Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.192 – 195

Cloud Storage Security with Double Encryption Policy

Vishesh Gaikwad, Anand Shangarpawar, Akshay Wankhede, Amol Ghodmare, Mohanish Ganorkar
Department of Computer Science, RTM Nagpur University, Nagpur, India
gaikwad.vishesh7@gmail.com, anandshangarpawar@gmail.com, akshay.official1993@gmail.com, amolghodmare05@gmail.com, mohanish05@gmail.com

Abstract— This paper shows that cryptography can be used to efficiently provide security and privacy for the next generation cloud systems. We focus on deploying the most fundamental data services, e.g., data management and data utilization, while considering reliability and privacy assurance.

Keywords— AES, DES, Cloud Storage

I. INTRODUCTION

In the digital world using technology and new technologies require safe and reliable environment, and it also requires consideration to all the challenges that technology faces with them and address these challenges. Cloud computing is also one of the new technologies in the IT world in this rule there is no exception. According to studies one of the major challenges of this technology is the security and safety required for providing services and build trust in consumers to transfer their data into the cloud. In this paper we attempt to review and highlight security challenges, particularly the security of data storage in a cloud environment. Also, provides some offers to enhance the security of data storage in the cloud computing systems that by using these opinions can be overcome somewhat on the problems.

Here, we design a secure virtual cloud storage service which addresses the reliability issue with security of the confidential data. Client-server type storage and computation outsourcing constitute some of the major applications that the next generation cloud schemes will address. Since these applications are just emerging, it is the perfect time to design them with security and privacy in mind. Furthermore, considering the high-churn characteristics of such systems, the cryptographic protocols employed must be efficient and scalable.

The proposed system is a web based application which maintains a centralized repository of all necessary information. This allows the users to access the information easily. The system allows to track and manage all information through well-defined interfaces.

II. OBJECTIVE

The objective of this application is to make sure the security of the file storage. In this project-

- User can register their details.
- The administrator can view all details of the new user and authorize the user.

- The administrator provides a master key to every user.
- The administrator allow user to login and upload their file in the cloud storage.
- The user login and upload their files into the cloud storage. The user gives a private key to encrypt the file and also applies master key to again encrypt the file.
- The user can change their password. The user can view all uploaded file in the cloud storage.
- If the user wants to download a file, the user must give the correct private key and master key.
- If the user gives the correct secret key while downloading the original file will be downloaded, else the encrypted file is downloaded.
- Also the user wants to delete his uploaded file, the user must give the correct secret key else the user cannot delete the file.
- The user can view all uploaded file.
- The administrator can view all user details also can view all uploaded files, but cannot open them.

Admin involves the followings: -

- Can view the new user details.
- Can authorize the user to upload the files in to the cloud storage.
- Can view all uploaded files.
- Can view all existing user's details.

User involved the followings: -

- Can register to the cloud storage.
- Can login and upload their files.
- Can view all uploaded files.
- Can download the file by giving the correct secret key.
- Can delete the file by giving the correct secret key.
- Can change the password.

III. MODULES

User account management

The administrator can view the new user details and authorize the user to upload the files in to the cloud storage. The administrator can view all uploaded files. Also can view all user's details.

New User

In this module the Admin can view the new user details. The admin authorizes new user to upload their files. If the admin not authorize the user, the user could not login.

User Details and file details

In this module the Admin can view the All user details. The administrator generates reports based on the user details. Admin can view the uploaded files details. The administrator generates reports based on the uploaded details.

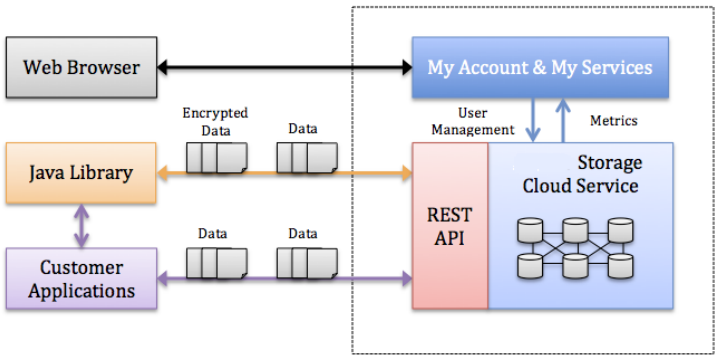

Fig. 1 Working of Cloud Storage

Splitting & Encrypting file

Splitting a single file into sequential segments and Encrypting the file. The user module consists of the file upload. In this module the user can upload the files. The user should give a private key while file uploading. This secret key and the uploading files are stored in encrypted form then user applies the master key known to both user and admin and again the file is encrypted.

For this purpose, we are using DES algorithm and AES algorithm.

Storage Cloud Service

The program creates a connection to your MySQL Storage instance.

Downloading Manifest Object

The Manifest Object has been created successfully, the Java program downloads it and saves it as a local file.

If the user wants to download a file, the user must give the correct secret key. If the user gives the correct secret key while downloading the original file will be downloaded, else the encrypted file is download. Also the user wants to delete his uploaded file. The user must give the correct secret key else the user cannot delete the file.

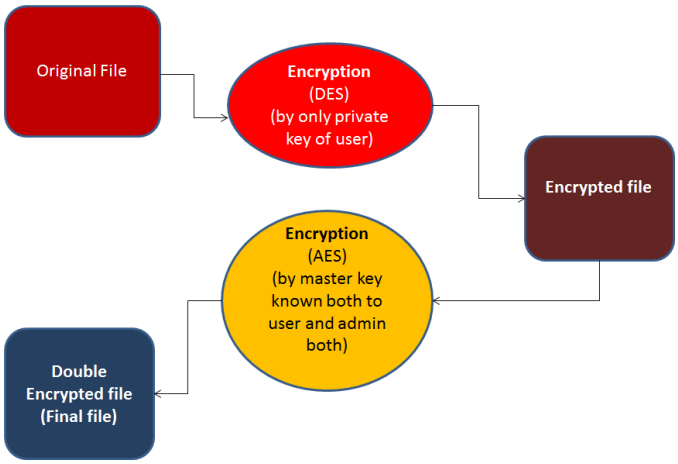

Fig. 2 Encryption Process

IV. CONCLUSION

From a proper analysis of positive points and constraints on the component, it can be safely concluded that the product is a highly efficient GUI based component. This application is working properly and meeting to all user requirements. This component can be easily plugged in many other systems. Storage security on cloud using secret key which provides reading services to its members. Any person can become a member by filling a registration form.

REFERENCES

[1] Cloud Security Using Third Party Auditing and Encryption Service Dissertation Submitted in partial fulfillment of the requirements for the degree of Master of Technology, (Computer Engineering) by Swaroop S. Hulawale MIS No: 121022014 under the guidance of Professor: S. U.Ghumbre.

[2] International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS) "A Survey of Cryptographic Algorithms for Cloud Computing" International Association of Scientific Innovation and Research (IASIR) (An Association Unifying the Sciences, Engineering, and Applied Research)

[3] H.Takabi, J.B.D.Joshi, G.Ahn., "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security Privacy Magazine, Vol 8, 2010

[4] Qian Wang; Cong Wang; Kui Ren; Wenjing Lou; Jin Li; , "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," Parallel and Distributed Systems, IEEE Transactions on, vol.22, no.5, pp.847-859, May 2011.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.

[6] Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-7, 2011.

[7] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online), 2012.

[8] Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847), Volume 3 Issue 3, pp.171-176, March 2014.

[9] Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.

[10] Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 3, pp.1922-1926, Jul-Aug 2013.

[11] Lizhe Wang, Gregor von Laszewski, Marcel Kunze, Jie Tao, Cheng Fu, Xi He, Andrew Younge, "Cloud Computing: A Perspective Study", New Generation Computing- Advances of Distributed Information Processing, Volume 28, pp.137-146, 2010.

