Proceedings of Second Shri Chhatrapati Shivaji Maharaj QIP Conference on Engineering Innovations
Organized by Shri Chhatrapati Shivaji Maharaj College of Engineering, Ahmednagar
In Association with Novateur Publications JournalNX-ISSN No: 2581-4230
February, 22nd and 23rd, 2019

Implementation Of Re-encryption Based Security Meachinsm to Authenticate Shared Access in Cloud Computing

(Chaudhari Madhuri,Assistant Professor in Department of **Computer Engineering,**

Adsul Technical Campus Faculty Of Engineering & Management.)

Jadhav Shantanu Kailas
Student,Computer Engineering
ATC Faculty Of Engineering Ahemadnagar,India *jshantanu38@gmail.com*

Jadhav Shivaram Mahadeo
Student,Computer Engineering
ATC Faculty Of Engineering Ahemadnagar,India *shivaram.jadhav@gmail.com*

Golhar Amol Dattatrya
Student,Computer Engineering
ATC Faculty Of Engineering Ahemadnagar,India *agolhar06@gmail.com*

***Abstract*: Cloud computing provides facilities of shared computer processing resources and data to computers and other device on demand. System environment developed by using three key entities trusted third party, data owner and user. The concept of shared authority based privacy preserving authentication protocol i.e., SAPA used to develop system to perform shared access in multiple user. Security and privacy issue as well as shared access authority achieved by using access request matching mechanism e.g. authentication, user privacy, user can only access its own data fields. The multiple users want to share data so that purpose re-encryption is used to provide high security for user private data. Privacy preserving data access authority sharing is attractive for multi user collaborative cloud applications.**

Keywords*:- *Authentication, security, shared access and cloud computing.

I. Introduction

Cloud computing is a promising information technology architecture for both enterprises and individuals. It has attractive data storage and interactive structure with the advantages of on-demand user services user can easily access the network [1], [2]. Cloud computing have characteristics such as: 1) Device and location independent: these are enable user to access system using a web browser regardless of their location or what they use (e.g., PC mobile phone).and access via the internet, users can connect to it from anywhere. 2) Maintenance: on each user's computer no need to install cloud computing application. These are access from different places.

3) multitenancy: resources are share across large number of users. Towards the cloud computing, a typical service architecture such infrastructures as a services, platform as a services, software as a services, and others are applied for interconnections. Now a day cloud computing works toward the internet of services. Cloud service uses frequently so that popularity of cloud services become increases so that security and privacy issues are becoming key concern for increasing popularity of cloud services[3], [4]. In conventional security approach user access its own data in on-demand mode so that strong authentication is made by accessing data remotely. The number of user access the cloud storage and user may want to access and share authorized data to each other to achieve productive benefit which occurs new security and privacy challenges for the cloud storage [5], [6], [7]. An example of supply chain management system in cloud storage there is various interest groups such as supplier group, carrier group, retailer group. These groups own its users which give permission to access authorized field of data. Each group owns its users which are permitted to access the authorized data fields, and relatively independent access authorities own by different user. It means that different data fields of the same file can be access by any two users from different group. In that example supplier may want to access data from carrier. But it is not guarantee the carrier will allow its access request. If the carrier reject its request, then the supplier's access not possible and it will nothing obtained towards the desired data fields. It is unreasonable to thoroughly disclose the supplier's private information without any privacy considerations.

Security protocol should achieve the following requirement in the cloud environment. 1) Authentication: A real user means those having access permission with their identification information e.g., login id and password. Real user can access its own data fields as well as only legal user only can identify authorized data field. 2) Data anonymity: Data not identifiable nothing but data anonymity. Irrelevant or unauthorized entity cannot obtain the data from communication between entities. 3) User privacy: privacy which can be includes the concept of security, confidentiality. It provides the protection of user private information from irrelevant entity. If and only if the both users want to share authorized data field to each other. Then these two users will inform by cloud server to recognize the access permission sharing. 4) Forward security: There are various cryptographic algorithms to address potential security and privacy problems, including security architectures, data possession protocols, data public auditing protocols, secure data storage and data sharing protocols, access control mechanisms, privacy preserving protocols, and key management. This protocol used by most researches for provide high strength of security protection and privacy problem [8], [9], [10], [11], [12]. The previous researches concentrate on the authentication in which for achieving productive benefits different user may only real user can access its authorized field of data. They ignore case in which for achieving productive benefits different user may want to share and access to each other authorized data field. To request other user for data sharing for that purpose user challenges to the cloud server. Access request itself may disclose the user's privacy there is no matter data access permission can obtain or not. In this work aim to protect user private data, achieve access control, privacy preservation and develop system free from attack.

II. RELATED WORKS

Liu, Huansheng Ning, Qingxu Xiong [1], Laurence T. Yang, as per their research it proposed scheme to achieve privacy preservation in cloud computing. It identify privacy challenge during data accessing in cloud computing. It established authentication. Confidentiality achieved. User privacy obtained by access requests inform the cloud server about user accessing services. Drawback is absence of analysis of attack on the system.

Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan [2], in cloud computing dynamic group are present. It proposed multi-owner data sharing secure scheme (MONA) for dynamic group of interaction. In this scheme MONA design for dynamic group in untrusted. User revocation and new user joining supported by MONA. User revocation achieved through public revocation list. MONA satisfies the security requirement.

Mohamed Nabeel, Ning Shang, Elisa Bertino [3], as per their research ,based on BGKM scheme it proposed ACV- BGKM scheme to support attribute based access control. This approach supported by new GKM scheme. It shows that user efficiently derive decryption keys from portion of document with guaranteed security.

Smitha Sundareswaran, Anna C. Squicciarini[4] mark out the system it describes the approaches in which data in the cloud together automatically logging any access to the data with an auditing mechanism. It allows the data owner audit his content as well as enforces strong back end protection the main features of this work is that it enables data owner to audit copies of the data that were made without his knowledge.

Rafael Moreno Vozmediano, Rubén S. Montero, and Ignacio M. Llorente [6] , it describes, in the cloud computing key challenges play very important role. This key challenges help in the development computing infrastructure, in the development of the future Internet of Services, enabling on-demand provisioning of applications, and computing infrastructures. The development of cloud aggregation supports to improve security, reliability and energy efficiency of cloud infrastructures.

III. PROCEDURE OF SYSTEM DEVELOPMENT

Proposed system includes three main entities are as follows:

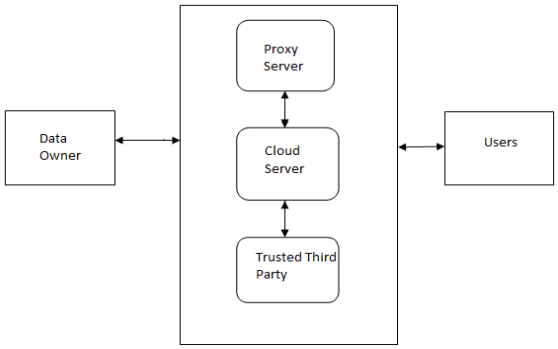

fig. 1 System Model for shared access in cloud computing

Owner should register first, for that he/she need to fill the registration details in the registration form. These details maintain in database. The above mentioned person have to login, they should login by giving their email-id and password. Owner upload the file into database, with the help of this metadata and contents, the end user has to download the file. The file uploaded which has to be in encrypted form. File is encrypted using cryptographic ECC algorithm. If user wants to access the data which is stored in cloud, he/she should register their details first. These details maintain in database. The authorized users download the file by using file id which has been stored by data owner when it was uploading. Owner can permit access or deny access for accessing the data if owner does not allow user can't able to get the data. Re-encryption is done by using different key-id and same ECC encryption algorithm when data sharing perform between multiple users. Owner can not send directly to the user so it will send to the third party auditor to verify the file. After verifies file Trusted third party send that file to the user then user can download the file. If cloud service provider wants to do some cloud offer, they should register first. After cloud provider logged in, he/she can see cloud provider can view the files uploaded by their client. Also upload this file into separate cloud database. Advantages: 1) Data accessing and data sharing will achieve without compromising user private information. 2) Re- encryption used for sharing data between multiple users. 3) System integrity satisfies by testing system by performing user authentication.

IV. DETAILS EXPERIMENTAL

A. Data Owner Login

In this owner of data perform login operation to upload data by using username and password.

Fig.2. login by Owner

B. Upload File to Share with Another User

Data owner select another user for example user (Payal) for sharing data. Data owner have three options for accessing data. First is grant read access. Second is read/write access. Third is revoke access. Select any one access type. Here select write grant access option and choose the file(text, doc, image etc.) to upload file or data for share with second user (Payal) and file is upload in encrypted form by using ECC encryption algorithm and key then logout by data owner

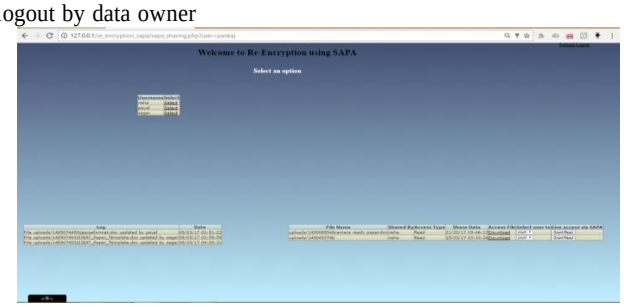

Fig.3. Upload files to share with another user

C. Download file by Second user i.e. Payal

Login by second use (Payal) and files are decrypt and download by second user using key. If this second user wants to perform write action it simply download the file and done write action and upload again this file. Write operation perform to change the content of file. After changing and uploading this file is new updated data file. This second user wants to share file with another user i.e. third user. It chooses the access type (write or read) and select user to share data or file. Here select the third user (Pankaj) and grant read access type. File is shared between second and third user using re- encryption. The re-encryption is done by ECC and by generating another key. Then perform logout by second user (Payal).

Fig.4.Upload files to share with another user

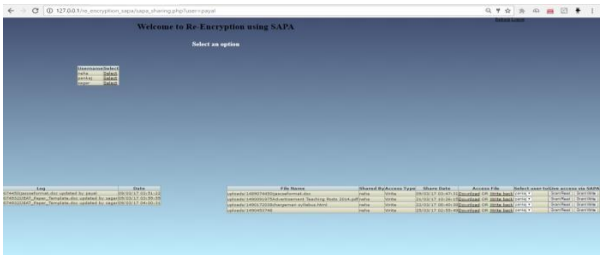

Fig.5.Write back to change file

D. File Download Third user

After login by third user, he or she downloads the file. Third user has the read access permission he/she can view file. If third user wants to share anyone else then he/she only gives the read access permission to access file.

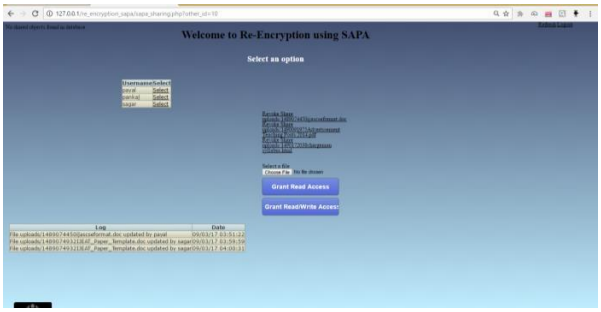

Fig.6.Download file by third user

In this way file sharing is done between multiple users by using re-encryption for secure communication

V. RESULT AND DISCUSSION

The expected results are as follows:Data owner: individual or group of users, which owns its data stored in the cloud for online data storage and computing. In this, users become a data owner which upload data or file in cloud server or database. Cloud server: An entity, which is managed by a particular cloud service provider or cloud application operator to provide data storage and computing services. The cloud server is an entity it include unrestricted storage and computational resources for sharing data between users. Trusted third party: These entities perform data public auditing and file verification before send to the user. End user: If owner permit then authorized user only can download the file. User can perform data write operation on that file if he/she wants to upload file and perform re-encryption again to share with another user before sending file. Re- encryption is done with different key-id between numbers of users to share file securely.

CONCLUSION

The privacy preserving protocol is used in cloud computing for secured access. In this work using SAPA protocol a new privacy challenge is identified during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. ECC algorithm and multiple key used for re-encryption purpose for sharing file with numbers of user therefore confidential transaction are achieved. A secure system for encrypted transaction is made and tested against attack.

FUTURE SCOPE

In cloud computing data is access between multiple users. In this work system environment is developed to access data securely between numbers of users. ECC algorithm is used for encryption. By using multiple key data is in re-encrypted form and performed secure access between numbers of users. Future scope can be, to introduce compression in the cluster for improving speed of data sharing and it can be used another encryption algorithm.

ACKNOWLEDGEMENT

I am thankful to Professor Madhuri Chaudhari for their guidance and support. I would also thank our head of department of computer science and engineering and ATCFOE College, Ahemadnagar for their guidance and encouragement.

REFERENCES

[1] Hong Liu, Huansheng Ning, Qingxu Xiong, Laurence T.Yang,"Shared Authority Base Privacy-Preserving Authentication Protocolin Cloud Computing", IEEE transactions on parallel and distributedsystems, vol. 26, no. 1, january 2015.
[2] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan "Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE transactions on parallel and distributed systems, vol. 24, no.6, june 2013.
[3]Mohamed Nabeel, Ning Shang, Elisa Bertino,"Privacy Preserving Policy-Based Content Sharing in Public Clouds , IEEE transactions on knowledge and data engineering, vol. 25, no. 11, november 2013.
[4] Smitha Sundareswaran, Anna C. Squicciarini, "Ensuring Distributed

Accountability for Data Sharing in the Cloud", IEEE transactions on dependable and secure computing, vol. 9, no. 4, july/august 2012.

[5] Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," IEEE Comm. Magazine, vol. 50, no. 9, pp. 24-25, Sept. 2012.

[6] R. Moreno-Voz media no, R.S. Montero, and I.M. Llorente, "Key Challenges in Cloud Compute into Enable the Future Internet of Services," IEEE Internet Computing, vol.17, no.4, pp.1825 July/Au 2013.

[7] Chia-Mu Yu, Chi-Yuan Chen, and Han Chieh Chao "Proof of Ownership in Deduplicated Cloud Storage with Mobile Device Efficiency", IEEE network, March/April 2015.

[8] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol.45,no.7, pp.73-78, 2012.

[9] L.A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment, IEEE Trans. Information Forensics and Security, vol. 8, no. 2, pp. 402-413, Feb. 2013.

[10]S. Grzonkowski and P.M. Corcoran, "Sharing Cloud Service User Authentication for Social Enhancement of Home Networking," IEEE Trans. Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, Aug.2011.

[11] Y. Zhu, H. Hu, G. Ahn, D. Huang, and S. Wang, "Towards Temporal Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 2576-2580, Mar. 2012.

[12] H. Zhuo, S. Zhong, and N. Yu, "A Privacy-Preserving Remote DataIntegrity Checking Protocol with Data Dynamics and Public Verifiability, " IEEE Trans. Knowledge and Data Eng., vol. 23, n9, pp. 1432-1437, Sept. 2011.