ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Providing Security for Data at Rest in Cloud Computing

Aishwarya R Nayak[1], Shubhashree G Joshi[2], Sushma D[3], Pooja Nayak[4], Priyanka Prasad[5]

Assistant Professor, Department of Computer Science and Engineering, BITM College, Ballari, Karnataka, India[1].

U.G Student, Department of Information Science and Engineering, BITM College, Ballari, Karnataka, India[2].

U.G Student, Department of Information Science and Engineering, BITM College, Ballari, Karnataka, India[3].

U.G Student, Department of Information Science and Engineering, BITM College, Ballari, Karnataka, India[4].

U.G Student, Department of Information Science and Engineering, BITM College, Ballari, Karnataka, India[5].

ABSTRACT: Many storage servers are required for storage of data in Cloud storage system. Data confidentiality is important for the data stored in Cloud storage system. General encryption schemes available before provided security for the data to limited extent but failed to provide security in trustworthy manner and are costly. Central authority is required for constructing a secure distributed storage system and is challenging task in case of unavailability of central authority. Hence in this paper, we propose a formulation of secure distributed storage system by introducing a proxy re-encryption scheme which is integrated with decentralized erasure code. The aim of the proposed scheme is that it supports encoding operations over encrypted messages. Thus provide security for the data at rest in cloud.

KEYWORDS: Cloud, Decentralized erasure code, Proxy re-encryption, Secure storage system.

I. INTRODUCTION

Cloud Computing is a type of Internet-based computing that provide resources and data for the computers and devices on demand. Cloud Computing provide users various benefits to store as well as to process the data. The main advantage of cloud computing is it reduces the up-front infrastructure cost and also it helps the organization to fore on their core functionality rather than spending money and time on computer infrastructure.

CHARACTERISTICS OF CLOUD

1. **Device and location independence:** It enables the users to access the system through web browsers irrespective of their location and the devices used, as the cloud is typically provided by third party and as it can be accessed via internet, users can connect to it from anywhere.
2. **Maintenance:** Maintenance of the cloud computing applications is easier, as they need not be installed on each user computer and it can be accessed from different places.
3. **Multitenancy:** Cloud enables sharing of data across large number of users thus it allow centralization of infrastructure, peak-load capacity increases, improvement of utilization and efficiency.
4. **Scalability and Elasticity:** It is provided by dynamic provisioning of resources.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

MODELS OF CLOUD COMPUTING

There are Four different deployment models of cloud computing

1. Public Cloud
2. Private Cloud
3. Hybrid Cloud
4. Community Cloud

1. **Public Cloud:** Public also called external cloud is the one whose resources can be used by the user by paying for the services.
2. **Private Cloud:** It is the one where the cloud is specially designed for a particular organization and is used by only that organization.
3. **Hybrid Cloud:** It is the combination of public and private cloud and is more expensive when compared to public cloud.
4. **Community Cloud:** This type of cloud can be shared by several organizations if their requirement is same, the community cloud is costlier than public cloud but it provides greater security.

- Earlier Cryptographic algorithms used for the encryption of data in the cloud for the purpose of data security cannot be used as there is lack of data confidentiality in cloud computing and even the checking for correctness of the data and checking for redundant data is difficult task in case of primitive cryptographic algorithms.

- Cloud cannot be considered just a third party warehouse. The data stored in the cloud is updated by the users frequently i.e the users can perform actions such as deleting, updating, appending etc

In this paper, we propose an efficient and effective form of cryptographic scheme called proxy-re encryption which encodes over the encrypted message to provide security for the data at rest in cloud.

II. LITERATURE SURVEY

- In 1998, Blaze, Bleumer, and Strauss proposed an application called atomic proxy re-encryption.
- Lin and Tzeng addressed robustness and confidentiality issues by presenting secure decentralized code for network storage system, this system was not that scalable and robust.
- Proxy re encryption scheme by Mambo, Okamoto and Blazeetal, here a proxy server transfer a cipher text under a public key using re-encryption key, this scheme didn't provide full data confidentiality and the data forwarding was not trustworthy.
- Lin et al. proposed a security scheme that makes use of two kinds of servers namely data servers and key servers in order to store data and security keys respectively. Though this scheme is secure, it suffers from inconsistencies in communication among the servers.
- K Ren and Q Cao said about "Erasure coded data". From the year 2010

III.EXISTING SYSTEM

In the existing system general encryption schemes are used which hinders the data confidentiality, as well as it limit the functionality of storage system as most of the operations cannot be performed over encrypted data. Storing data in cloud provides serious concern on security of data stored. General encryption scheme is used for encryption,DES algorithm is used for generation of keys, for the storage of data in the existing system user need to maintain the keys as wel a sthe whole file is stored in a single server.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

DISADVANTAGES OF EXISTING SYSTEM

- Management of cryptographic keys by the user of the system.
- Communication traffic between user and storage servers.
- Storing and retrieving of data is difficult for storage servers.
- One time encryption is done using general encryption schemes.

IV. PROPOSED SYSTEM

In this paper we have proposed a scheme called proxy re-encryption in which a decentralized erasure code is used for distributed storage system which provide security for the data by performing encoding operations over encrypted data where two servers namely storage server and key servers are used for storage of data and keys respectively. Encryption is done by using Blowfish algorithm.

ADVANTAGES OF PROPOSED SYSTEM

- Provides high data security thus it provide trustworthy data confidentiality.
- Data is highly protected by an security mechanism of the server.
- This scheme helps in present a secure cloud storage system which provide secure data storage and secure forwarding of data in a decentralized structure.
- Less time consuming.
- Distribution and forwarding of data is easy.

SYSTEM ARCHITECTURE

System Architecture is a conceptual model that defines the structure and behaviour of the system. It is a formal description and representation of the system.

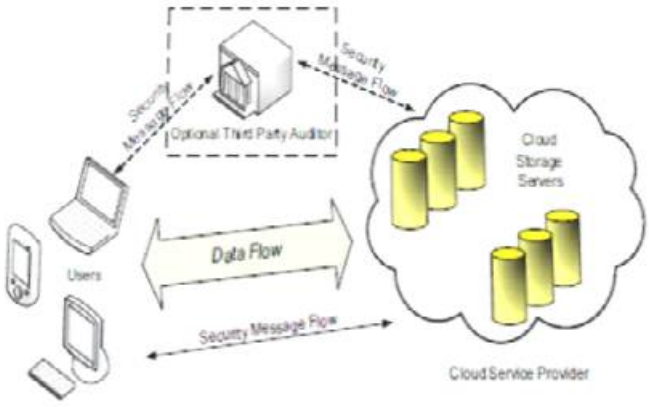

Fig 4.1System architecture

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

MODULES

1) Construction of Cloud Data Storage Module
2) User Module
3) Data Encryption Module
4) Data Forwarding Module
5) Data Retrieval Module

1) **Construction of Cloud Data Storage Module:** It is also called admin module in which admin needs to log in by his username and password so that the remote server setup is opened where the admin sets the IP address of remote server for storage server as well as key server, then the port number must be specified then the admin can either activate or deactivate to setup the process. The activated IP address are stored in storage server. The IP address which is set for remote server is available and can be viewed by clicking available storage server button.

2) **User Module:** If the user is a registered previously then he can login to the cloud by his details such as user name and password, If in case the user doesn't have account then he must register to the cloud by providing the details to use and access the cloud. The details asked for registration may be Username, Email, Password, Date of Birth, Gender, Location by filling all the details in the form the user need to click on register button to get register for the cloud. Once the registration of user is done then the details of the user will be stored in the database of the cloud system. Then the user must login to the cloud using the registered details Username and Password.User can even create a folder, it will ask a question for security then the folder name is to be given after submission the folder will be created.

3) **Data Encryption Module:** File can be uploaded to the folder created, for uploading of file, user have to click on the file upload option provided. A dialogue box will appear where the file that is to be uploaded is to be browsed and then selected for upload after submission an alert box will appear with a message like File encrypted as:Filename.txt.enc and the corresponding Encryption key is Filename.txt.key

4) **Data Forwarding Module:** The details of the file consists of filename, question, answer, forward(false) and the forwarded email. Forwarding of file to other users depends on the value in the forward column if the value is true then the user cannot forward it, if it is false then the user can forward it. For forwarding of the files, the folder, filename, emailed to whom the code need to be forwarded and the code need to be entered and on pressing forward button an alert message is popped saying code sent to mail then the value of forward for that corresponding file becomes true.

5) **Data Retrieval Module:** Retrival module is also called the download module in which the files can be downloaded from the cloud by the submission of folder name, file name and the secret key which is sent to the mail id and on submission then clicking the download option the client can view the encrypted key and using that key the client can view the file and use that file. If the user wants the decrypted file then he needs the encrypted file as well as key file. Browse the respective file and submit the files for decryption in alert box we will get a message that file successfully decrypted.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

V. SIMULATION AND RESULTS

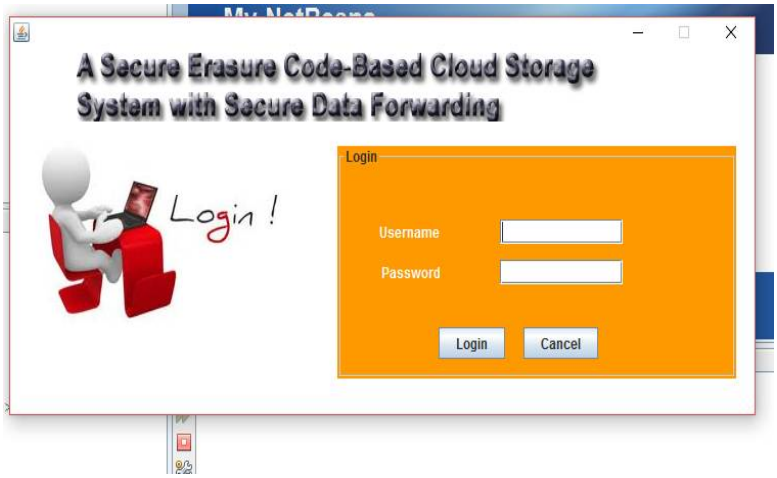

Fig 5.1 Admin login

This figure shows the admin login module in which admin logs in by giving his username and password for authentication to perform further operations.

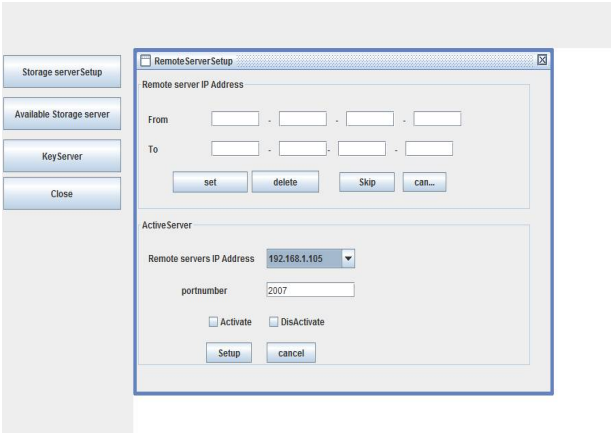

Fig 5.2 Operations performed by Admin

After successful login of admin he can perform some operation such as storage server setup, selection available storage server , selection of key server for storage of data and key.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

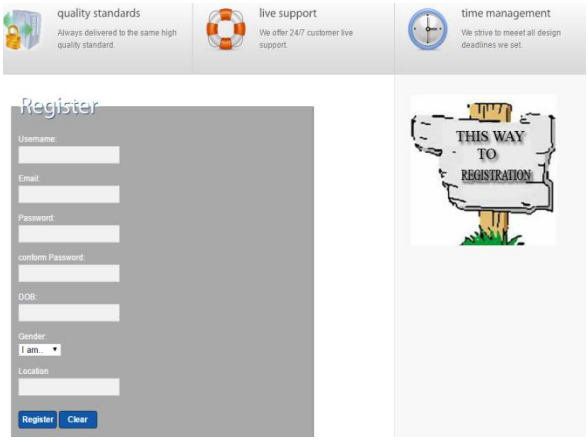

Fig 5.3 Registration of user

This figure shows the registration module for new user who needs to register before performing operations on cloud.

Fig 5.4 Details of file

This figure shows the details of the file such as filename, forward value, forwarded email.

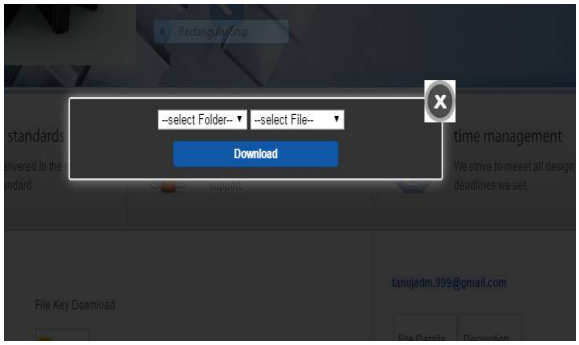

Fig 5.5 Download of file

This figure shows the download module of the file required by selecting the folder name and file name.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Fig 5.6 Download of key file

This figure shows the download of the file key which is used for the decryption of the file downloaded

Fig 5.7 Decryption of file

This figure shows the decryption module of the file by choosing file name and key used for decryption.

VI. CONCLUSION

In this paper, the proposed cloud system have two servers storage and key. This scheme proposed Is the combination of Threshold proxy re-encryption and erasure code. Encoding, Forwarding and decryption of operations are performed by using this proxy re-encryption. Thus we present a secure cloud storage system with the help of the proposed scheme which has provided secure data storage.

VII. FUTURE SCOPE

The scheme proposed in this paper can be further enhanced to provide security for pdf files and Images.

REFERENCES

[1] Hsiao-Ying Lin, Wen-Guey Tzeng, "A secure Erasure Code-Based Cloud Storage System with secure Data Forwarding", IEEE TRANSACTION ON PARALLEL AND DISTRIBUTED SYSTEM, VOL. 23, NO.6, JUNE 2012.
[2] Mills, Elinor (2009-01-27), "Cloud computing security forecast: clear skies" , CNET News.Retrieved 2017-05-01
[3] Chhibber. A (2013), "SECURITY ANALYSIS OF CLOUD COMPUTING" (PDF), International Journal of Advanced Research in Engineering and Applied Sciences2, Retrieved 2017-04-14
[4] L. Carter and M. Wegman, "Universal Hash Functions", Journal of Computer and System Sciences, vol. 18, no. 2, pp. 143– 154, 1979.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing" , Proc. IEEE 29th Int'l Conf. Computer Comm. (INFOCOM), pp. 525533, 2010.