Architecture for Data Security In Multicloud Using AES-256 Encryption Algorithm

[1]Rashmi S. Ghavghave, [2]Deepali M. Khatwar
Department of Computer Science and Engg.,
Agnihotri College of Engineering ,Nagthana Rd, Wardha,(MH) INDIA
Email ID: rashmighavghave@gmail.com

Abstract—In cloud computing, data security is the major issue. Security in single cloud is less popular than in multicloud due to its ability to reduce security risks. In this paper, we describe a new architecture for security of data storage in multicloud. We use two mechanisms-data encryption and file splitting. When user upload a file ,it is encrypted using AES encryption algorithm. Then that encrypted file is divided into equal parts according to the number of clouds and stored into multicloud. This proposed system enhances the data security in multicloud.

Keywords—AES encryption algorithm, file splitting, multicloud, security.

*****

I. INTRODUCTION

Cloud computing is an emerging technology that is growing fast day by day. Cloud computing delievers the computing services over the internet. The cloud computing allows access to information and computer resources from anywhere where network connection is available. In general cloud providers offer three types of services i.e. infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS). As the data storage is the main facility provides by cloud, there are security threats and issues regarding to the data storage in cloud.

Providing security in cloud computing is major issue. There are more security risks in single cloud as it is more prone to attacks. We described a new concept of multicloud to solve security problems. Multicloud is also called as interclouds i.e. cloud of clouds. Data can be stored in multiple number of clouds. Security regarding with data storage in multicloud is more popular than in single cloud due to its less risks of attacks.

In our design ,we used multicloud storage system to store clients data. We are using two mechanisms-file splitting technique and data encoding technique using AES encryption algorithm. These are combined together to give a new system architecture which provides security in data storage. Clients file can be encrypted using AES encryption algorithm and file is splitted into 3 equal number of parts and then stored into multiclouds.

This paper is organized as follows:-section 2 describes literature reviews, section 3 describes system architecture, section 4 describes methodology and AES encryption in detail and final section concluded the paper.

II. LITERATURE REVIEW

Mohammed A. AlZainfocuses on the security issues and solutions related to the single cloud and multicloud. In the recent years, it shows that the research into the use of multicloud providers to maintain security has received less attention than the use of single cloud. Their work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.[2]

Cong Wang, Qian Wang, KuiRenNingCaoandand Wenjing Lou proposed a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed ensure-coded data to achieve secure and dependable cloud storage services. The proposed design support secure and efficient dynamic operations on outsourced data, including block modification, deletion and append. [3]

In recent years, various issues related to security has been discussed. Possible solutions for these security risks and threats have been studied. Solutions related with application, accessibility, authentication, data verification, tampering, loss and theft, privacy and control, physical access, data confidentiality, trusting computation are discussed by AbhinayB.Angadi, AkshataB.Angadi, KarunaC.Gull.[4]

Security issues in three deployment models i.e. IaaS, PaaS, SaaS are discussed.[5]. In SaaS model, there are traditional security which are related with authentication and authorization, availability, data confidentiality and virtual machine security and cloud specific security issues include

information security, network security, resource locality, cloud storage, data segregation, data access, web application security, data treatches, backup, identify management. Also the study of threats and countermeasures helps to increase the security in cloud computing.[6][7]

In this paper, AES encryption algorithm is used to provide security in multicloud because AES is considered secure. Encryption and decryption time taken by AES is minimum as compared to others. So it is fastest block cipher algorithm amongst all analyzed cipher algorithms such as blowfish, DES, triple DES.[8][9][10] .

III. SYSTEM ARCHITECTURE AND PROPOSED METHODOLOGY

In this paper, we design a framework which allows users to upload files to cloud server and at the same time the system provides function to split the files into multiple parts. The security is provided using AES encryption algorithm which helps to secure data when it is outsourced to cloud database. So even if the cloud is unreliable the data is secured by two ways.

- The data is split into multiple part so it is not readable.
- The data is encrypted using AES encryption algorithm so it will be very hard to decipher it without key.[1]

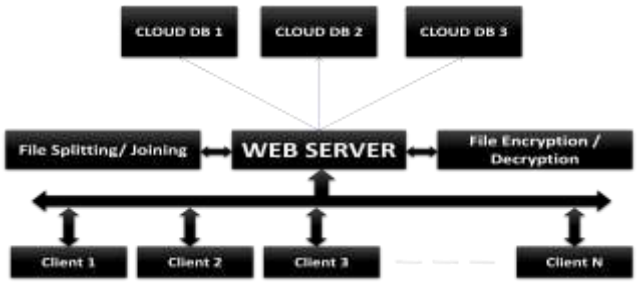

Figure 1.System Architecture

Figure 1 shows system architecture of proposed scheme. The proposed scheme works in following steps:

-User should register on the website. System will send a verification link on user email id. After verification the user will be able to login, upload and download file. When the user upload data, data is encrypted using AES -256 encryption algorithm. Ones the data is encrypted, the data is divided into multiple parts according to the number of clouds (i.e. 3 in project)and store them in individually in different clouds. Then user can download a file.

IV. MODULES

Here we are developing a cloud computing system. We are using Apache Tomcat server as a cloud service provider (CSP) and MySQL to create databases which refers to cloud data storages. The registered users can upload and download only their files to and from the cloud data storages. In this project there are following modules:-

1. Registration Module

In registration module, user create account by filling his details like name and email id and profile picture. Then a verification link sends temporary password to user on email id. Using Email-id and temporary password, user can login. User can also update his password.

2. Upload and Download module

After registered successfully, homepage for user is opened on which options of upload file and download file are given. User can upload all file types on cloud such as doc file, video, mp3, images, etc.

Homepage will show list of file uploaded by user from user specific directory. User can also delete files and download files.

3. File encryption technique module

When user uploads file, it is encrypted using AES encryption algorithm of 256 bit key size. We used Zip4j i.e. java library file to handle zip files. It supports only AES 128/256 encryption and deflate compression method at ultra level.

4. File splitting and joining module

In Proposed system, file splitting is done after encrypting file. File splits into multiple parts according to the number of cloud databases. We used 3 cloud databases. File joining is done by string concatenation which is inbuilt in java.

V. AES ENCRYPTION ALGORITHM

Advanced Encryption Standard (AES) is a symmetric- key block cipher published in December 2001 by the National Institute of Standards and Technology (NIST). It is a block cipher intended to replace DES for commercial application. It uses 128 bit block size with key size of 128, 192 or 256 bits. We used AES-256 in this project. It does not use Fiestel Structure. Each full round consists of 4 separate functions: byte substitution, permutation, arithmetic operation over a finite field and XOR with a key.

ISSN: 2321-8169
157 – 161

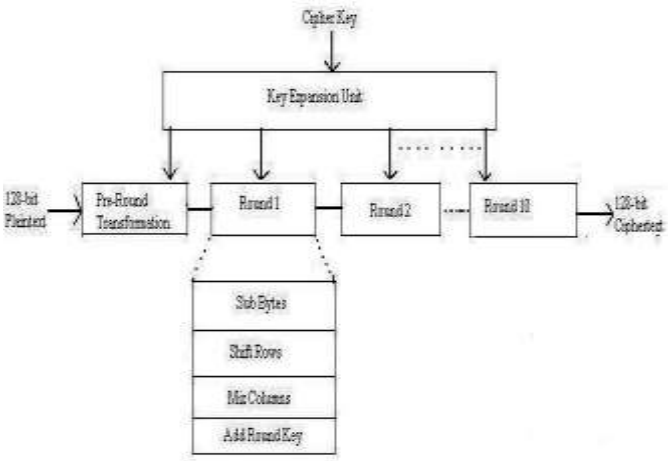

Figure 2. AES Encryption

- Algorithm:

1. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round

Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

- SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- AddRoundKey

4. Final Round (no MixColumns)

- SubBytes
- ShiftRows
- AddRoundKey.

- SECURITY USING AES

Table no.1: comparison of symmetric encryption algorithm [12]

Characteristics	AES	Blowfish	RC5	IDES	3-DES	DES
Key Length	128,192 or 256	32-448 (default128)	Max 2040	128s	112,168	56
Block Size	128,192 or 256	64	32,64 or 128	64	64	64
Security	Considered secure	Considered secure	Considered secure	Proven Inadequate	Considered secure	Proven Inadequate
Cryptanalysis Resistance	Very strong against differential ,truncated differential, truncated, linear,inter-polation and square attack	strong against standard differential and linear cryptanalysis	Vulnerable against differential ,truncated differential, truncated, linear, interpolation and square attack	Vulnerable to differential and linear cryptanalysis	Strong against differential ,truncated differential,tr uncated, linear, interpolation and square attack	Vulnerable to differential and linear cryptanalysis, weak substitution table.
Speed	Very fast	Fast	slow	Slow	Slow	Very slow

Above table shows comparative study of symmetric encryption algorithms which includes AES, Blowfish, RC5,IDES,3-DES,DES. The study shows that key size of AES is greater than other and encryption speed is also very fast. Security provided by AES is considered secure than DES.

VI. RESULTS AND DISCUSSION

Figure 3. Home Page

Above figure shows new user creation in home page.

Figure 4. User Login

Figure 5. Update password

Figure 6. upload file

Figure 4 shows user login using email-id and password. Figure 5 shows update password window and in figure 6, user can upload files. There are other options like save and delete a file. It shows one file uploaded.

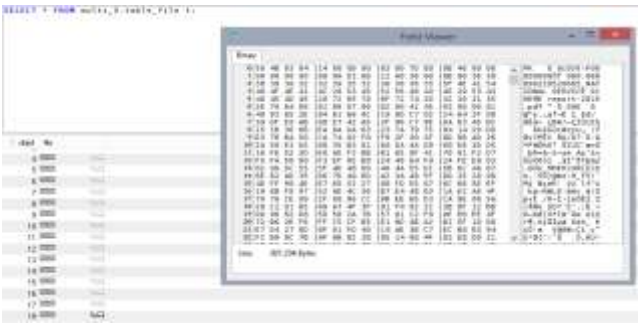

Figure 7. File Split1 stored in 1st cloud database

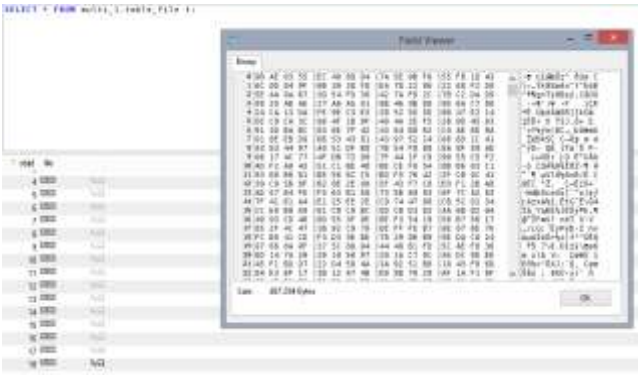

Figure 8. File Split2 in 2nd cloud database

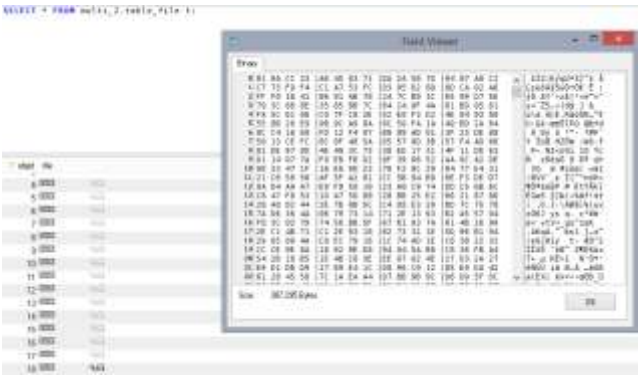

Figure 9. File split3 in 3rd cloud database

In figures 7, 8 and 9, file splitting is shown in 1st, 2nd , 3rd - cloud databases respectively. File is divided into 3 equal parts size i.e. 387,294bytes size. It shows the encrypted files.

VII. CONCLUSION

In this paper, we described a new architecture for security of data storage in multicloud based on two mechanism-file splitting and data encryption technique. AES-256 is used for encryption as it is more secure than other symmetrical encryption algorithms. Also file splitting is used which divides file into subparts and stored into individual clouds.

Our methodology helps to protect files from hackers in viewing whole file. And also even if the hacker viewed the file stored, he may not know which part of file it is and also

he cannot understand what data it contains as it is encrypted. The architecture which we developed is a more secure cloud storage methodology than the existing one as in existing systems whole file is stored into single cloud which is not secure.

REFERENCES

[1] Rashmi S. Ghavghave,Deepali M.Khatwar, "Load balancing and security in multicloud iaas using distributed file system "in International Journal of Informative and Futuristic Research ,Volume 2 ,Issue 4, December 2014.

[2] Mohammed A. AlZain, Eric Pardede , Ben Soh , James A. Thom"Cloud Computing Security: From Single to Multi-Clouds "in 45th Hawaii International Conference on System Sciences,2012.

[3] Cong Wang, Qian Wang, KuiRenNingCaoandand Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing",2011.

[4] AbhinayB.Angadi, AkshataB.Angadi, KarunaC.Gull," Security Issues with Possible Solutions in Cloud Computing-A Survey"inInternational Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.

[5] AnujKumarYadav, Ravi Tomar, Deep Kumar and Himanshu Gupta," Security and Privacy Concerns in Cloud Computing" in International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 5, May 2012.

[6] Rashmi, Dr.G.Sahoo, Dr.S.Mehfuz,"Securing Software as a Service Model of CloudComputing: Issues and Solutions"in International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, August 2013.

[7] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez," An analysis of security issues for cloud computing", in Journal of Internet Services and Applications 2013.

[8] RanjeetMasram, VivekShahare, Jibi Abraham, RajniMoona, "analysis and comparison of symmetric key cryptographic algorithms based on various file features" in International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014.

[9] ShraddhaSoni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma ,"Analysis and Comparison between AES and DES Cryptographic Algorithm" in International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012.

[10] Sumitra," Comparative Analysis of AES and DES security Algorithms" in International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013.

[11] Manpreet Kour , Rajbir Singh." Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing"in International Journal of Computer Applications (0975 – 8887) Volume 70– No.18, May 2013.

[12] Chander Kant,Yogesh Sharma "Enhanced Security Architecture for Cloud Data Security"International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 5, May 2013.