Security System for Cloud Based Services

Jasna Susan Alias, Manasa M, Pallavi Krishna B R, Asha Rani M*

Department of Computer Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, India

DOI: https://doi.org/10.21467/proceedings.1.22

* Corresponding author email: asharanim@gsss.edu.in

Abstract

The computer technology has come up with various technology one among is the cloud-based services have become more important and prominent. Cloud based services provide users with lots of security issues. Therefore, the study of access control scheme to protect users privacy in cloud environment is of great significance. In this paper, we present an access control scheme to the stored data in the cloud . The users who access the data stored in the cloud should request the data owner. The Key is generated in order to obtain the data. This provides the security feature to stored information. Function and performance testing shows that the PS-ACS scheme can achieve privacy protection in cloud based services.

Keywords: security; key generation; privacy protection; cloud-based services

1 INTRODUCTION

1.1 What is cloud computing?

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

1.2 How Cloud Computing Works?

The “cloud” has always been a metaphor for the Internet; in fact, cloud symbols are often used to portray the Internet on diagrams. As a virtual space that connects users from all over the globe, the Internet is like a cloud, sharing information by way of satellite networks. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

1.3 Advantages of cloud computing

Worldwide Access. Cloud computing increases mobility, as you can access your documents from any device in any part of the world. For businesses, this means that employees can work from home or on business trips, without having to carry around documents. This increases productivity and allows faster exchange of information. Employees can also work on the same document without having to be in the same place.

More Storage. In the past, memory was limited by the particular device in question. If you ran out of memory, you would need a USB drive to backup your current device. Cloud computing provides increased storage, so you won't have to worry about running out of space on your hard drive.

Easy Set-Up. You can set up a cloud computing service in a matter of minutes. Adjusting your individual settings, such as choosing a password or selecting which devices you want to connect to the network, is similarly simple. After that, you can immediately start using the resources, software, or information in question.

Automatic Updates. The cloud computing provider is responsible for making sure that updates are available – you just have to download them. This saves you time, and furthermore, you don't need to be an expert to update your device; the cloud computing provider will automatically notify you and provide you with instructions.

2 SYSTEM ARCHITECTURE

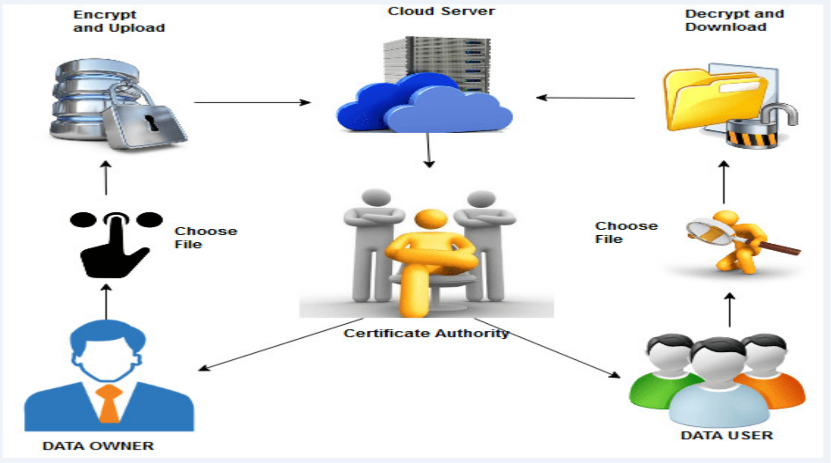

Fig2.System Architecture

In Fig2: The main actors are data owner, server, certificate Authority and users .First the data owner uploads the files to the cloud server. The User request for the files that are uploaded in the server and as the Request are send, the data owner they check whether the user is authorized are not. Later the owner asks for the key aggregate from the certificate Authority for the access permissions. After they receive the key, the user can view that file by providing access permissions to them. The user can download the respected file of their wish.

3 IMPLEMENTATION

Actors:

Cloud service provider

Certificate Authority

Data Owner

User

Actors description:

Cloud Service Provider

There are two parts of cloud service provider.

1. Data Storage Server
2. Data Service Manager

Data Storage server is responsible for storing confidential data files, and data service management is in charge of controlling external users' access to secret data and returning the corresponding cipher text.

DSS is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. All the uploaded data will be stored in Storage service provider.

DSS will be in charge of controlling the access to that data from outside users. It will be storing all the data and provides the data only to authorized users. The files which are uploaded by the Data Owner will be stored in the DSS.

Certificate Authority

In the actual cloud environment, CA manages multiple AA, and AA each manages attributes in their own field. The attributes owned by the user are issued by different authority.

Data Owner

Data Owner, based on the characteristics of users in public and personal domain to develop different access control strategy, encrypt uploaded files using the corresponding encryption method and then send to the cloud server.

User

Users, here the users may download the file of their intrest, the file or the data stored can be downloaded through a key. The key is generated and given to the users via OTP this provides security feature.

4 SYSTEM SIMULATION AND PERFORMANCE ANALYSIS

System analysis: In this system the user can only download the files of their choice. In order to download the files, the user ha store request for key, once the key is generated the user can access the file. Corresponding to the received aggregate keys the users do not have access to other files, so that the data owner controls the users access permissions. When the data file is modified, although CA is trusted, also the system parameters and revocation instructions are generated by the CA. The signature policy is formulated by the data owner and sent directly to the cloud server. The CA does not know the signature policy. Assuming that CA cannot give itself authorization, as long as the attributes of CA cannot meet the access policy, it is not valid to modify the file. The key generation is a important role in the entire system these generated keys are sent to the users via OTP to the users mail. Therefore, the user's identity is safe and key security is maintained. On the whole, the IABS scheme can protect users' identity privacy. The user's private keys are managed by multiple authorized agencies, which can avoid users' privacy leakage. Key generation is done by the random sequence of alphabet and numeric. It is done by the certificate authority, this provides a major security feature to our system and ensures the data is safe and protected from unauthorized users.

5 CONCLUSION

In this paper, we provide a security system for the cloud-based services which as highly significance in present days. In order to provide security to the data stored in cloud the key is generated and this key generation plays a very important role. The key is generated through a random sequence of numbers and alphabets. This key is given to user via OTP the users enter these keys and secret code to download. Furthermore, the paper analyzes the scheme from security and efficiency, the proposed scheme shows the feasibility and superiority to protect the privacy of data in cloud-based services. It also ensures the data is protected in the cloud environment. This idea of security system for cloud-based services can be implement in the real-time, so that no data can be accessed by any unauthorized users. It can be implied by using security features like encryption data hiding and so on.

REFERENCES

[1] S. Yu, C. Wang, K. Ren, Achieving secure, scalable, and fine-grained data access control in cloud computing, Proc. IEEE INFOCOM, pp. 1-9, 2010.

[2] J. Bethencourt, A. Sahai, B. Waters, Cipher text-policy attribute-based encryption, Proc. Security and Privacy, pp. 321-334, 2007.

[3] J. Hur, D.K. Noh, Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2011.

[4] A. Lewko, B. Waters, Decentralizing attribute-Based encryption, Proc. Advances in Cryptology-EUROCRYPT, pp. 568-588, 2011.

[5] M. Li, S. Yu, Y. Zheng, Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encryption, IEEE Transactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131-143, 2013.

[6] C.K. Chu, S.S.M. Chow, W.G. Tzeng, Key-aggregate cryptosystem for scalable data sharing in cloud storage, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, 2014.