
Cloud Computing-Data security using cryptographic technique to control Data Access Privileges in Cloud.

Maheswararao Kenguva*

Ratna Kumar J**

Abstract

In the cloud computing environment, the data security plays a major role, because the data is placed in various locations across the world. Data security and isolation protection are the two main factors of user's concerns about the cloud computing technology. Data stored in the cloud to provide data confidentiality, data integrity, data access control, and data sharing. This paper is developing a system to control the data access by the unauthorized users. Using Google App Engine to provide various types of access controls and also protect the data for the users through cryptographic technique with minimal performance degradation the data should be securely stored in the public cloud service provider. This paper describes briefly about CCAF (Cloud Computing Adoption Framework) model for securing cloud data. This system is designed based on the necessities and the execution demonstrated by the CCAF multi-layered security. CCAF multi-layered security can be categorized into three layers to protect the data in real-time: 1) firewall and access control; 2) identity management and intrusion detection and prevention and 3) Encryption. CCAF can merge with the Auditing facility to record each and every action done by the user and system details of the registered users. CCAF also achieves to identify de-duplication is performed on a single file based on their hash values. The hash numbers are relatively easy to generate. Hence it requires less processing power.

Keywords:

Isolation;
Confidentiality;
Integrity;
data sharing;
de-duplication;
CryptographicTechnique;
CCAF.

Author correspondence:

Maheswararao Kenguva,
Student of CSE Department, Baba institute of Technology and Science, Vishakhapatnam, India

2

1. Introduction

Maheswararao Kenguva

Student of Computer Science and Engineering, Baba institute of Technology and Science, Vishakhapatnam, India

Ratna Kumar J**

Head, Dept. of Computer Science and Engineering, Baba institute of Technology and Science, Vishakhapatnam, India

Cloud computing is an emerging technology to use of hardware and software resources as a service through the Internet. The Internet is a backbone of the clouds, hence the computations in the “cloud computing” done through the Internet. By using Cloud Computing, users can access database resources via the Internet from anywhere in the world and anytime can access, without any maintenance. Besides these, databases in the cloud may be highly dynamic and scalable. Cloud computing is a collection of software and hardware based on computing resources to deliver network as a service to IT companies, these services enable anytime access to a common pool of applications and resources. By using a simple web browser these applications and resources can be accessed and any authorized users can access the resources from any client device such as laptops, desktops and mobile devices.

1.1 Data security in Cloud

In the cloud, huge amount data is stored and migrates from one place to another place, meanwhile, there is a loss of confidentiality, integrity, availability, and authentication of data.

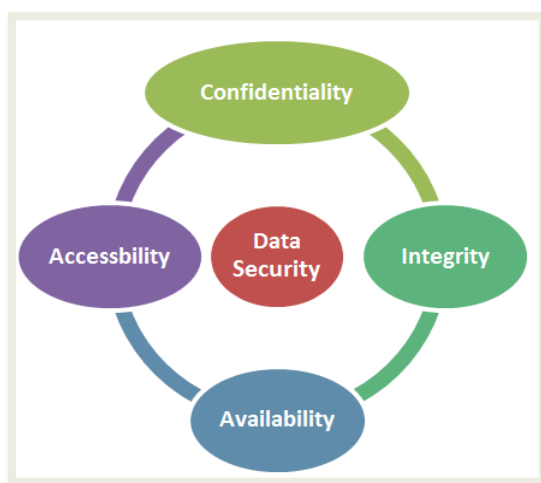


Figure 1.1 Data security factors in cloud

Data security is a major concern as entire working with data and applications depend on other cloud vendors or providers.

In the cloud systems, the user’s private information may be revealed when the service provider knows. The cloud vendors have the ability to access the personal data of the cloud user. In the cloud, the cloud vendors can characterize the import of user data.

Data Access:

In the cloud environment, the data accessibility is the main issue because there are many users can access the public data without any use even though all the resources in a cloud computing system are handled by the service providers, the user has to concern about accessing the services. Because of many technical problems arises in the cloud like loss of internet connectivity and unable to get services of the cloud. In the worst case scenario the user can lose the access to data he has stored in the cloud.

2. Related Work

Many of the research scholars provide the detailed information that related to data security in cloud computing. Hashizume[1] stated that few points about the Cloud Computing, and it presents a further level of a hazard because the sensitive information of the company stored in the cloud, but the main services are often maintained by a third party, which makes it is very complicated to maintain data security and privacy in the cloud. Cloud Computing has many features: flexibility, less cost, and a good platform for maintaining information technology and related to business services over the Internet. Amir Mohamed Talib[2] projected a MAS architecture. They are mainly categorized into five types of agents: Cloud Service Provider Agent, Cloud Data Confidentiality Agent, Cloud Data Correctness Agent, Cloud Data Availability Agent, and Cloud Data Integrity Agent. To verify our proposed security system using MAS architecture, and he is conducted a pilot study using a feedback form survey designed and implemented in Java. Using Oracle database packages and

triggers are implementing the agent functions. Ramachandran and Victor Chang [3] these two people develop a framework called CCAF and also a design a software scheme called quarantine to reduce the viruses and improve how to enforce security and ensure all users are protected. Tao Jiang et.al [4] stated an efficient public integrity auditing scheme with user revocation placed on vector commitment and verifier-local revocation group signature. In this approach, verify the integrity of dynamic data using public auditing. B. ArunaKumari [5] A Virtual Datacenter is a pool of cloud infrastructure resources designed specifically for enterprise business needs. Those resources include compute, memory, storage, and bandwidth, so it requires more security. This Paper states that encrypting the data using Data Encryption Standard Algorithm before uploading in Virtual Data center and it produces best results in computation time.

3. Methodology:

In this paper design a multi-layered approach like CCAF (Cloud Computing Adoption Framework) model to achieve the efficiency over data access for restricted users.

3.1 CCAF Framework:

CCAF provides the three-tier security model: firewall, identity management, and encryption are based on the development of enterprise file synchronization and share technologies.

Layer 1: Access Control

This layer is to allow or restrict the users depends on the access privileges and it is enforced to ensure that right level of access is only granted to the right person. Three types of access are given to authorized users.

Partial Access: Users only can view or read the files

Semi Access: Users only can view or Download

Complete Access: Users have all the rights like read, update/modify and Download.

Layer2: Identity Management

In the Identity Management layer, every cloud user has unique identity management system to control access to their personal data and the resources. The cloud providers a facility to the users incorporate the customer identity management system into their own infrastructure or provide an identity management system to the individual.

Layer3: Encryption Technique

Data is encrypted by use of cryptographic technique and upload the file to the storage cloud. Data is encrypted with the key that is randomly generated by the admin and transforms into the cipher text and uploads in the drive.

3.2 Data de-duplication:

Data de-duplication the objects usually files are compared and remove all duplicate copies of files which are non-unique. In this paper, Online data de-duplication is used which means de-duplication process is performed before storing the data in storage disk or data center.

3.2.1 File-level de-duplication: The de-duplication is performed on a single file. The files are checked based on their hash values. In this method, the duplicate files are identified. The hash numbers are relatively easy to generate. So it requires less processing power.

3.3 Roles of the modules

There are four modules are involved in this model.

- Admin
- Data Owner
- Data User
- IDs Manager

3.3.1 Admin:

Admin acts a major role in this project. It can validate both data owner and user through sending the OTP to their registered mail. It sets the access rights to the user given by the owner. It sends the file information to the public cloud service provider (GAE: GOOGLE DRIVE). It uploads or appends or edits the data as per the access is given by the owner to the user. Admin has set the user requests and Data owners and blocked users list.

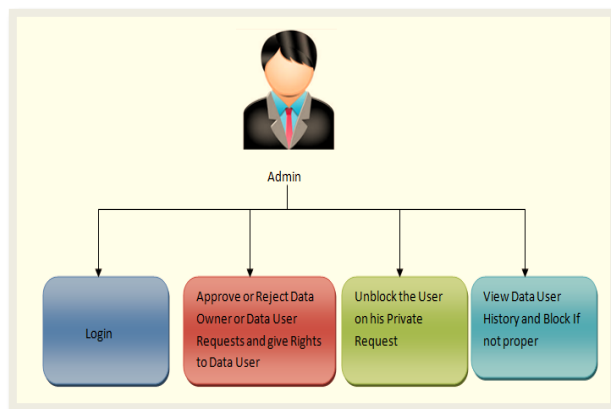


Figure 3.3.1 Admin Activities

3.3.2 Data Owner:

The Data owner is a separate type of login account. The data owner is registered with his own user id and password along with some basic details. Owner will be activated by the admin, then he has a facility to login to his account with his Username and Password along with the OTP that was reached that was sent to the owner mail id. Once the data owner is login to his account, then the owner can choose a file, which must be able to encrypt that file initially from owner side and then try to upload that into the cloud.

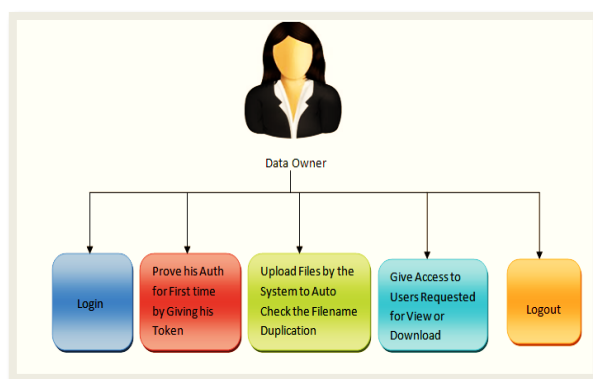
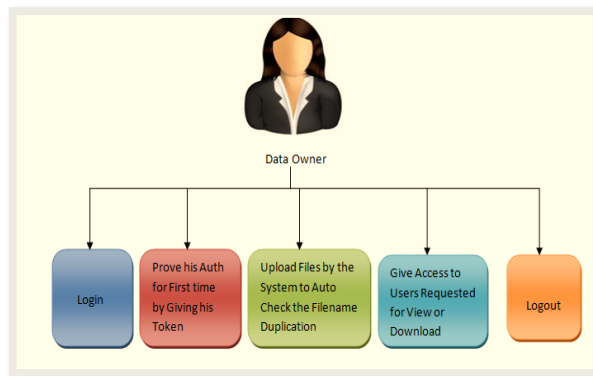


Figure 3.3.2 Data Owner Activities

3.3.3 Data User:

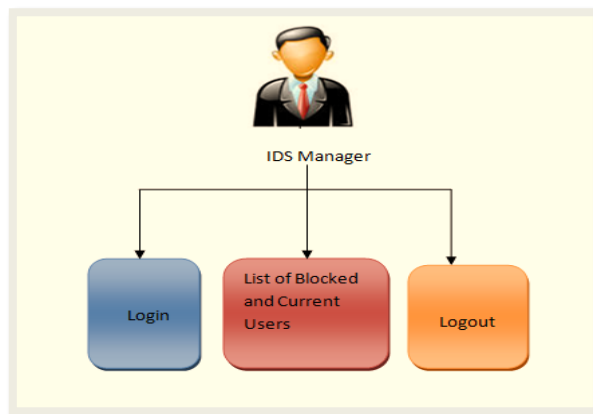
A user is a person who will initially register with his valid User id and Password and if he/she was approved by the admin user will get OTP to his mail id, through which he/she can be able to participate in the login of his account



3.3.4 IDS Manager

This is the last module where it has a facility like a login to the account with a valid login id and password, which is pre-defined earlier by the application. There will be no registration for the IDS because it is treated as an in built module in the application.

The manager has the list of all current users in a separate list view with their access rights. And also a list of all Blocked or Attacked users in a separate table with that blocked details like type of file name what they attempted and time and date. If any user who got re-access activated by admin then, that the username should be automatically enter into the normal user list from the blocked user list.



3.4 Cloud Service Provider:

The Cloud service provider is the ability to provide services to the users. CSP buys and manages the required cloud infrastructure for providing the services using the cloud software through network access (internet). The cloud service provider (CSP) has a responsibility to provide the security to the clients.

Google App Engine (GAE) is one type of service model of the cloud computing. That is Platform as a Service (PaaS), and it is a platform for developing and hosting web applications. Google has many data centers in the world. Google App Engine is used to execute web applications on Google's infrastructure.

- Very easy to build the applications.
- Less maintenance.
- Scalability one of the feature. It is easy to scale as the traffic and storage needs grow.

4. Implementation:

This project is implemented by using the .Net technology in Visual Studio 2015 IDE and cloud service provider is Google App Engine. The Back End database is SQL 2008.

- Initially, configure the Google APP Engine in Google API Console and create an Application or project with a valid mail id.

- Design front end design forms for Registrations of the user and Data Owner.

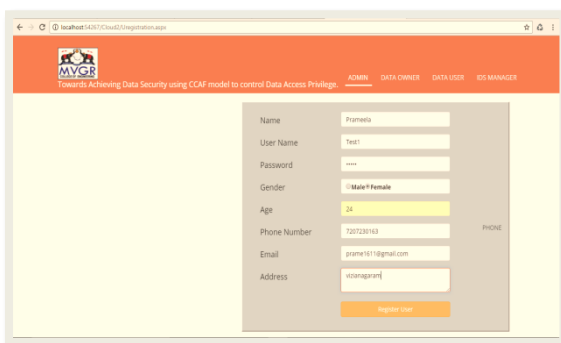


Figure 4.1 Registration page for the user.

- Token generation is implemented by use of a method with a parameter of a specific mail Id.

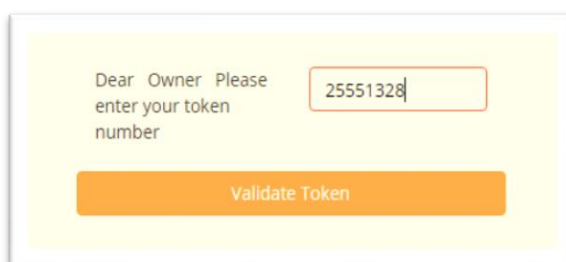


Figure 4.2 Validate token for the Data Owner

- Validate the Users or Owner through their generated tokens and set the rights by the Admin.

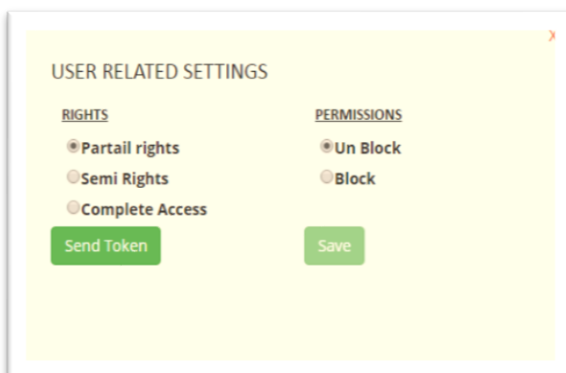


Figure 4.3 Admin set the right to the user

- Storage of encrypted files and the Usernames and passwords through the SQL Server 2008.
- De-duplication is done through the hash values generated by the admin page.

5. Conclusion and Future Work:

Security is one of the most difficult tasks to implement in cloud computing. This paper proposes a framework for security sensitive data sharing in the cloud, including secure data delivery, storage, usage, and destruction on a semi-trusted in a cloud environment. Proposed a solution based on arising needs to improve current Cloud security, offers the multilayered security layer for Cloud Computing services using GAE as cloud service provider.

This paper is uploading the text files and the documents only. My future work is to upload the different types of files formats like spreadsheets, images etc.

References

- [1] Title: An analysis of security issues for cloud computing, Author: Hashizume et al. Journal of Internet Services.
- [2] Title: Towards a Comprehensive Security Framework of Cloud Data Storage Based on Multi-Agent System Architecture. Author: Amir Mohamed Talib, Rodziah Atan, Rusli Abdullah, Masrah Azrifah Azmi Murad, Journal of Information Security, 2012, 3, 295-306.
- [3] Title: Cloud Security Proposed and Demonstrated by Cloud Computing Adoption Framework. Author: Muthu Ramachandran and Victor Chang.
- [4] Title: "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation," Author: Tao Jiang, Xiaofeng Chen, and Jianfeng Ma, IEEE 2015.
- [5] Title: "Enhancing the Security for Information with Virtual Data Centers in Cloud," springer link, vol. 143, pp. 277-282, 2012. Author: B. ArunaKumari, J. VenkataRao V. Sreenivas.
- [6] Title: "Business intelligence as service in the cloud," Author: V. Chang, Future Gener. Comput. Syst., vol. 37, pp. 512-534, 2014.
- [7] Title: A Platform Computing Whitepaper. "Enterprise Cloud Computing: pp6, 2010.
- [8] Title: "Secure Auditing and De-duplicating Data in Cloud", 2015 IEEE TRANSACTIONS ON COMPUTERS. Author: Jingwei Li et.al.
- [9] Title: "The Threats of Data Security over the Cloud as * Perceived by Experts and University Students", Author: Louai A. Maghrabi, 2014 IEEE.
- [10] Title: "SeDaSC: Secure Data Sharing in Clouds", Author: Mazhar Ali et al 2015. IEEE SYSTEMS JOURNAL.
- [11] Title: "An Analysis of the Cloud Computing Security Problem" Author M. A. Morsy, J. Grundy and Müller I. In PROC APSEC 2010 Cloud Workshop. 2010.
- [12] Title "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", Author: Rashmi, Dr.G.Sahoo and Dr.S.Mehfuz, International journal on cloud computing: services and architecture (IJCCSA), vol.3, no.4, august 2013.
- [13] Title: "Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments". Author: Jeong-Min Do et. al, 1st IEEE ACIS/JNU int. conference on computers, networks, systems, and industrial engineering (cnsi 2011), korea.
- [14] Title: "Proficient privacy Keyword Search over Encrypted Cloud Data," " Author: Kedarnadh, | B.Aruna kumari Kasamsetty, IJSRCSAMS, vol. 3, no. 5, september 2014.