International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-6 Issue-3, February 2017

Survey on Privacy Preserving Authentication Protocol in Cloud Computing

Neha Mahakalkar, Vaishali Sahare

Abstract: ***Cloud computing provides facilities of shared computer processing resources and data to computers and other device on demand. System environment will develop 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 will be achieve 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. Universal Composability (UC) model use to prove that design of SAPA correctness. Develop a system with high security and attack free by analysing different attack related to the system. Privacy preserving data access authority sharing is attractive for multi user collaborative cloud applications***

Index Terms: 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. 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. 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.

An example of supply chain management system in cloud storage there is various interest groups such as supplier group, carrier group, retailer group. These group owns its user 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 entity.

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 user 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.

Manuscript published on 28 February 2017.
***** Correspondence Author (s)
Neha Mahakalkar, Department of Computer Science and Engineering, G.H.R.I.E.T. Nagpur (Maharashtra) India. E-mail: nehamahakalkar20@gmail.com
Vaishali Sahare, Department of Computer Science and Engineering, G.H.R.I.E.T. Nagpur (Maharashtra). India. E-mail: vaishali.sahare@raisoni.net

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, Laurence T. Yang [1], 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 enforce 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[5] 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 support to improve security, reliability and energy efficiency of cloud infrastructures.

III. SYSTEM MODEL AND DESIGN GOAL

A. System Model

A system model proposed system includes three main entities are as follows.

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. Re-encryption performs for data sharing between multiple users.

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.

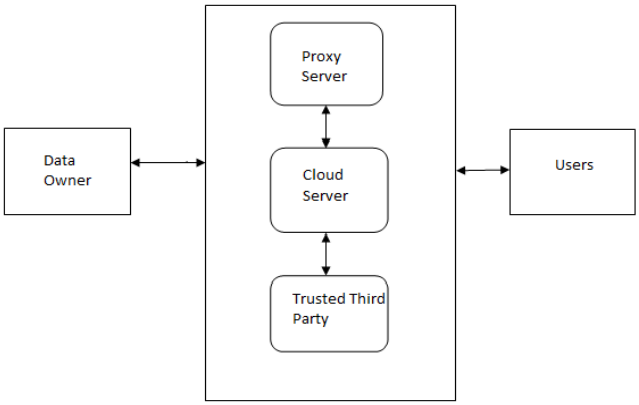

Fig. System Model for Shsred Access in Cloud Computing

B. Design Goal

In this work aim to protect user private data, achieve access control, privacy preservation and will develop system free from attack.

IV. CONCLUSION

In this work during data accessing in the cloud computing will identify new privacy challenge to achieve privacy-preserving data access authority sharing. A secure system for encrypted transaction will be made and test against attack. System integrity will be achieve for secure and correct data access on cloud environment.

REFERENCES

1. Hong Liu, Huansheng Ning, Qingxu Xiong, Laurence T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing", IEEE transactions on parallel and distributed systems, 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.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

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. Privacy-preserving Authentication Protocol in Cloud Computing",10.1109/TPDS.2014.2308218, IEEE Transactions on Parallel and Distributed Systems,2015
8. 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.