PRIVACY PRESERVING IN CLOUD

C. BAGAVATHY RAJAMMAL

(Department of CSE, National Engineering College, Kovilpatti)

Ms. S. SAVITHA

(Assistant Professor, Department of CSE, National Engineering College, Kovilpatti)

ABSTRACT:

Cloud Computing is emerged as next generation architecture of IT Enterprise. The application software and database is moved to the large centralized data centres. A Cloud storage system consists of collection of servers for storage and also provides long term services for storage over the Internet. The Third Party's cloud system for storing data causes serious concern over 'Data Secrecy'. Therefore, new security challenges arise. This paper helps to identify the difficulties and potential security problems with full dynamic data updates from prior works and then to show how construction of an elegant verification scheme for the integration of these two features in the design. Efficient data dynamics is achieved by improving the existing proof of storage models by manipulating block tag authentication. To support multiple auditing task , the main result is extended by the technique of signature into a multi-user setting, where TPA can perform multiple auditing task simultaneously.

Keywords :TPA, PaaS, SaaS, IaaS

I. INTRODUCTION:

Cloud storage is a service which provide options for maintaining, managing and backing up the data. The service allows the user to store files online, so that they can access them from any location via the Internet. The user is concerned about the integrity of data stored in cloud. The user's data can be modified or attacked by outside attacker. Therefore, a new concept called "Data Auditing" is introduced.

The Data Auditing checks the integrity of data with the help of an entity namely THIRD PARTY AUDITOR. The purposeis to develop an auditing scheme which is secure, efficient to use and possess the capabilities such as privacypreserving, public auditing and maintaining the data integrity along with confidentiality. It consists of three entities namely,

1. Data Owner
2. TPA
3. Cloud Server

Though security is provided in a good manner, some security issues also arises. To avoid major problems an encryption scheme has been used by the users to protect their data from intruders.

Many Cloud clients tend to use their own standards and security technologies, and provide differing security models, which need to be evaluated on their own merits.

II. CLOUD:

Cloud computing is one of the practical approach to experience the cost benefits and it also has the ability to transform a data centre from a capital-intensive set up to a variable priced environment. It is a place where large pool of systems are connected in public networks or private networks that provides dynamically scalable infrastructure for data file storage and application.

1. CHARACTERISTICS:

The essential characteristics of cloud are as follows,

RESOURCE POOLING:

The resources are pooled to the server with multiple clients.

RAPID ELASTICITY:

The ability to scale quickly the in and out services.

MEASURED SERVICE:

To control and optimize the services based on metering.

2. SERVICE MODELS:

There are three service models namely,

1. SaaS – Software as a Service

   Provider applications are used and the user doesn't manage or control the network, servers, OS, storage or applications.

2. PaaS – Platform as a Service

   The user applications are deployed on the Cloud and the user doesn't manage servers, IS and storage.

3. IaaS – Infrastructure as a Service

   The access is given to the consumers to deploy their stuff and it doesn't manage or control the infrastructure but manage or control the OS, storage, application and selected network components.

3. DEPLOYMENT MODELS:

There are four deployment models namely,

1. Public
   Available to the general public.
2. Private
   Available to the single organization only.
3. Community
   Shared by the several organizations.
4. Hybrid
   Combination of one or more Clouds bounded by the standard.

4. STORAGE :

The distributed data is stored at more locations which increases the risk of unauthorized physical access to the data. By sharing the storage and networks with many users or customers provide way for other customers to access the data. The risk of having data read during the transmission can be overcome with the help of Encryption technology.

III. SNAG IN PRIVACY:

The lack of security in the Cloud include threats, data loss, service disruption, outside malicious attacks and multitenancy issues. Data security becomes a serious issue in the Cloud because data is distributed in different machines and storage devices including servers, PCs and various mobile devices such as wireless sensor networks and smart phones.

The threat of insiders accessing customer data held within the Cloud is greater as each of the delivery models can introduce the need for multiple internal users.

The threat from the external attackers may be perceived to apply more to public internet facing Clouds. However, all types of delivery models are affected by external attackers, particularly in private clouds where user end points can be targeted.

A threat from widespread data leakage amongst many competitor organizations, using the same Cloud provider could be caused by human error or faulty hardware that will lead to information compromise.

IV. RISKFUL ACTIONS IN CLOUD:

Cloud providers have unlimited access to user data. Therefore, controls are needed to address the risk of privileged user access.

Users may not know where their data is stored and there may be a risk of data being stored alongside other users information.

Data deletion and disposal in Cloud is a risk. Particularly, where data is dynamically issued to users based on their needs.

Users cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security models within their agreements.

V. PROPOSED SYSTEM:

To ensure the correctness of user data in the Cloud, an effective distributed scheme with two features opposing to its predecessors. By utilizing the Homomorphic Token with distributed verification of data our scheme achieves the storage correctness insurance and data error localization (identification of misbehaving servers).

Cloud computing is not just a Third Party Warehouse. The data stored in the Cloud can be frequently updated by the users such as,

1. Insertion
2. Deletion
3. Updation
4. Appending
5. Modification, etc…

They utilize the HARS- based Homomorphic Linear authenticators for auditing

the outsourced data and also suggest some random sampling of few blocks of file. This ring signature scheme is extended to construct our Public auditing privacy preserving mechanism. This implies that only the user in the group can generate a valid verification metadata (signatures) on the shared data.

This paper helps users to upload their files and also to preserve them with the help of encryption mechanism called Homomorphic Encryption by which the important Business files can be kept safely from the intruders.

This paper is implemented as a Web Service, which consists of three modules namely, Client, TPA and Server. The first module 'Client' includes two sub-modules as follows,

1. CLIENT REGISTRATION

In Registration module, the user can register their details to get access into the Cloud. The details such as Client Id, Password, Gender, Age, Phone number, Email-ID and date.

2. CLIENT LOGIN

In Login module, the user should enter the Client Id and Password to use the service. There is a button to generate the KEYGEN key. After entering the Client Id and Password, there is an option to generate random key by which the user get a message in his/her mail as well as mobile. The message contains the six digit key which is used to ensure that the login is attempted by the register user only.

The Client can upload files and send them to the TPA by encrypting it with nine blocks of password.

The second module is the TPA which is the login provided for the Third Party auditor, who further checks the details of the registered user and allow them to save their files in the main Server.

The third module is the Server which is the login provided for the Server and the files remain safe in the Server. Whenever the Client has the need to download the file, downloading can be done by entering the nine block password. If suppose some intruders tend to open the file, wrong password downloads the duplicate file and the original file will not be affected.

VI. HOMOMORPHIC ENCRYPTION:

It is a form of encryption that allows computation on ciphertext, generating an encrypted result which when decrypted, matches the result of the operations as if it is performed on the plaintext. The main purpose of Homomorphic encryption is to allow computation on the encrypted data.

Cloud platform can perform difficult computations on the homomorphically encrypted data without having access to the unencrypted data. Homomorphic encryption can be used to securely chain together different services without exposing sensitive data.

A Cryptosystem that supports arbitrary computation on the ciphertext is known as the fully Homomorphic encryption (FHE). Such schemes enables the construction of programs for any desirable functionality, which can be run on encrypted inputs to produce an encryption of the result.

In abstract algebra, a homomorphism is a structure-preserving map between two algebraic structures, such as groups.

A group is a set, *G*, together with an operation (called the group law of *G*)that combines any two elements *a* and *b* to form another element, denoted *ab*. To qualify as a group, the set and operation, (*G;*), must satisfy four requirements known as the groupaxioms:

Closure: For all a; b in G, the result of the operation $a \cdot b$ is also in G.

Associativity: For all *a; b*, and*c*in *G*, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Identity element: There exists an element *e* in *G*, such that for every element *a*in *G*, the equality $e \cdot a = a \cdot e = a$ holds. Such an elementis unique, and thus one speaks of the identity element.

Inverse element:Foreach*a*in*G*,thereexistsanelement*b*in*G*suchthat, $a \cdot b = b \cdot a = e$, where*e* is the identity element.

The identity element of a group *G* is often written as *1*.

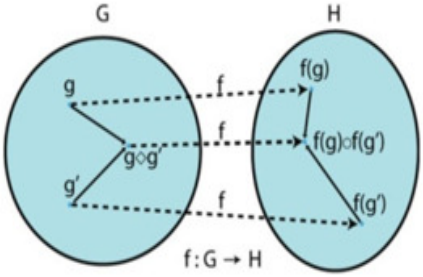
Theresultofanoperationmaydependontheorderoftheoperands.Inotherwords,theresultofcombiningelementawithelement

bneednotyieldthesame resultascombiningelementbwithelementa;theequationaıbDbıamaynotalways be true. This equation always holds in the group of integers under addition, because $a + b = b + a$ for any two integers (commutativity of addition). Groups for which the commutativity equation $a \cdot b = b \cdot a$ always holds are called abelian groups.

Giventwogroups$(G;\cdot)$and$(H;1)$,agrouphomomorphismfrom$(G;\cdot)$to $(H;1)$isafunction$f: G \to H$suchthatforall$g$andg'in$G$itholdsthat

$$f(g \cdot g') = f(g) \cdot f(g')$$

Group homomorphism can be given as follows,



Let (P; C; K; E; D) be an encryption scheme where, P; C are the plain text and ciphertext spaces, K the key space and E; D are the encryption and decryption algorithms. Assume that the plaintext forms a group (P,~) and the ciphertext forms the group $(C;1)$, then the encryption algorithm E is a map from group P to group C, i.e. $E_k: P \to C$, where k is either a secret key (in a secret key crypto-system) or a public key (in a public key crypto-system).For all a and b in P and k in K, if

$$E_k(a) \cdot E_k(b) = E_k(a \sim b)$$

Then the encryption scheme is Homomorphic.

VII. CONCLUSION:

The result of the Cloud Service as Web Service can be give as follows,

1. The Client Registers his/her details as described above.
2. Login is made successful with high security i.e.with the help of Keygen key.
3. The Client is provided with options such as to upload the file, to send file as packets to the TPA and to download the stored files.
4. File Uploading is done by protecting the specific file with the help of Homomorphic Encryption scheme, in which the file is separated into nine block packets and each packet has a particular letter or number as its password.
5. The encrypted file is sent to the TPA. Now, TPA get an alert message that a new file is ready to be stored from one of his Client.
6. TPA is provided with options such as to view the file details i.e. (size, name and type of the file), to view the Client details i.e. (all the registered Clients with the service) and to check the key response part which is helpful in sending the file back to the Client during downloads.
7. The Server (here considered as a person) who store all the encrypted files is provided with an option to get a key request message, which is sent back to the TPA and is forwarded to the Client during download session.
8. As explained above, at the time of download session, the exact password for each block which is given during packet sending session should be used to download the file with the original content else, a duplicate file will be downloaded.

Though cloud has security, to reduce the security issues this type of privacy preservation can be made which seems to be an useful scheme for those who are in need to protect their files at great ends.

VIII. REFERENCES:

[1]"SECURITY ISSUES FOR CLOUD COMPUTING", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010 39

[2]"EVOLUTION OF CLOUD STORAGE AS CLOUD COMPUTING INFRASTRUCTURE SERVICE", IOSR Journal of Computer Engineering (IOSRJCE), ISSN: 2278-0661 Volume 1, Issue 1, (May- June 2012), PP 38-45

[3]"CLOUD COMPUTING-RESEARCH ISSUES, CHALLENGES, ARCHITECTURE, PLATFORMS and APPLICATIONS: A SURVEY", International Journal of Future Computer and Communication, Vol.1, No. 4, December 2012

[4]"DYNAMIC OUTSOURCED AUDITING SERVICES FOR CLOUS STORAGE BASED ON BATCH-LEAVES AUTHENTICATED MERKLE HASH TREE", IEEE Transactions on Service Computing, Vol. PP, Issue: 99, May 2017