wjert, 2017, Vol. 3, Issue 3, 379 -385 *Original Article* ISSN 2454-695X

World Journal of Engineering Research and Technology

WJERT

www.wjert.org

SJIF Impact Factor: 4.326

A HYBRID APPROACH TO PROVIDE SECURE COMMUNICATION FOR CLOUD SYSTEMIN HADOOP ENVIRONMENT

[1]*Sonia Rani and [2]Kirti Bhatia

[1]Sat Kabirdas Institute of Technology and Mang., M.Tech Student.

[2]HOD of CSE department, Sat Kabirdas Institute of Technology and Mang.

Article Received on 13/03/2017 Article Revised on 04/04/2017 Article Accepted on 25/04/2017

***Corresponding Author**
Sonia Rani
Sat Kabirdas Institute of Technology and Mang., M.Tech Student.

ABSTRACT

In this paper, a cloud system security mechanism is defined for information management in Hadoop environment. The work has integrated in the Hadoop environment to manage the information on cloud server. It includes the file level security, user level security and communication level security. At the earlier stage of work, as the user enters to the system, the user role will be identified by performing the authentication and authorization. Once the authentication is proven, the information management over the Hadoop server will be performed under file level security. A key based hybrid approach will be applied to achieve the file level security. In this work, SHA and AES based combined approach will be applied for file level security. In third stage of work, the secure information transmission will be provided for private users using session based communication. The work will be implemented in java integrated Hadoop environment using Netbeans IDE.

KEYWORDS*:* Hadoop, SHA, AES, Encryption, Cloud Server.

INTRODUCTION

There have been many definition of cloud computing by given by different researchers. One of the definitions by Barkley RAD defines cloud computing as: "Computing refers to both the applications delivered as services over the net and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds. People can be users or providers of SaaS, or users or providers of Utility Computing. It is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. It is a computing platform for sharing resources that include infrastructures, software, applications, and business processes. Cloud computing provide services to user by internet. Some example of cloud computing services are as: face book, Skype,onedrive,amazon.com, googledrive, googledocs, etc.

System Design

A. User level Security

As the user enters into the cloud system for accessing data, user role will be identified by performing authentication. Only registered user can perform data accessing operations i.e. private user. A public user cannot perform any downloading operations. So, this layer provides user level security.

B. File Level Security

File level security means all files will be saved in encrypted form on cloud system. A key based hybrid approach is used to achieve file level security. SHA and AES encryption technique is used to encrypt file during uploading and to decrypt during downloading. User has to enter the secret key before download any file.

C. Communication Level Security

The secure information transmission is provided for private users using session based communication when some data transfer will take place between user and client and a session key will be generated for a specific time and deactivated after data transmission take place between user and server.

Security Algorithm

A. AES: also referenced as Rijndael is a specification for encryption of electronic data established by U.S. NIST It a types of symmetric key algorithm because in this same key is used for encryption and decryption and is based on design principle known as substitutions and permutation network, combination of both substitution and permutation and it is fast in both software and hardware. It is successor of DES. It AES operates on a 4*4 columns –

major matrix of bytes. Termed the state .most AES calculations are done in a specific finite field. The key size used for it specifies the number of repetitions of transformations rounds that convert the input, called the plaintext into cipher text i.e. encrypted format. The number of cycles of repetitions is as follows:

- 10 cycles for 128- bit key
- 12 cycles for 192 –bit key
- 14 cycles for 256-bit key

Each round consist of several processing steps, each consists four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to convert cipher text to plain text using the same key.

B. SHA

In cryptography, SHA-1 is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST.SHA-1 produces a 160-bit (20- byte) hash value. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long. SHA stands for secure hash algorithms. The four SHA algorithms are structured differently and are named *SHA-0*, *SHA-1*, *SHA-2*, and *SHA-3*. SHA-0 is the original version of the 160-bit hash function published in 1993 under the name "SHA": it was not adopted by many applications. Published in 1995, SHA-1 is very similar to SHA-0, but alters the original SHA hash specification to correct alleged weaknesses. SHA-2, published in 2001, is significantly different from the SHA-1 hash function.

Implementation and Proposed Work

A. Implementation: Our implementation was done using Netbeans IDE. We used MySQL for our IDE (Integrated development environment).The Java JRE version is v1.6.0_26.We used Apache Tomcat 7.0 as web server for our web application. For the cloud Infrastructure and data storage we used Hadoop version 2.3.0. We also used Hadoop libraries jar files for cloud server environment.

B. Proposed algorithm: Proposed algorithm provides complete flow of security layer before storing file on cloud server and also shows encryption of file by using AES and SHA algorithm.

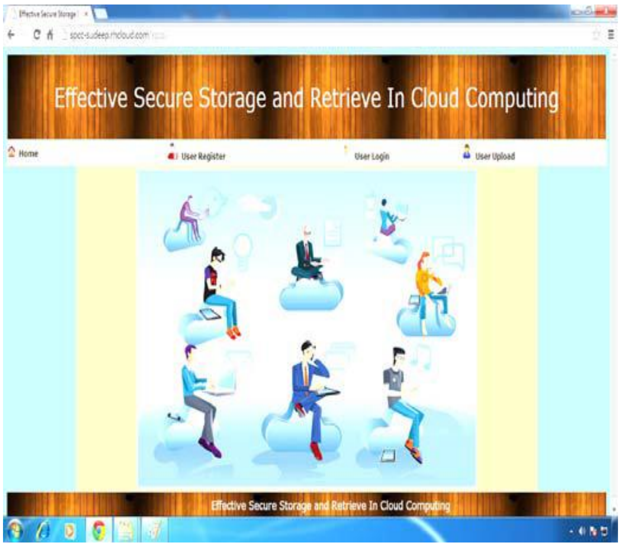
```
Algorithms (user)
/*user is the communicating user to the cloud server*/{
□ Accept user key information including use rid and password
□ If(Authentication(userid,password)=False)
[Check for user level security]
{
□ Print "Invalid User"
[Only authenticated user can work on cloud server]
Return
}
□ Textcontent=Upload(file)
[Upload the file content that user wants to upload in secure way]
□ TextContent=Split(TextContent,Block)
[Perform hash apdative block division to apply SHA]
□ For i=1 to TextContent.Blocks.Length
[Process all the message blocks]
{
□ Seqtext=GetSeq(TextContent.Blocks(i))
[Transform the text in adaptive sequence form]
□ Encoded=ApplyHashOperatons(seqtext,OR, Shift,Agg)
Apply a series of hash coded operations to generate the coded message]
□ Matrxtext=Tranform(Encoded,matrix)
[Transform the message to the matrix form for applying the AES operatons]
□ Matrixtext =ApplyRowSwitch(Matrixtext)
[Apply row level change in message matrix formation]
□ Matrixtext =ApplyColSwitch(Matrixtext)
[Apply Col level change in message matrix formation]
□ Matrixtext =Interchange(Matrixtext,Row,Column)
[Perofrm matrix row column interchange under AES]
□ EncodedTextblock=Transform(Matrixtext)
[Obtain the encoded text blocks]
□ Message=Message U EncodedTextblock
[Combine the message blocks to combine the final message]
}
```

Return message

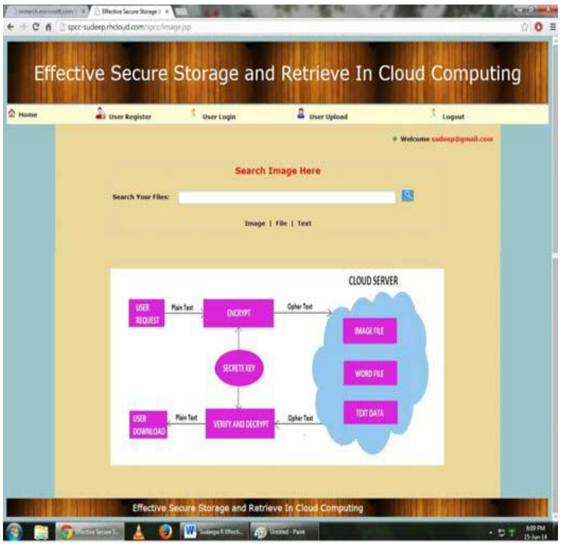
}

RESULTS

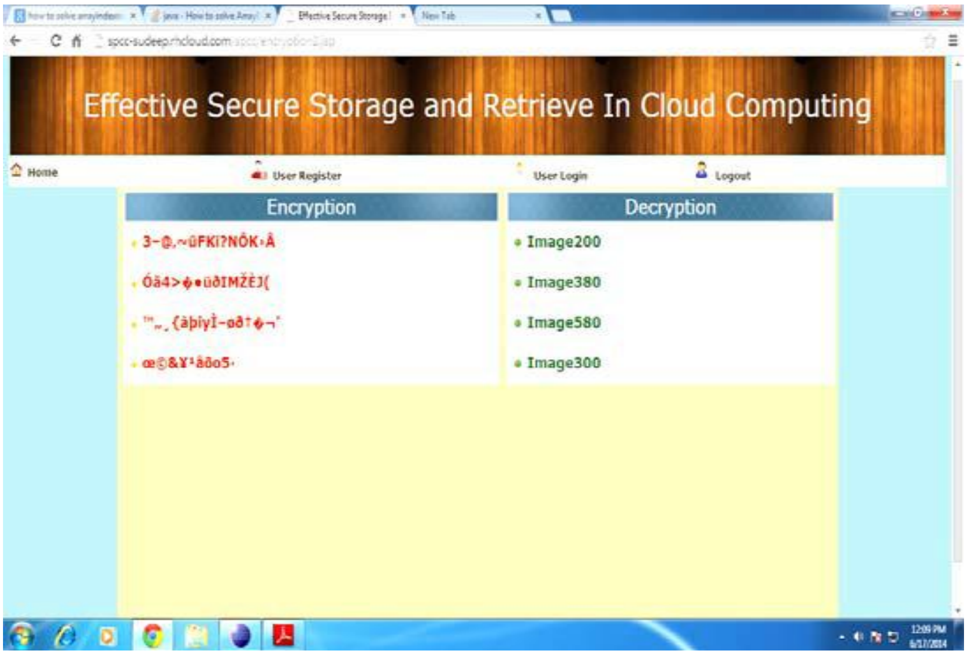
This part of paper will show that how hybrids approach will increase the security of cloud storage system and data confidentiality. In the present architecture, cloud storage system is created. User can login into the cloud system by his/her user id, password which provides security at user level. If user is new than a new account can be created by clicking on resister now link present on cloud login page. After entering login details user can see the contents of its account. A user has following options at his/her account: file upload, file download, create new folder, receive key and file details, information about file before uploading file a user will create a folder and this folder will be create on Hadoop server and then user can upload files and all files uploaded by that user will be store on Hadoop server in encrypted form. And each file two files will store on server one is encrypted file and second is key file. File will be encrypted by using AES algorithm and key will be encrypted by using SHA. This will provide file level security because all files will be saved in encrypted format. If user wants to download file than he has to enter the security question and name of file given by user during folder creation time for downloading key. File received by user will be in now decrypted form.


Effective Secure Storage
spcc-sudeep.rhcloud.com
Effective Secure Storage and Retrieve In Cloud Computing
Home
User Register
User Login
User Upload
Effective Secure Storage and Retrieve In Cloud Computing

Home Page



File Upload Page



Effective Secure Storage and Retrieve In Cloud Computing

Encryption	Decryption
3-@.~ûFKi?NÔK·Â	Image200
Óä4>ф•üðIMŽÈJ(	Image380
™‚{àþiyÌ-øð†ф¬˚	Image580
œ©&Y¹âðo5·	Image300

Encryption/Decryption

Form which provide communication level security. Aiming at the existing popular cloud data security weakness, we put forward a security encryption scheme which satisfy the data transmission and storage security and satisfy client. It is an encryption system that could increase security of data on the cloud server and finally achieve security, stability, efficient and effective storage. File uploading time using proposed security algorithm takes less time than DES algorithm for different size of file.

CONCLUSION AND FUTURE WORK

Proposed work provides security of data on cloud system by providing different levels of security so that an attacker cannot easily access the data on stored on cloud system. In future this work can be extended by using different new security algorithms and also from key splitting methods in which we can store parts of key on different server so that attacker cannot easily access the file.

REFERENCES

1. Minqi Zhou, Rong Zhang, Wei Xie and Weining Qian, Aoying Zhou, Security and Privacy in Cloud Computing: A Survey. Sixth International Conference on Semantics, Knowledge and Grids, 2010.
2. Jianfeng Yang and Zhibin Chen, Cloud Computing Research and Security Issues. 2010.
3. Louis J. Freeh, Keynote talk at International Cryptography Institute, Sept. 1995. Available through http://www.fbi.gov/crypto.htm

4. V. D. Cunsolo, Achieving Information Security in Network Computing Systems, Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
5. Christian Schridde, an Identity-Based Security Infrastructure for Cloud Environments, 2010.
6. Yingjie Xia, Hierarchy-Aware ECC Model for Cloud, 2nd International Conference on Industrial and Information Systems, 2010.
7. Yanping Xiao, An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing, 2010.
8. M.Venkatesh, Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing, 2012.
9. Vasyl Ustimenko, on some mathematical aspects of data protection in cloud computing, 2012.
10. Dexian Chang, TSD: A Flexible Root of Trust for the Cloud, 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.