International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 1 233 - 237

Security Enhancement for Privacy Preservation in Cloud Computing by Anonymous Request Access

[1]Ashwini Khodwe , [2]Prof. V.R. Wadhankar

Abstract: Cloud computing is a computing technology or information technology architecture used by organization or individuals. It launches data storage and interactive paradigm with some advantages like on-demand self-services, ubiquitous network access. Due to popularity of cloud services, security and privacy becomes major issue.

There is the issue of legitimate responsibility for information (If a client stores some information in the cloud, can the cloud supplier benefit from it?). Numerous Terms of Service assentions are quiet on the topic of proprietorship. Physical control of the PC hardware (private cloud) is more secure than having the gear off site and under another person's control (open cloud). This conveys awesome motivation to open distributed computing administration suppliers to organize building and keeping up solid administration of secure administration. This paper addresses design of proposed system.

Keywords:*Cloud Computing, Authentication Protocol, Privacy Preservation, Shared Authority, Universal Composability.*

*****

I. INTRODUCTION

1.1 Cloud Computing

Cloud computing is a relatively new business model in the computing world. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

1.2 Cloud Models

There are three types of cloud models.

a. Private Cloud
b. Public Cloud
c. Hybrid Cloud

Private Cloud

Private cloud give the capacity to all the more specifically oversee assets that oblige a larger amount of control than is typically accessible from people in general cloud. Private cloud are typically utilized for a solitary business. For some associations considering distributed computing, private mists structures better beginning stage. They permit the association to have software's, situations, and databases in a cloud, while tending to concerns with respect to imparting and security and protection that can emerge in the general population the earth.

Typically, in Premises or Internal Private the earth, the client possesses the greater part of the information and supplies in the private cloud, has complete obligation regarding all the IT assets and also the information. That is the reason not at all like an open cloud, setting up shop in a private cloud obliges ability with system joining and with great virtualization and cloud stage innovations; you'll need to run your equipment, stockpiling.

Public cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. The public cloud is a blending of figuring administrations accessible on the Internet. It incorporates (Saas) Software as a Service applications, for example, Amazon.com or Yahoo's Ymail, programming advancement (Paas) Platforms as a Service, for example, Microsoft's Azure, and (Iaas) Infrastructures as a Service from an extensive variety of merchants. Nonetheless, general society cloud just isn't the best decision for each little business.

With the special cases of some new organizations and a hand sized scoop of existing organizations who have actualized new frameworks, none of the business information dwell absolutely in general society cloud. Major purpose behind this is that most open cloud applications run on a multi-inhabitant premise. That is, however your information and data is divided from others information, it is constantly prepared by literally the same application programming code that is likewise being utilized by numerous different organizations.

Hybrid cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

A hybrid cloud is for the most part best-ofbreed. It joins the solace level of a private cloud with the adaptability and flexibility of people in general cloud.

Crossover stages utilize either open mists or off-site Hosted Virtual Private Clouds for a few applications and courses of action. They combine these with on premises private mists for highsecurity application situations to power the best of

both planets. Likewise with the private model, in a mixture cloud, an association may decide to keep on using their current server farm gear and keep touchy information secured all alone system. Furthermore like general society cloud, a half and half model lets an association exploit a cloud's versatility, availability, reinforcement, and fiasco recuperation. It's an approach to address a percentage of the constraints of people in general cloud while even now picking up a considerable lot of the general population cloud's profits.

1.3 Cloud Services

Cloud Software as a Service (SaaS).

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS).

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS).

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Storage as a service

Capacity as an administration (Staas) is a plan of action in which an expansive administration supplier rents space in their stockpiling foundation on a membership premise. The economy of scale in the administration supplier's framework permits them to give stockpiling a great deal more cost adequately than most people or organizations can give their own particular stockpiling, when aggregate expense of possession is considered. Capacity as a Service is frequently used to illuminate offsite reinforcement challenges. Faultfinders of capacity as an administration point to the vast measure of system data transmission needed to direct their stockpiling using a web based administration.

1.4 Security Issues

As per the Cloud Security Alliance, the main three dangers in the cloud are "Unstable Interfaces and API's", Data Loss & Leakage", and "Equipment Failure" which represented 29%, 25% and 10% of all cloud security blackouts individually - together these structure shared innovation vulnerabilities. In a cloud supplier stage being shared by distinctive clients there may be a plausibility that data having a place with diverse clients dwells on same information server. In this manner Information spillage may emerge by slip-up when data for one client is given to other.[86] Additionally, Eugene Schultz, boss innovation officer at Emagined Security, said that programmers are investing considerable energy and exertion searching for approaches to enter the cloud. "There are some genuine Achilles' heels in the cloud foundation that are making huge gaps for the terrible fellows to get into". Since information from hundreds or a huge number of organizations can be put away on substantial cloud servers, programmers can hypothetically pick up control of tremendous stores of data through a solitary assault — a procedure he called "hyperjacking". There is the issue of legitimate responsibility for information (If a client stores some information in the cloud, can the cloud supplier benefit from it?). Numerous Terms of Service assentions are quiet on the topic of proprietorship. Physical control of the PC hardware (private cloud) is more secure than having the gear off site and under another person's control (open cloud). This conveys awesome motivation to open distributed computing administration suppliers to organize building and keeping up solid administration of secure administration.

II. RELATED WORK:

Cloud computing is a relatively new business model in the computing world. According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three "service models" (software, platform and infrastructure), and four "deployment models" (private, community, public and

hybrid) that together categorize ways to deliver cloud services. The definition is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing.[1]

Cloud computing is a popular and widely accepted paradigm built concepts such as on-demand computing resources, elastic scaling, elimination of up-front capital and operational expenses, and establishing a pay-as-you-use business model for computing and information technology services. And the adoption of virtualization, service oriented architectures, and utility computing there has been a significant development in the creation of cloud support structures for IT services within QoS bounds, service level agreements, and security and privacy requirements. The challenges related to the architecture, performance, reliability, security, maintainability, and virtualization were all within the scope of this issue. Connecting devices such as Switch , Router , Ethernet are used for creating network and one protocol called as Spanning Tree Protocol(STP) is the switching protocol calculates a loop-free single-path tree structure for the entire network. This STP works well in classical Ethernet but while deploying on cloud, it has some limitations such as Reduction in aggregate bandwidth as a result of blocking of redundant paths, Scalability, Path isolation , Support for multiple applications — multiple tenancy , The need to discover a new path if a node or a link fails on a given path adds latency of several seconds to minutes, causing disruptions to virtual machine migrations. To overcome this limitations Multiple Spanning Tree Protocol (MSTP) and Link Aggregation Group (LAG, IEEE 802.3ad) protocols have been standardized.[2]

The virtualize platform helps to reduce cost and effective hardware and software utilization and cloud is also used for data storage but it also come with security challenges and user always worried about data stored on cloud. The challenges are like Snooping , Cloud Authentication,Key Management, Data Leakage, Performance. To overcome this challenges there are two algorithms named as KeyGen algorithm used for generating set of keys and TagGen algorithm used for generating secrete tag key to each data component. Using this auditing system is generated in two phases, Audit and Key generation. The data owner updates frequently so auditing protocol must handle the static as well as dynamic data but while dynamic operations auditing protocol does not provide security properly.[3]

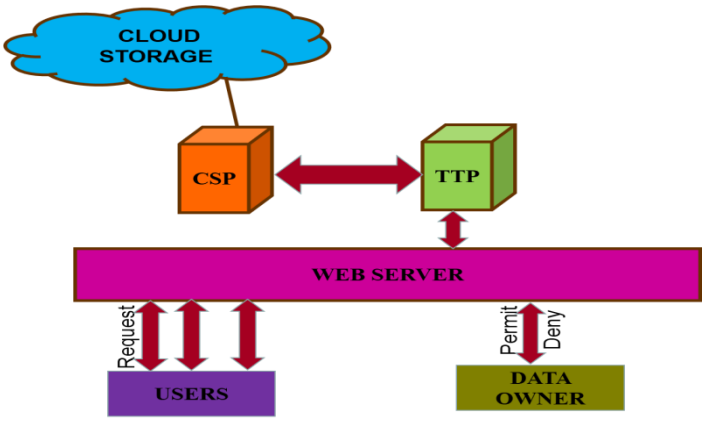
Shared authority based privacy preserving authentication protocol (SAPA) is another protocol which deals with privacy issue for cloud storage. It provides authentication and authorization without compromising a user's personal data. In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security); 2) attribute based access control is adopted to realize that the user can only access its own data fields; 3) proxy re-encryption is applied to provide data sharing among the multiple users. Meanwhile, universal composability (UC) model is established to prove that the SAPA theoretically has the design correctness. It indicates that the proposed protocol is attractive for multi-user collaborative cloud applications.[4]

There are many issues related to privacy preservation in cloud computing such as unauthorized access of data. The existing security system focuses on the authentication so that user's data cannot be access by unauthorized people.

One of the method of privacy preservation is an anonymous ID assignment. An algorithm is developed for anonymous sharing of private data among parties. This method is iteratively assign the ID numbers to the nodes from 1 to so on. Suppose there is a group of people and IDs are assign to them then these ID are unknown to the other members of group. This ID assignment allow user to share more complex data very safely. This algorithms are built on top of a secure sum data mining operation using Newton's identities and Sturm's theorem. Markov chain representations are used to find statistics on the number of iterations required. The identities are called as Newton identities which decreases the communication overhead.[5]

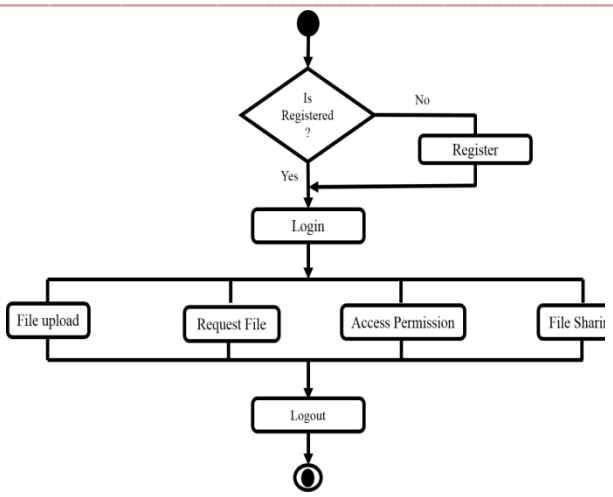
III. PROPOSED WORK:

The proposed system plan is carried out in following manner.



This project solves the security issues related to cloud access as well as cloud storage. This project mainly includes securing data by encrypting it and the data access permission is totally depend on data owner that is data owner will permit or deny the access permission. So that the privacy of data owner will be preserved.

The basic flow of proposed system is given below.



IV. MODULES

a. Registration and Login:

In this module an owner has to upload its files in a cloud server, he/she should register first. And a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

b. Database Connectivity:

In this module file uploading and file downloading to the database, these to actions will performed.

File Upload:

In this module Owner uploads the file(along with meta data) into database. The uploaded file was in encrypted form, only registered user can decrypt it.

File Download:

The Authorized users can download the file from database.

c. uploading to cloud:

In this module, all the files present in the database will be uploaded on cloud.

d. Timestamp and Approvals:

Owner can permit access or deny access for accessing the data. So users can able to access his/her account by the corresponding data owner. If owner does not allow, user can't able to get the data.

V. CONCLUSION

In this work, we have identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. And according to it, architecture and flow of proposed system is defined. The whole system is divided into modules as well.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of CloudComputing," National Institute of Standards and Technology, USA, 2009.

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

[3] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEETransactions on Parallel and Distributed Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, 2012.

[4] A.Gomathi P.Mohanavalli ,"Anonymous Access Control by SAPA in Cloud Computing" IJCSEC, Vol.3, Issue 2, 2015, Page.848-853, ISSN: 2347–8586.

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

[6] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," IEEETransactions on Parallel and Distributed Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.

[7] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Transactionson Knowledge and Data Engineering, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.

[8] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEETransactions on Services Computing, vol. 5, no. 2, pp. 220-232, 2012.

[9] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEETransactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, 2012.

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

[11] N.Vaitheeka, V.Rajeswari, D.Mahendran,"Preserving Privacy by Enhancing Security in Cloud" ,IJIRCEC, Vol. 3, Issue 3, March 2015.

[12] Kopparthi Lakshmi Narayana, M.Purushotham Reddy, G.Rama Subba Reddy,"Privacy Preserving Authentication With Shared Authority In Cloud", International Journal of Science Technology and Management, Vol. No.4, issue 07, july 2015.

[13] Yerragunta Harshada , K.Janardhan,"Ranking Based Shared Authority Privacy Preserving Authentication Protocol in Cloud Computing"IJIRCCE, Vol. 3, Issue 5, May 2015.

[14] R. Moreno-Vozmediano, R. S. Montero, and I.M. Llorente,"key challenges in cloud computing to enable the

future internet of services",IEEEinternet computing,Vol.17,no.4,pp.18-25.

[15] R. Sanchez, F.Almenares, P. Arias, D. Diaz-Savchez and A. Marn,"Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing" IEEE Trans. Consumer Electronics, Vol. 58. No. 1,pp.95-103,Feb.2013.

[16] K. Yang, X. Jia. "an efficient and secure dynamic auditing protocol for data storage in cloud computing", IEEE Trans. Parallel and Distributed Systens, vol. 24, no.9,pp.1717-1726,Sept 2013.

[17] S. Ruj, M. Stomenovic, and A. Nayak, "decentralized access control with anonymous authentication for securing data in cloud", IEEE Trans. Parallel and Distributed Systems, Vol. 25, no. 2, pp.384-394,Feb.2014.

[18] K. W. Park, J. W. Chung, and K. H. Park,"THEMIS:A mutually verifiable billing system for the cloud computing environment", IEEE Trans. Services computing, vol. 6, no. 3, pp.300-313,July-Sept 2013