International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

A Cloud Architecture for Privacy Preserving on Cloud Storage using Secured Private and Public Keys

Sai Priya.P & Dr.K.Venkata Subba Reddy

[1]PG Scholar, Department of CSE Malla Reddy Engineering College (Autonomous)

[2]Professor, Department of CSE Malla Reddy Engineering College (Autonomous)

Mai Id: - saipriya.panduga@gmail.com & **Mail Id: -** kvsreddy2012@gmail.com

ABSTRACT

Cloud computing is the use of internet for performing the tasks in the system. The cloud services are the applications to the end users. This is a best efficient way for organizing and managing applications by Cloud service provides, there are three ways providing the services such as Infrastructural, Platform, and application services to the end users. The applications of cloud is Google drive, Amazon cloud services etc. The problem or challenges of cloud data is security, this can be provided by in the cloud environment to cloud servers and users, but existing methods increasing the maintenance and management. The proposed model privacy preserving on cloud data storage with public and private keys, the model has three objectives key distribution, access control and protection of attacks with little management. The model Architecture is described with modules and the results shown. In future the model can be extended for secure communication un-trusted clouds.

Keywords: - Security, Cloud computing, Access control, Privacy, key generation .

1. INTRODUCTION

Cloud computing is data utilization of resources on internet, with Platform as Service, Infrastructure as Service, and Application as service. Cloud data sharing, maintenance and management of systems. Cloud computing needs low maintenances, high storage capacity, with reliable services at high security and the system management local management in the cloud data servers. Distributed computing the providing the services with local and at least one global application at remote system which can be accessible via internet. The distributed application information shared among the users. The users may be cloud users, access the information from cloud data servers.

Now a day's large amount of data is generated and stored by the systems, these data can be stored by cloud service providers.

Cloud service providers, administrators provide high security. The security provided by cryptography, verification of remote cloud data by third party auditors.

Cloud users, Cloud service provides, and security algorithms. Security by public and private keys, encryption and decryption methods. User can send the request the data, the information is stored in the cloud data with encryption way. The user can decrypt the key using public and private keys. Key generation plays significant role in the cloud data retrieval by authenticated users. Key generator, code generator, and verifier with security mechanism in the cloud environment.

2. RELATED WORK

2.1 Existing System

Kallahalla et al secured data sharing in unworthy servers due to heavy key distribution and overhead.
Yu et al , proposed re-encryption to achieve data access and control without disclosing the data contents., they used two keys attribute key and group signature key for privacy and preserving and tractability.
Lie etl proposed data sharing to achieve fine access control and revoke the uses who are unable to access the sharing of data. And others presented a secured access control scheme in cloud storage by role based encryption technique.

2.2 Proposed System

In this paper, we propose a model, data sharing in the cloud requires data privacy for upload and download the documents, secure sharing on un-trust servers using security techniques.
User has two keys
1. Attribute key: Used to decrypt the data on encrypted messages
2. Group signature key: used for privacy and traceability Authors suggested a model has cloud, Group manager and Group members.

Cloud: It can be used to provide the resources

Group manager: send the file with key distribution to the group members.

Group members; Group members receives the key distribution and registration of the user under the group manger.

The Group manger can upload the data file into the cloud; the authenticated group members who registered under group manger can receive the files from the cloud using the decryption methods.

The Design Goals are key distribution, Access control, Data confidentiality and efficiently.

Key distribution: The user will get private key from group manger with Certificate Authorities.

Access control: First of the group members who are the registers for services only can access the cloud data.

Data confidentiality. Unauthorized uses not able to store and access the data and maintain available for authorized users with security mechanism (encryption and decryption techniques)

3. CLOUD DATA SECURITY

3.1 Security:

Security is the one of most important and essential for cloud based applications the security can be implemented in following ways by Chris J Mitchell[11] confidentiality: The Information cannot be disclosed to unauthorized users.

Data integrity: The information cloud data cannot be modified by Un-authorized users. Non repudiation: Denying access for un-authorized users, relevant action for suspicious attacks. Availability: The cloud data services always available for cloud authentication users.

Security Analysis: The analysis of security [1]

(i). Key distributions: Public key and private key. The public key is shared to all the users known and shared to public, where as private means it is protected and only accessible, shared to authenticated users.
(ii). Access control: Access control is based on the security privatizes given to user in the group. This is generally performed in the cloud, and verified by group manger.
(iii). Data confidentiality: is the protecting data on the cloud and content is stored with high security.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

4) PROPOSED ARCHITECTURE AND IMPLEMETATION

4.1. Architecture**:** The Figure.1.shows the proposed architecture it has three components

1) Cloud Data services(IaaS, PaaS, and AaaS)
2) Cloud Group manager
3) Cloud group members

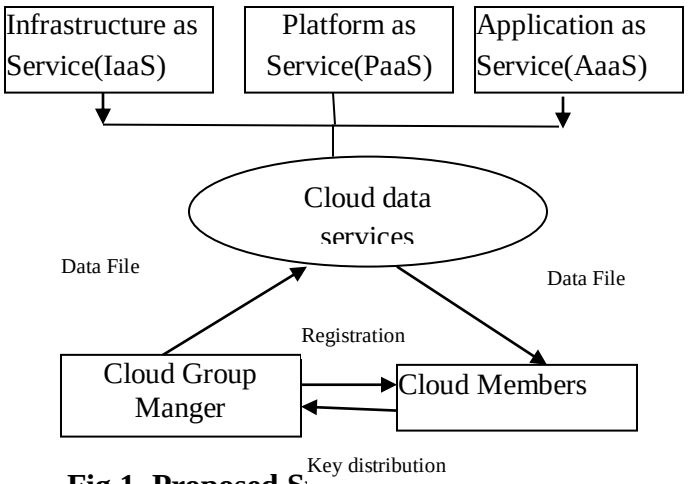

Fig.1. Proposed System model

Cloud data services has three kind of services, infrastructure as Services (PC, networks, communications and others facilities for cloud applications) Platform as service: Services like operating systems, middle ware and other services. Application as a service: The cloud server will provide the application services. for example it can be memory, applications and other services.

4.2 Modules:

The proposed model has six modules

1) cloud module: This is used for creating local cloud and storage with security

2) Group Manager Module is responsible for system parameter generation, user generation, user revocation and revealing the real identity of a dispute data owner

3) Group member module is responsible for group users accessing file securities and storage in the cloud system

4) File security module is responsible for files stored in the cloud with encryption and decryption techniques

5) Group security module: is deals with user invocations, registrations, users to allow sign the messages with secret verification

6) User revocation module: It is used for revocation of group manager by using public available revocation list based on group member's confidentiality.

3.1Cloud Module:

In this module is responsible for neighborhood Cloud and give estimated cloud storage and price. The clients can transfer their information in the cloud. This is build up in distributed storage with security. It has Cloud service provides used for trusted domain service applications.

3.2Group Manager Module:

It deals with group management and security and access previlizes to the users who are in the group. This is responsible for system parameters generations, user registrations, user revocations and revealing the real identity of the user with dispute of ownership. wal also.

3.3 Group Member Module

This responsible for Group members who are registered users can store their private data on cloud server and share the same with the group members.

3.4 File Security Module:

This is responsible for files security management and stored files can be accessed

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

to with group manger guidelines to the group members

3.5 Group Signature Module

This responsible for Group identity from verifiers, in the designated group manger can reveal, signature originator, when a dispute occurs and traces information.

3.6 User Revocation Module

This module is Group manager can be available revocation list based on the group members security privileges.

4.3 Implementation with Experimental Results

The proposed model is implemented in Java/J2EE, and tested and the results shown in the following.

Fig. 2. Home Page for Cloud Storage

The figure.2. shows the home page of the proposed application with Home page contains, Home, Group manager, Group Members and Member register.

Fig 3 Registration Page for Members

The figure.3 shows the registration page for the members with form layout contains username, password, confirm password, group, Emailid, mobile number and place details. After registration details entered successfully the details will be stored in cloud database.

Fig 4. View Group details.

In the Figure.4. shows the group information contains user-id, file name, group, status and date. This is used to view the group information.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

Fig 5. File upload Page

The Figure.5. shows the File upload with security techniques.

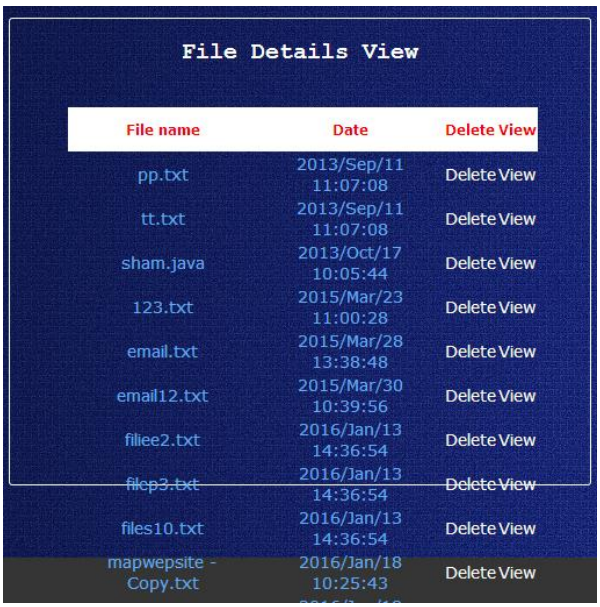

Fig 6 File Download Details from the Cloud

The Figure. 6. Shown the files download information when user want to download the file he/she has be a members in the group with security privileges.

5. CONCLUSION

In this paper it is proposed a model architecture is shown in Figure.1. cloud data shared, security by key distribution, access control and protection of attacks, with low maintenance, little management cost, the goal is privacy preservation of cloud data to dynamic groups. The model has three components cloud data service (which as Infrastructure as Service, Platform as Service and Application as Service), Cloud Grou The proposed model is implemented in Java/J2EE and outputs shown in Figures. 2 to 6., to create , store manage the cloud application.

6.REFERENCE

[1] M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz,A.Konwinski, G. Lee, D.Patterson, A.Rabkin, I.Stoica, andM.Zaharia. "A View of Cloud Computing,"Comm. ACM, vol. 53,no.4, pp.50-58, Apr.2010.

[2] S.Kamara and K.Lauter,"Cryptographic Cloud Storage," Proc.Int'l Conf.Financial Cryptography and Data Security (FC), pp.136-149, Jan. 2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K.Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[4] E.Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and

DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003.
[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.
[6] Shucheng Yu, Cong Wang, KuiRen, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006
[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography,
[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.
[11] Chris J Mitchell on "SECURITY TECHNIQUES", 1-6
[12] Manjur Kolhar,Mosleh M. Abu-Alhaj, and Saied M. Abd El-atty on "Cloud Data Auditing Techniques with a Focus on Privacy and Security". IEEE. 2017, pp. 42-51