An Improved User Authentic and Privacy of Shared Data with Forward Security

Peddada Harika[1], E. Deepthi[2]

Final M.Sc. Student[1], Lecturer[2]
[1, 2] M. Sc Computer Science, Chaitanya Women's PG College, Old Gajuwaka, Visakhapatnam 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:

Put your keywords here, keywords are separated by comma.

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 [1], [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 [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

Cloud computing is the computing the resources(hardware and software) that are delivered as a service over a network .The name comes from the shape of the cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. The below Fig.1.shows that overview of cloud computing. Cloud computing presents a new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing for dynamically scalable and often virtualized resources as a service over the Internet. Now a day's most of the persons are accessing the large volumes of data from clouds. In this way they don't provide the security because of the wide adaption of cloud services. In this now I am provide the accountability and secure JVM. This two are providing the security.

Cloud computing as a fast growing technology provides many scalable services. It moves user's data to the centralized large data centers, where the management of the data and services may not be fully trustworthy. Users may not know the machines which actually process and host their data in a cloud environment. Users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant to the wide adoption of cloud services. It is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the following features characterizing cloud environments.

First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments. To overcome the above problems, we propose a novel approach, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability [3]. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information accountability focuses on keeping the data usage transparent and track able. Our proposed CIA framework provides end-to-end accountability in a highly distributed fashion. One of the main innovative features of the CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honored, but also enforce access and usage control rules as needed. Associated with the accountability feature, we also develop two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stakeholder while the pull mode refers to an alternative approach whereby the user (or another authorized party) can retrieve the logs as needed.

Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, service-oriented architecture, and utility computing. The advantages of cloud computing comprise decreased costs and capital expenses, scalability, increased operational, immediate time to promote, flexibility, and so on. Different service-oriented cloud computing models have been designed, Platform as a Service (PaaS), including Infrastructure as a Service (IaaS), and Software as a Service (SaaS). Frequent commercial cloud computing systems have been built at different levels, e.g., Amazon's EC2, Amazon's S3, and IBM's Blue Cloud are IaaS systems, while Google App Engine and Yahoo Pig are representative PaaS systems, and Google's Apps and Sales force's Customer Relation Management (CRM) System be owned by SaaS systems. The cloud service supplier directs a cloud to offer data storage service. Data owners encrypt their statistics files and store them in the cloud for sharing with data customers. To contact the shared data files, data customers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is managed by a domain influence. A domain authority is directed by its parent domain authority or the believed authority. Data owners, domain authorities, data consumers, and the conditioned authority are prearranged in a hierarchical way. The confidences authority is the root authority and responsible for organization top-level domain authorities. Data owners/consumers

may communicate to employees in an organization. Each domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain.In our system, neither data owners nor data customers will be forever online. They arrive online only when essential, whereas the cloud service provider, the confidences authority, and domain authorities are always online. The cloud is unspecified to have plentiful storage capacity and computation power. Additionally, we suppose that data customers can right of entry data files for reading only. This paper deals with a novel business model for cloud computing supported on a separate encryption and decryption service in Fig. 1. In this business model, Encryption/Decryption as a Service and Storage as a Service (SaaS) are not provided by a single operator. In Addition, the SaaS provider may not store unencrypted user data. Once the provider of Encryption/Decryption as a Service has completed, encrypting user data supplied it off to an application (e.g. a CRM system). The encryption/decryption system must delete all encrypted and decrypted user data.

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_i

where: $\beta = \alpha^x \bmod p_i$

The public keys α, β, p_i are published in a public file and is known to everybody while the secret key x is kept secret.

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

(α,β,p_i) - public key

x ($1< x <\phi(p)$) 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, pi-1) =1.

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

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

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

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

Signature of user is (γ, λ, and δ).

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 is as follows.

3. Signature Verification

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

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.

$$K = \text{Radom (range)}$$
$$X_i = K/P_i$$
$$Y_i = K\%P_i$$
$$\text{Secret Point}_i = (X_i, Yi)$$

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.

$$K = X_i * P_i + Y_i$$

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 user blowfish encryption process stored data into cloud. If any user will retrieve data from the cloud and decrypt that 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.

REFERENCES

[1] Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud,", IEEE Transaction on dependable a secure computing, VOL. 9, NO. 4, pg 556-568, 2012

[2] S.Sundareswaran, A. Squicciarini, D. Lin, and S. Huang, "Promoting Distributed Accountability in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2011.

[3] ZhiguoWan, Jun'e Liu,Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for flexible and Scalable Access Control in Cloud Computing".

[4] HP Cloud website.

[5] S.Pearson, Y. Shen, and M. Mowbray," A privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (cloudcom), pp.90-106,2009.

[6] S.Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud, " Proc First Int'l conf. Cloud Computing, 2009.

[7] R.Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.

[8] A.Squicciarini , S. Sundareswaran and D. Lin, " Preventing Information Leakage from Indexing in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2010.

[9] B.Chun and A. C. Bavier ,"Decentralized Trust Management and Accountability in Federated System," Proc. Ann. Hawaii Int'l Conf. System Science (HICSS), 2004.

[10] A.K. Awasthi and S. Lal. Id-based ring signature and proxy ring signature schemes from bilinear pairings. CoRR, abs/cs/0504097, 2005.