Review on Privacy-Preserving in Cloud Computing

Jeur Nagaraj S
M.E. Computer Networks Student
G.H. Raisoni College of Engineering and Management, Pune, India

Pavan Kumar
Asst. Professor
G.H. Raisoni College of Engineering and Management, Pune, India

ABSTRACT
Cloud computing is emerging technology. Cloud offers several applications to users. Cloud computing use the basic fundamental infrastructure is help full for coming model of service that has the several benefit of decreasing cost by sharing computing and storage resources. Without appropriate privacy solution for cloud become a large failure. There is a lot of research techniques made to provide security. Privacy means that the person to be free from all interference. Privacy control allows the person to maintain a degree of intimacy. Privacy is the protection for the truthful use of personal information of cloud user. Privacy problems have become very challenge one in an cloud computing environment. So we use several techniques to protect the confidentiality data.

Keywords
Cloud Computing Component, Privacy-Preserving methods, Privacy-Preserving Algorithms.

1. INTRODUCTION
Cloud computing has made a drastic changes in IT field. Cloud computing service is a most recently used in IT area which offers different model. Cloud computing is emerging technology. Cloud offers several applications to user which consist of existing techniques combining with new technology .such technology shared different resources like hardware, software and some important information's provided to users and other people on internet whenever needed. Increasing population using emerging technology along with privacy and security in cloud because most of user having high sensitive data while sharing those data user needs privacy, providing such secure and privacy-preserving of data services is the big challenge. Security and privacy protection may be impeding the functionality and data services performance. This aims to covered the some common security and privacy threat and the crucial research, while focusing on the works that protect confidentiality data and query access privacy for sensitive data to stored and query in cloud[1]. In the continuous development of cloud computing technology, now a days, cloud computing is often used with another equivalent techniques such as grid computing, cluster computing, distributed computing, autonomic computing. Privacy is a most important issue in cloud whenever user needs to make his individual data in secure mode. So rapid development of internet technology, privacy preserving data publication has become needed. Preserving for the privacy of user, his data and identity in the cloud is very compulsory. The increase popularity of cloud computing, the concerned about privacy preserving are also getting more increased. But reaching the peak in providing and assurance the privacy-preserved data access in cloud is still in progress and needs much attention to the goal. Addressing of all these issues and designed of system which couldn't be compromised by the attackers would mark a success of Cloud Computing.

2. BACKGROUND
As development and extension of Cloud Computing technology and component of cloud computing.

2.1 Cloud computing
Cloud computing can be defined as the aggregation of computing as a utility and software as a service, infrastructure as service, platform as service Where the applications are fork out as services over the hardware and internet and systems software can provide the data centers for those services. Also called as 'on demand computing utility-grade computing', the concept behind cloud Computing is to of computer data computation to remote resource providers[2].Cloud computing system is not only storing data on the cloud servers but also shared the multiple users, and using the cache memory technique in the client to convey the data. Those clients can be PCs, laptops, smart phones and so on.

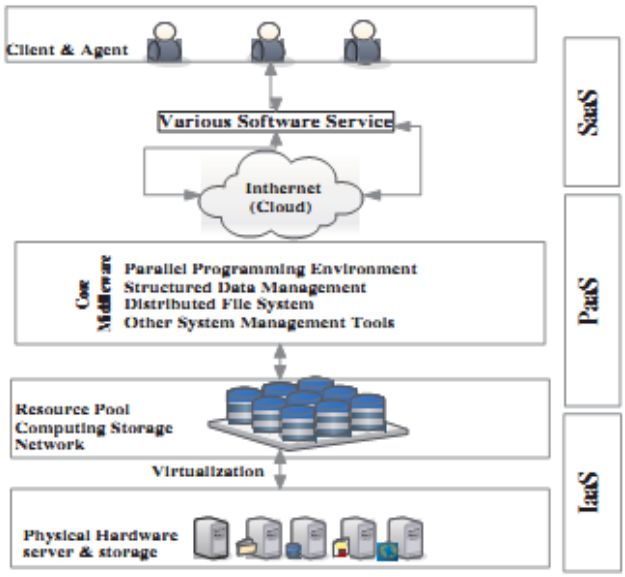

Fig: framework of cloud computing

2.1.1. Infrastructure as service layer (IaaS)
It includes resources of computing and storage. This is a bottom layer of the framework, and its having the physical devices and hardware, such as servers and storages are virtualized as a resource syndicate to provide computing storage and network services users, in order to install operation system and operate software application so it is denoted by Infrastructure as a Service. Typically services in this layer have such as Elastic Computing Cloud of Amazon.

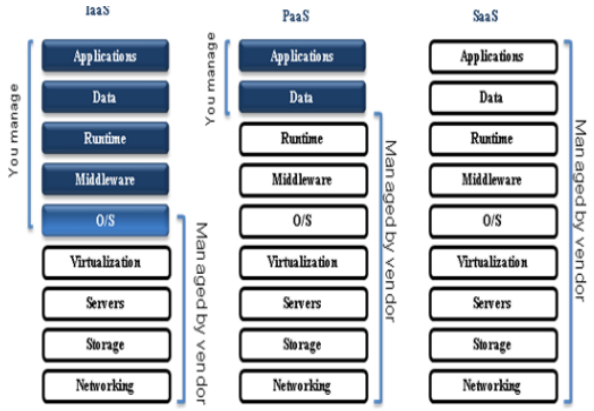

Fig: Model of cloud service

2.1.2 Platform as service layer(PaaS)

Platform as service layer is conceive as a core layer in the cloud computing system, which including the environment of parallel programmed designing ,storage distributed and management system for structured mass data, distributed file system for mass data, and different management system tools for cloud computing. Programmers are the major clients of the platform as service layer.

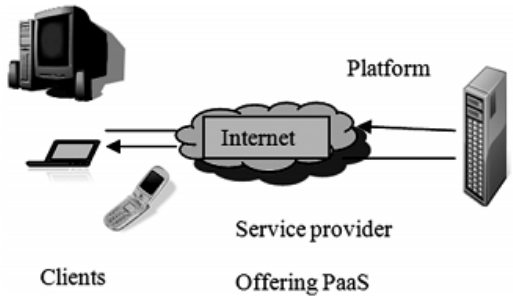

Fig: Platform as service

All Platform resources like a program testing, running and Maintenance are provided by the platform service directly but not to the end users. so, this type of services in a platform layer is Called as Platform as a Service. The typical services such as Google App Engine and Azure from Microsoft.

2.1.3 Application layer

This layer can provides simple software and applications, as well as customer interfaces to end users. so , this type of services in the application layer as Software as a Service. Users can use client software or providers can call service as browser through the Internet.

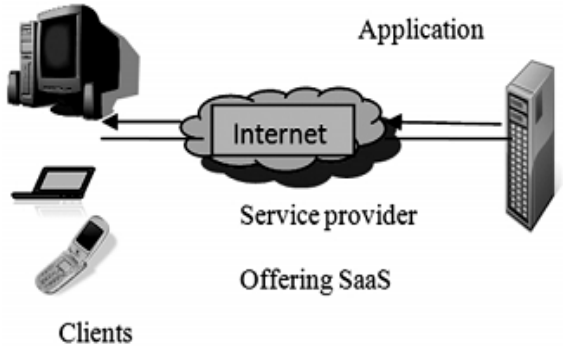

Fig: Software as service

3. PRIVACY PRESERVING METHODS

3.1 Anonymity-based

Privacy-preserving in cloud computing can be achieved using Anonymity-based method. The data and anonymity all or information should be releasing before in the cloud surrounding for the anonymity algorithm processes. Whenever cloud required, the service provider can use the background knowledge and absorb the details with the anonymous data is needed knowledge for mine [4]. So this approach totally different from the traditional cryptography technology solution for preserving the user's privacy as it acquired rid of key management and it should be stands very simple and flexile. While anonymsing is easier, the attributes anonymous varies is depends on the cloud service provider and this approach will be convenient only for limited number of services. So this method has to be best by automating the anonymisation.

3.2 A privacy-preserving Architecture

Preserving the privacy of users' data this reaching prevents the hazard of both external and internal attacks to the revamp data. The architectural main components are the user interface, user engine, rule engine and the cloud database. Through user interface can request for accessing database is occupy, and those data is sent as an XML/RPC request to the user engine, rule engine and lastly to the cloud database and each stage of requesting and responding to keep more secured the encrypting and assigning identities, also privacy is preserved together with the permutation of machine readable usage /access right. While it is more easier to accomplish the encryption schemes and it is difficulty in providing machine readable access rights. This problem of effective right expressions is bearing the future work that has to be carried out.

3.3 Privacy-Preserved Access Control

The privacy of users can proposed a flexible method of access control in the cloud environment. Certain attributes is linked with each cloud user, which resolve their access authority. Here recommend a two-tier encryption model in that first one is the base phase and second one is surface phase frame up the two tiers of the model properly. In first phase, performs the local attribute-based encryption on the data that has to be outsourced by the data owner. In second phase the surface phase performs the cloud servers, after the initialization completion by the cloud data owner.So this phase is implements the Server re-encryption mechanism (SRM)[7]. In cloud data is encrypt and re-encrypt dynamically by the SRM.The SRM arises when a new user has to be created or an existing user has to be cancel. So the re-encryption is takes place in cloud server, the privacy of users all data is not consult as the access policies remains hidden to the cloud servers. Privacy-Preserved Access Control scheme allows only valid users to decrypt the stored data. It can also preventing the different reply attacks, and achieving authenticity and privacy. But all the access policy for each record should be stored in the cloud it should be based on that cloud supervisor is honest but it doesn't support complex access control.

3.4 Auditability Schemes

Auditing Schemes reduces risk for user as well as it gives the motive to providers to improve their services. Auditability having two parts such as private auditability and public auditability. In the scheme of private auditability can get highest efficiency. Public auditability means it used publicly means to permits anyone, not just the client or user, data

owner to deal with the cloud server when there is no private information. Then, clients are smart to pass the service performance to an absolute public verifier and also without giving their computation resources [5]. So we can use the types of auditing protocols such as Data Owner Auditing and public verifier. Data storage auditing method having three parts such as: Message Authentication Code, RSA- based Holomorphic methods and Boneh-Lynn-Shacham signature (BLS) – based Holomorphic methods and. they lead to use the development of efficient privacy-preserving methods.

3.4.1 Remote Data Possession at Untrusted Host

The main target of RDP is the checking schemes. so my propose is that an efficient Remote Data Possession scheme is efficient in the computation and communication; it can allows verification and it need not for the challenger to compare versus the original data.it uses only small challenges and replies, and users necessary to store two secret keys and several random numbers. Finally using Euler's theorem and challenge is updating.

3.4.2 Public Verifiability for Storage Security

The problem is that the integrity of data storage in Cloud computing. To guarantee that the accurate of data can allows the public verifier and to work on the cloud to check then the integrity of the stored data in the cloud storage device. So this scheme is guarantee that the storage at the client side is minimum and that will helpful for other thin clients.

3.4.3 Privacy Preserving Data Integrity Checking

Public verifiability and privacy-preservation data integrity checking protocol with data dynamic make use of a RD Integrity Checking Protocol. The protocol should be provides the public verifiability. In public verifier does not leak any privacy information and it can provides well performance without help of the trusted public verifier and provides independent arbitration of data retention contracts. an efficient privacy preserving keyword search scheme in cloud computing that allows a service provider to the keywords on encrypted files and It makes use of a EPPKS also it provides to protect the privacy of user data. A privacy preservation approach for data source in cloud computing environment and that make use of Fragmentation and heuristic algorithm is used.

3.4.4 Encryption Method

Using the encryption techniques to achieve privacy in cloud and the design of privacy-preservation of cloud storage to puzzle the privacy security problem. To improve privacy with secret key the in cloud storage that should be give the permission to authorized user can encrypt his files in cloud storage. Secret sharing algorithm can used key recovering the mechanism. AES-128 to encrypt user's file and then the key length is to be set 128 bits. User also doesn't know the encryption key information that's reason Key reformation scheme partially trusted. Interaction protocol, Key derivation Algorithm, The Mix of symmetric and asymmetric encryption and Bloom Filter is using and It can operate on encrypt data and reducing the client workload on managing the data and storage space, reduced the communication. It can manage several keys and is valuable, intact and commercial.

4. SECURITY ALGORITHMS

4.1 CP-ABE Algorithms

Two methods in the fine-grained access control based on ABE first one is KP-ABE and second is CP-ABE. In KP-ABE, each of the private key attribute is link with an access structure is specifies which type of ciphertexts the key is used to decrypt, and ciphertext is labeled with a sets of attributes. In a CP-ABE system, a user's key is link with a set of attributes and an encrypt the ciphertext will specifies an access policy over attributes. In KP-ABE constitution to realized the monotones access structures for key policies. The constitution is only proved the secure for the generic group model. To overcome this problem presented another constitution that is proved to be secure under the drastic standard model. Attribute-based encryption [ABE] means that encrypted access control. Ciphertexts not necessary for encrypt to one particular user [9]. User private keys and ciphertexts link with a set of attributes or a policy over the attributes. When A match in between the user's private key and the ciphertext, then only decryption is possible.

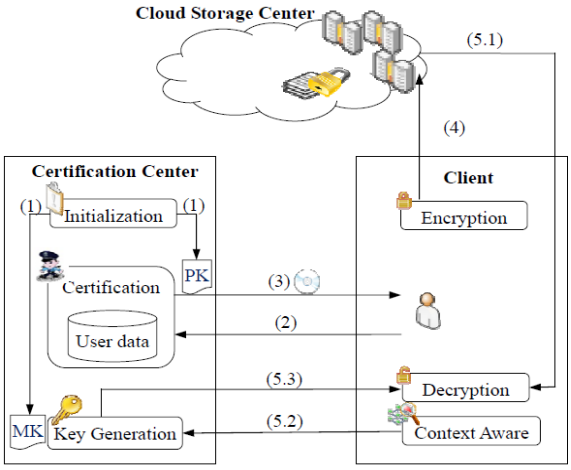

Fig: CP-ABE Algorithm structure.

- **Initialized system**-The First the certification center can generate the system security parameters like PK and MK, after transmitted PK to the user and MK to the key generation.
- First need to register for the user inputs ID and password to be log in the system.
- The user authentication unit should be verifies the CC in the first in first out manner, and then distributes the security parameter like PK and the client element to the authorized users.
- The user can accessing or receiving the data or resources from the cloud storage center.
- The context collector can collect the user's current contexts and transport or move to the key generation of the CC.
- The key generator of the CC generates decryption key according to MK and the get the contexts, and sends it to the decryption unit in the client. After decryption unit can be decrypt the resource.
- **Context-aware** -Access control is Policy based on CP-ABE algorithm with context its awareness.

4.2 Secure Hash Algorithm

Secure Hash Algorithm is one of the most important cryptographic hash functions and SHA is short. File verification purpose use SHA-1 is smart to contrast the checksums created after running the algorithms and require two files for contrasting purpose. This SHA-1 is the second iteration of the cryptographic hash function and destroy the last SHA-0. An SHA-2 cryptographic hash function is

prepared and also SHA-3 is being developed. SHA-256 transport an input messages into the 256 bits message digest[10]. SHA is use to generate the key signature. SHA having six steps:

Step 1: Padding Message: Input binary message is 1 and filled is 0 until length = 448 mod 512.Then attach 64-bit binary number. The filled message length is a Multiple of 512 bits, which decides how many '0' to be filled.

Step 2: Parsing: The padded message is separate into the N 512-bit blocks.

Step 3: Message Extension (Scheduler): Each 512 bit block can be split into 16 –bit words 32-bit words

Step 4: Message squeezing: The words from scheduler stage are then passed to the SHA squeezing function.

Step 5: The algorithm is implemented by 64-cycle repeated each block.

Step 6: After 64 emphasis of the squeezing function, an median the hash value.

5. CONCLUSION

Cloud Computing is emerging technology releases wider range of uses and increases the ease of usage by giving accessing through any kind of internet connection. Privacy problems have become very important in an cloud computing environment. So we use several techniques means use the CP-ABE Algorithm and Secure Hash algorithm to protect the user confidential data or information's.

6. REFERENCES

[1] CLOUD COMPUTING TUTORIAL Simply Easy Learning by tutorialspoint.com tutorialspoint

[2] B.Sujana1, P.Tejaswini2, G.Srinivasulu3, Sk.Karimulla4 "Secure Framework for Data Storage from Single to Multi clouds in Cloud Networking" Volume 2, Issue 2, March – April 2013

[3] Divyakant Agrawal Amr El Abbadi Shiyuan Wang "Secure and privacy preserving data Centric View.

[4] M. Suriyapriya1, A. Joicy2 "Attribute Based Encryption with Privacy Preserving In Clouds" Volume: 2 Issue: 2

[5] Neethu Mariam Joseph,Esther Daniel,N. A. Vasanthi "Survey on Privacy-Preserving Methods for Storage in Cloud Computing" (IJCA) (AICWIC'13)

[6] T. Jothi Neela1* and N. Saravanan2 Vasanthi " Privacy Preserving Approaches in Cloud: a Survey" IJST

[7] Zhou M, Mu Y et al. (2011)."Privacy-Preserved Access Control 3. for Cloud Computing", International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, 83–90.

[8] B. Raja Sekhar,B. Sunil Kumar, L. Swathi Reddy, V. PoornaChandar "CP-ABE Based Encryption for Secured Cloud Storage Access". Volume 3, Issue 9, September-2012 ISSN 2229- 5518

[9] Bethencourt, J., Sahai, A., Waters, B.: "Ciphertext-policy attribute-based encryption". IEEE Symposium on Security and Privacy, 2007

[10] Takabi H (2010). "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security and Privacy, vol 8(6), 24–31