

Data Security Using Multi-Layered Model to Control Data Access Privileges in Cloud

K.Prameela Rani

**M.Tech (CSE Branch),
Dept of CSE,
MVGR College of Engineering,
A.P, Vizianagaram, India.**

B.Aruna Kumari

**Associate Professor,
Dept of CSE,
MVGR College of Engineering,
A.P, Vizianagaram, India.**

Abstract:

Now-a-days, data security has constantly been a major issue in the cloud computing environment, because the data is located at different places across the world. Data security and isolation protection are the two main factors of user's concerns about the cloud technology. Data stored in the cloud to provide data confidentiality and integrity, data access control, and data sharing. This paper is developing a system to control the data access by the un-authorized users. By giving different types of access for the users and also protect the data by cryptographic technique with minimal performance degradation the data should be securely stored in the public cloud service provider, which is Google App Engine. This paper uses a brief layout of 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 protect data in real-time and it has three layers of security: 1) firewall and access control; 2) identity management and intrusion prevention and 3) Encryption. CCAF can be more effective when combined with Auditing facility to record the actions done by the user and system details of the registered users. This system also achieves to identify 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.

Keywords:

CCAF, Isolation, Confidentiality, Integrity, de-duplication, Cryptographic Technique.

1. Introduction:

Cloud computing is utilize of computing assets (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a 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. It 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. Cloud services are available on-demand and often bought on a "pay-per-use" or subscription basis. Cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down and also providing on-demand utility-like model of allocation and consumption.

1.1 Data security in Cloud:

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



Figure 1.1 Data security issues in cloud

Towards data security, where user's information may be disclosed when service provider knows where the user's private information resides in the cloud systems. The cloud service provider has the authority to access and gather user's private information in the cloud systems. And also the service provider can figure out the significance of user's information in the cloud systems.

Data Access:

In cloud environment 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 technological problems 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 on the cloud.

2. Related Work:

Many research work has been carried out related to data security in cloud computing. Hashizume[1] states that Cloud Computing presents a further level of hazard because critical services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability of data. Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Amir Mohamed Talib[2] proposed a MAS architecture includes main five types of agents:

Cloud Service Provider Agent (CSPA), Cloud Data Confidentiality Agent (CDConA), Cloud Data Correctness Agent (CDCorA), Cloud Data Availability Agent (CDAA) and Cloud Data Integrity Agent (CDIA). In order to verify our proposed security framework based on MAS architecture, pilot study is conducted using a feedback form survey. He design a prototype of the system is implemented using Java. To simulate the agents, oracle database packages and triggers are used to implement agent functions and oracle jobs are utilized to create agents. 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] provides an efficient public integrity auditing scheme with user revocation placed on vector commitment and verifier local revocation group signature. In this technique public auditing is done to check the integrity of dynamic data. B. Aruna Kumari [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 centre 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 multilayered security is based on the development and integration of three major security technologies: firewall, identity management, and encryption based on the development of enterprise file sync 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:

This layer provides for every data user or data owner will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure or provide an identity management solution of their own.

Layer3: Encryption Technique:

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

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 given by the owner to the user. Admin have set the user requests and Data owners and blocked users list.

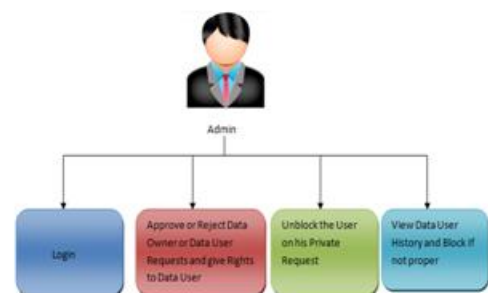


Figure 3.3.1 Admin Activities

3.3.2 Data Owner:

Data owner is a separate type of login account. Once 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 into his account with his Username and Password along with the OTP that was reached that was send to the owner mail id. Once the data owner is login into his account, then 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.

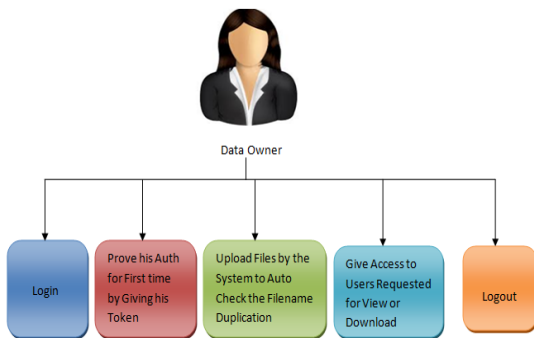
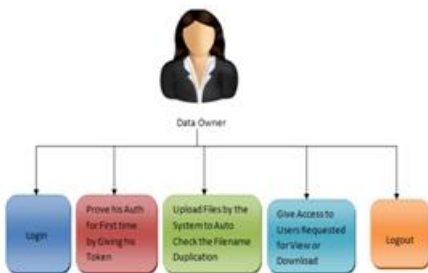


Figure 3.3.2 Data Owner Activities

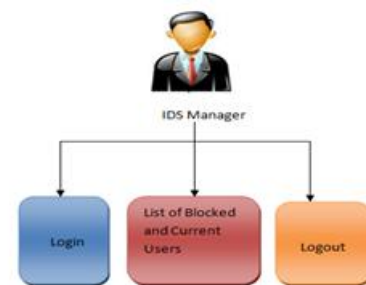
3.3.3 Data User:

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 login into 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. 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 user name should be automatically enter into the normal user list from the blocked user list.



3.4 Cloud service Provider:

The CSP, or cloud provider, is the entity of providing the cloud service, which acquires and manages the infrastructure required for providing the services, and runs the cloud software that provides the services, and also delivers the cloud services through network access. Cloud security is a shared responsibility between the cloud service provider (CSP) and its clients.

Google App Engine (GAE) is a Platform as a Service (PaaS) cloud computing platform for developing and hosting web applications. Google-managed data centers. Google App Engine lets you run web applications on Google's infrastructure.

- It is easy to build.
- It is easy to maintain.
- 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. Back End data base 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.

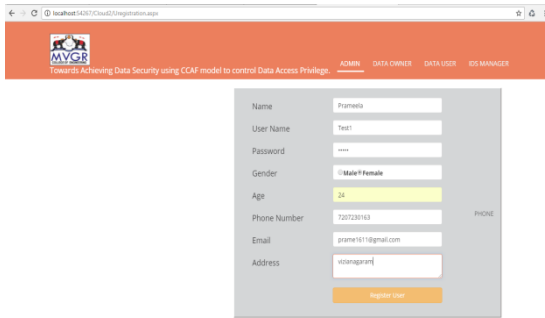


Figure 4.1 Registration page for the user.

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

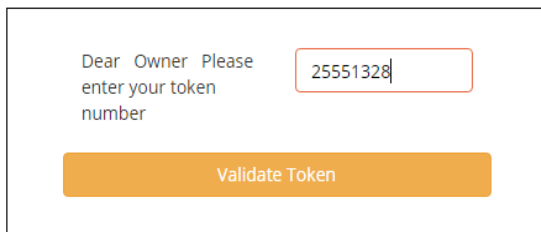


Figure 4.2 Validate token for the Data Owner

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

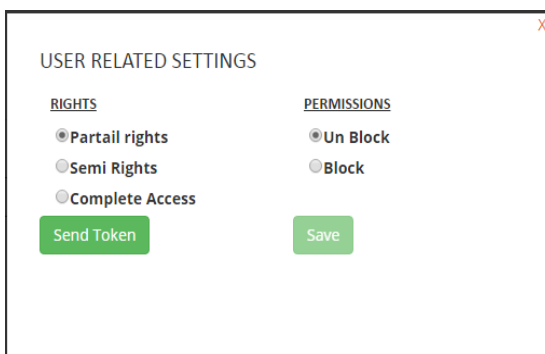


Figure 4.3 Admin set the right to the user

- Storage of encrypted files and the User names 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 task to implement in cloud computing. This paper proposes a framework for secure sensitive data sharing in cloud, including secure data delivery, storage, usage, and destruction on a semi-trusted in 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 only. My future work is to upload the different types of files formats like spreadsheets, images and documents etc.

6. 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 CloudComputing: 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.Arunakumari Kasamsetty, IJSRCSAMS, vol. 3, no. 5, september 2014.