International Journal of Research in Engineering, Science and Management
Volume 5, Issue 3, March 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

Secure File Storage on Cloud Using Cryptography

R. Purushothaman[1], A. K. Thejasree[2*], K. Udaya Bhaskar[3], B. Santhosh[4], K. Sai Sravya[5], M. Harshavardhan[6]

[1]*Associate Professor, Department of Computer Science and Engineering, Siddartha Institute of Science and Technology, Puttur, India*
[2,3,4,5,6]*Student, Department of Computer Science and Engineering, Siddartha Institute of Science and Technology, Puttur, India*

***Abstract*: Security in cloud computing is the emerging research issues nowadays. A lot of organization is moving from their traditional data storage to cloud storage, which provides an efficient way to access the data anywhere and anytime This paper proposed a cryptography-based security system for cloud computing. This model is an approach of cryptography algorithms. In this Advanced Encryption Standard (AES) are implemented to provide the encryption and decryption which increase the security of the cloud storage. This security model gives the transparency to the cloud user as well as cloud service provider in order to reduce the security threats. This model increases the data security up to a maximum extant and it takes less time in uploading and downloading the text file as compare to existing system.**

***Keywords*: Cloud computing, security, cloud storage, cryptography, encryption, decryption, upload, download, text file, data security, cloud service.**

1. Introduction

Cloud computing is emerging as the most suitable paradigm for individuals and organizations to access inexpensive, scalable, ubiquitous, and on-demand computing resources, applications, and data storage services. Cloud storage systems, such as Drop box, Google Drive, Apple's, i Cloud, Microsoft One Drive, etc., enable users to remotely store a large volume of data that can be accessed and shared among users, regardless of time and location constraints.

Cloud computing is a technology that uses the internet for storing and managing data on remote servers and then access data via the internet. This type of system allows users to work on the remote. It is an application-based software infrastructure that stores data on remote serves, which can be accessed through the internet. It can be divided into front-end and backend. Cloud computing is a general term for anything that involves delivering hosted services over the internet. These services are divided into three main categories or types of cloud computing: infrastructure as a service, platform as a service and software as a service.

2. System Design

The fig. 1 shows the system architecture.

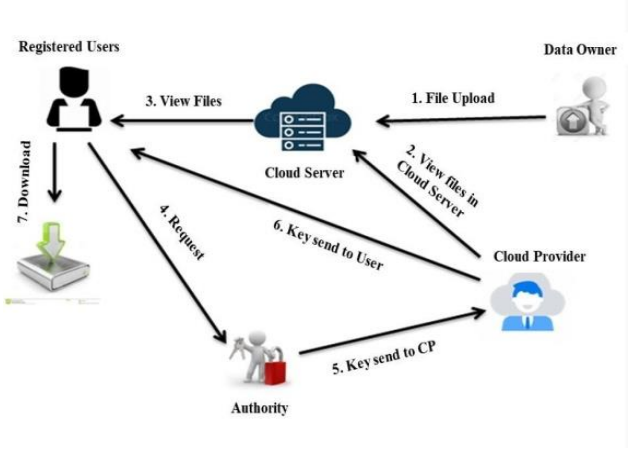

Fig. 1. System architecture

3. Module

A. *Data owner for uploading file in a cloud*

Data owners can perform the functions like Registering the owner, uploading the file, view the files and view the requests for a file.

- *Register:* Data owner can Register and login with valid credentials.
- *Upload File:* Data provider can upload the file on the cloud.
- *View File:* Data Owner can view uploaded file once means whether the file is correctly uploaded or not.
- *View Requests:* Data user can send the request to download a file. Authority can accept that requests and send data to Data owner for download the file.

B. *Registered users to download files from cloud*

Data Users can perform the functions like Registering the user with proper details and login with credentials, view the required files, get the keys from cloud and download the files.

- *Register:* Data user can do registration with his details for download a file.
- *Login:* The user needs to register and the data stored in My SQL database.
- *View all Files:* User can view files and send request to authority for download the file.
- *Get Key & Download:* Once User Request can

*Corresponding author: creativethuls05@gmail.com

accept by authority, they will send key to cloud. Cloud send key to user and then user can download the file.

C. Authority for views users request generating keys

Authority can perform the operations like login with proper credentials, view the user requests for the files and generate the keys to cloud.

- *Login:* Authority can login with his/her credentials.
- *View Users Requests:* Authority can view the user requests for file downloading.
- *Generate Key:* Authority can accept that requests and send key to cloud server.

D. Cloud provider for managing files in cloud server

Cloud Provider can perform many functions like login to browser and view the files uploaded b owner, view the number of users and data owner's login to cloud and send the keys to users for download the files.

- *Login:* Cloud server can login with his/her credentials in website.
- *View Files:* Cloud provider can view all uploaded files by the data owners.
- *View Users:* Cloud provider can view all the users' details to give permission for login the website.
- *View Data Owners:* Cloud provider can view all the data owners' details to give permission for login the website.
- *Send Key:* Cloud provider get a key from Authority and send to the users.

References

[1] S. Lu and A. I. A. Abomakhelb, "Secure Cloud Storage and Quick Keyword Based Retrieval System," 2017 International Conference on Computing Intelligence and Information System (CIIS), 2017, pp. 201-207.

[2] Sumathi, M., Sangeetha, S. A group-key-based sensitive attribute protection in cloud storage using modified random Fibonacci cryptography. Complex Intell. Syst. 7, 1733–1747 (2021).

[3] Madhumala R. B, Sujan Chhetri, Akshatha K. C, and Hitesh Jain, "Secure File Storage & Sharing on Cloud Using Cryptography," in International Journal of Computer Science and Mobile Computing, vol. 10, no. 5, pp. 49-59, May 2021.

[4] K. V. Pradeep, V. Vijayakumar, V. Subramaniyaswamy, "An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment", Journal of Computer Networks and Communications, vol. 2019, 2019.

[5] Singh, N., Singh, A.K. Data Privacy Protection Mechanisms in Cloud. Data Sci. Eng. 3, 24–39 (2018).

[6] K. Subramanian and F. L. John, "Dynamic Data Slicing in Multi Cloud Storage Using Cryptographic Technique," 2017 World Congress on Computing and Communication Technologies (WCCCT), 2017, pp. 159-161.

[7] R. Nivedhaa and J. J. Justus, "A Secure Erasure Cloud Storage System Using Advanced Encryption Standard Algorithm and Proxy Re-Encryption," 2018 International Conference on Communication and Signal Processing (ICCSP), 2018, pp. 0755-0759.

[8] B. Mishra and D. Jena, "CCA Secure Proxy Re-Encryption Scheme for Secure Sharing of Files through Cloud Storage," 2018 Fifth International Conference on Emerging Applications of Information Technology (EAIT), 2018, pp. 1-6.

[9] P. Ribeiro, R. Prior and S. Crisóstomo, "Secure File Storage for Android Devices on Public Clouds," 2019 IEEE 8th International Conference on Cloud Networking (CloudNet), 2019, pp. 1-4.

[10] H. Deng et al., "Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3168-3180, 2020.