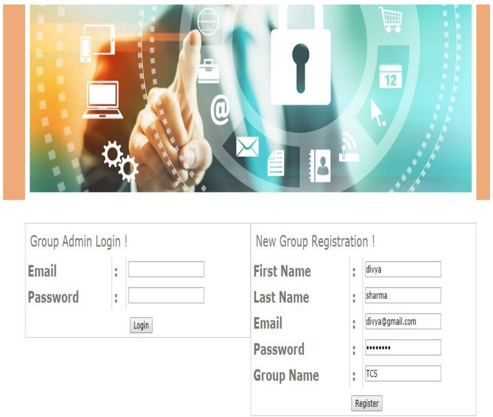
Contact No. : 9870657465

Email : purva@gmail.com

Password :

Duration : 15 Days

2. Group registration



Group Admin Login !

Email :

Password :

New Group Registration !

First Name : divya

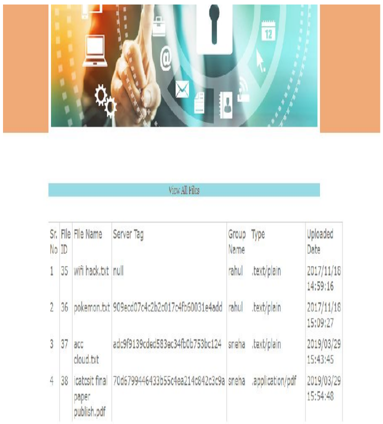
Last Name : sharma

Email : divya@gmail.com

Password : ••••••••

Group Name : TCS

3. File uploaded and verified



View All Files

Sr. No	File ID	File Name	Server Tag	Group Name	Type	Uploaded Date
1	35	wifi hack.txt	null	rahul	.text/plain	2017/11/18 14:59:16
2	36	pokemon.txt	909ecd07c4c2b2c017c4fb60031e4add	rahul	.text/plain	2017/11/18 15:09:27
3	37	acc cloud.txt	adc9f9139cded583ec34fb0b753bc124	sneha	.text/plain	2019/03/29 15:43:45
4	38	icatcsit final paper publish.pdf	70d6799446433b55c4ea214c842c3c9a	sneha	.application/pdf	2019/03/29 15:54:48

V. CONCLUSION

In this project we studied different cryptographic techniques to understand solution to achieving secure data sharing in the cloud is for the data owner to encrypt his data before storing into the Cloud. In this project a cloud based web application was implemented to encrypt data on the cloud servers using AES encryption algorithm. This technique is used to encrypt data and stored on the cloud. Hence, user's data is kept confidentiality as the cloud server that operates on it does not know what data it operated upon. Also, if the cloud service provider servers are hacked by malicious attackers, the user's data is secured and cannot be misused as it is encrypted.

VI. ACKNOWLEDGMENT

Apart from our own, the success of this report depends largely on the encouragement and guidelines of many others. We are especially grateful to our guide Prof. Anub Nair who has provided guidance, expertise and encouragement.

We express our gratefulness to Dr. R. B. Joshi , Head of Information Technology Department, JSPM's RSCOE, for their stimulating supervision whenever required during our work. We are also thankful to the staff of Information Technology Department for their cooperation and support.

REFERENCES

[1] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.

[2] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient

updates," IEEE Trans. Depend. Sec. Comput., vol. 12, no. 5, pp. 546–556, Sep. 2015.

[3] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2014.

[4] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Comput. Secur.,vol. 72, pp. 1–12, Jan. 2018, doi: 10.1016/j.cose.2017.08.007.

[5] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang,"Block design-based key agreement for group data sharing in cloud computing," IEEE Trans. Depend.

[6] C.Cachin,―Efficient private bidding and auctions with anoblivious Third party,‖ in Proc. ACM CCS, 1999, pp. 120–127.

[7] A Secure Revocable Ring Signature based Auction System for E-commerce Application , Anub .V.K, Pallavi. M. Tekade –March 2015.