Providing Multi User Authentication and Anonymous Data sharing in cloud computing

Swathi Jami\textsuperscript{1}, Konni Srinivasa Rao \textsuperscript{2}
\textsuperscript{1}\ Final M.Tech Student, \textsuperscript{2}\ Asst.professor
\textsuperscript{1,2}\ Dept of CSE, Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh

Abstract: The popularity and widespread use of cloud have brought great convenience for data sharing and collection. Not only can individuals acquire useful data more easily, sharing data with others can provide a number of benefits to our society. Due to its openness, data sharing is always deployed in a hostile environment and vulnerable to a number of security threats. Taking energy usage data sharing, there are several security goals a practical system must meet. By providing security of data in a cloud we can convert data into unknown format and stored into cloud. In this paper we are proposed mainly three concepts for performing authentication of data consumers, generation of group key and provide security of sharing data in cloud. By performing authentication of data consumers we can implement the concepts for identity based digital signature. By using this concept we can verify users are authenticated or not. After completion of authentication process the cloud will generate group key and send to all group members. By using that secret key each data consumer will retrieve data from the cloud and get original plain format. Before getting original plain format data each users will perform the decryption process. In this paper we are using blowfish encryption and decryption algorithm for converting data into unknown format and get original data by using decryption process. So that by implementing those concepts we can provide more security of data and also provide efficient user authentication.

Keywords: Privacy, digital signature, cryptography, authentication, group key and forward security.

I. INTRODUCTION

Cloud computing is a technology which uses internet and remote servers to store data and application. In cloud there is no need to install particular hardware, software on user machine, so user can get the required infrastructure on his machine in cheap charges/rates. Cloud computing is an infrastructure which provides useful, on demand network services to use various resources with less effort. Features of Cloud computing are, huge access of data, application, resources and hardware without installation of any software, user can access the data from any machine or anywhere in the world, business can get resource in one place, that’s means cloud computing provides scalability in on demand services to the business users. Everyone kept their data in cloud, as everyone kept their data in cloud so it becomes public so security issue increases towards private data. Data usage in cloud is very large by users and businesses, so data security in cloud is very important issue to solve. Many users want to do business of his data through cloud, but users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data \textsuperscript{[1]}, \textsuperscript{[2]}.

Data represents an extremely important asset for any organization, and enterprise users will face serious consequences if its confidential data is disclosed to their business competitors or the public. Thus, cloud users in the first place want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors. This is the first data security requirement. Data confidentiality is not the only security requirement. Flexible and fine-grained access control is also strongly desired in the service-oriented cloud computing model. A health-care information system on a cloud is required to restrict access of protected medical records to eligible doctors and a customer relation management system running on a cloud may allow access of customer information to high-level executives of the company only \textsuperscript{[3]}. To solve the security issues in cloud; other user can’t read the respective users data without having access. Data owner should not bother about his data, and should not get fear about damage of his data by hacker; there is need of security mechanism which will track usage of data in the cloud. Accountability is necessary for monitoring data usage, in this all actions of users like sending of file are cryptographically linked to the server, that performs them and server maintain secured record of all the actions of past and server can use the past records to know the correctness of action. It also provides reliable information about usage of data and it observes all the records, so it helps in make trust, relationship and reputation. So accountability is for verification of authentication and authorization.
It is powerful tool to check the authorization policies [4]. Accountability describes authorization requirement for data usage policies.

II. RELATED WORK

In this section review related works addressing security in cloud. Security issue is very important in cloud there are many techniques available so here is review of all these. S. Pearson et al describes privacy manager mechanism in which user's data is safe on cloud, in this technique the user's data is in encrypted form in cloud and evaluating is done on encrypted data, the privacy manager make readable data from result of evaluation manager to get the correct result. In obfuscation data is not present on Service provider's machine so there is no risk with data, so data is safe on cloud, But this solution is not suitable for all cloud application, when input data is large this method can still require a large amount of memory[5]. In [6], the authors present procedural and technical solution both are producing solution to accountability to solving security risk in cloud this mechanism these policies are decided by the parties that use, store or share that data irrespective of the jurisdiction in which information is processed. But it has limitation that data processed on SP is in unencrypted at the point of processing so there is a risk of data leakage.

In [7], the author gives a language which permits to serve data with policies by agent; agent should prove their action and authorization to use particular data. In this logic data owner attach Policies with data, which contain a description of which actions are allowed with which data, but there is the problem of Continuous auditing of agent, but they provide solution that incorrect behavior. Should monitor and agent should give justification for their action, after that authority will check the justification. In [8], authors gives a three layer architecture which protect information leakage from cloud, it provides three layer to protect data, in first layer the service provider should not view confidential data in second layer service provider should not do the indexing of data, in third layer user specify use of his data and indexing in policies, so policies always travel with data. In [9], authors present accountability in federated system to achieve trust management. The trust towards use of resources is accomplished through accountability so to resolve problem for trust management in federated system they have given three layers architecture, in first layer is authentication and authorization in this mechanism requires third party services to observe network resources.

III. PROPOSED SYSTEM

Cloud computing is internet-based computing which contains large groups of remote servers that are interconnected to allow the centralized data storage as well as online access to various services or resources. Popularity of cloud computing is increasing rapidly in distributed computing environment. In this paper we are implementing cloud architecture contains mainly three concepts for authentication of data consumers in cloud, sharing of secret key in a group members and also contain concepts for provide privacy of sharing data. Cloud provides three service models, which are; platform as a service, infrastructure as a service and software as a service. Under the Database as a service, this is having four parts which are as per mentioned below.

Encryption and Decryption - For security purpose of data stored in cloud, encryption seems to be perfect security solution.

Key Management - If encryption is necessary to store data in the cloud, encryption keys can’t be store there, so user requires key management.

Authentication - For accessing stored data in cloud by authorized users.

Authorization – Rights given to user as well as cloud provider.

To solve the security issues in cloud; other user can’t read the respective users data without having access. Data owner should not bother about his data, and should not get fear about damage of his data by hacker; there is need of security mechanism which will track usage of data in the cloud. So that before store data into cloud the data owner will encrypt data using blowfish algorithm and stored into cloud. The data consumer will retrieve data from the cloud and decrypt using blowfish algorithm. Before performing encryption and decryption process each users will verify by cloud service for the purpose of authentication. In this paper we are using identity based digital signature schema for authentication of users. The implementation procedure of identity based digital signature schema is as follows.

1. Set up:

For each user, there is a secret key x which is selected by the signer, and public keys α, β, p, where: β = α^x \mod p.
The public keys $\alpha$, $\beta$, $p_i$ are published in a public file and is known to everybody while the secret key $x$ is kept secret.

$$\alpha^x = \beta \mod p_i$$

$(\alpha,\beta,p_i)$ - public key

$x(1 < x < \sqrt{(p_i)})$ is the signer's private key.

The above things are performed once by the signer. $p$ is a large prime.

2. Signature Generation

Choose a random number $k$ such that $0<k<p_i-1$ and $\gcd(k,p_i-1)=1$.

Choose a random number $t$ such that $0<t<p_i-1$ and $\gcd(t,p_i-1)=1$.

$$\lambda = \alpha^t \mod p_i$$

$$\gamma = \alpha^k \mod p_i$$

$$m = (x \gamma + k \lambda + t \delta) \mod (p_i-1)$$

Signature of user is $(\gamma,\lambda,\delta)$.

After generating signature of each user will send that signature to cloud service. The cloud service will retrieve signature and again will generate signature and verify both signatures. The verification process will be done by cloud service as follows.

3. Signature Verification

$$\alpha^m = \beta^\gamma \lambda^\delta \mod p_i$$

Using this equation the receiver verifies the authenticity of the signature by computing both sides of the equation.

4. Key Generation Process:

The cloud service will verify all users' authentication status and generate secret key for all users in a cloud. The cloud service will choose secret key and send that key all users in a secure manner. In this paper the cloud service will send secret point to individual users and using that secret point each user will get original secret key. The generation of secret points is as follows.

$$K= \text{Random} \text{(range)}$$

$$X_i = \frac{K}{P_i}$$

$$Y_i = \frac{K \mod P_i}{P_i}$$

Secret Point_i = (X_i, Y_i)

After generating secret points the cloud server will send those points to individual users in cloud. Before sending points to users the cloud server will also send status to individual users and also send secret key to data owner.

5. Encryption of sharing data using blowfish algorithm:

In this module the data owner will perform the encryption process for converting data into unknown format and stored into cloud. Before performing encryption process the data owner will retrieve secret key from the cloud service and encrypt data using blowfish encryption process. After encrypting shred data the data owner will stored into cloud.

6. Decryption of sharing data using blowfish algorithm:

In this module each user or data consumer will retrieve data from the cloud and perform the decryption process of blowfish algorithm. Before performing blowfish decryption process each user will retrieve authentication status and secret points from the cloud service. If the authentication status is true it will get secret points and generate secret key. The generation of secret key is as follows.

$$K = X_i \cdot P_i + Y_i$$

After getting secret key each user will retrieve cipher format data from the cloud and decrypt that data. After completion of decryption process each user will get plain format data.

IV. CONCLUSIONS

In this paper present an effect approach for performing authentication of data consumers and also provide more privacy of shared data in a cloud. Before performing sharing of data each user will verify by the cloud service for the purpose of authenticated user or not. After completion of authentication process the cloud service will send authentication status to individual users in cloud and also send secret key. Before sharing data in the cloud the data owner will stored data into cloud in the form of cipher format. So that by converting data into cipher format the data owner will use blowfish encryption process stored data into cloud. If any user will retrieve data from the cloud and decrypt that data.
using blow fish algorithm will get original plain format data. By implementing those concepts we improve efficiency of authentication process and also provide more privacy of shared data in cloud.

V. REFERENCES


[4]. HP Cloud website.


BIOGRAPHIES:

Swathi Jami, is student in m.tech(CSE) in sarada institute of science technology and management, srikakulam. She has received his b.tech (IT ) from Avanthi’s St.Theressa Institute of Engineering & Technology garividi (cheepurupalli), vizianagaram. Her interesting areas are network security,cloud computing.

Konni Srinivasarao is working as an Assistant Professor in Sarada Institute of Science, Technology and Management, Srikakulam, Andhra Pradesh. He received his M.Tech (cse) from Pragati engineering college,Kakinada, East Godavari,Andhra Pradesh. His research areas include Network Security and Computer Networks.