International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 7, 2017 ISSN: 2348-6600
Reference ID: IJCS-187 PAGE NO: 1137-1144
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

SECURE DATA STORAGE AND SHARING IN MULTI CLOUD COMPUTING ENVIRONMENT USING MULTILEVEL ENCRYPTION ALGORITHMS

N.M.MALLIKA,
Assistant Professor, Department of BCA,
Sri Vasavi College (Self Finance), Erode -638316.
nm.mallika@gmail.com

Dr.B.SRINIVASAN,
Associate Professor, PG & Research Dept of Computer Science.
Gobi Arts & Science College, Gobichettiplayam-638476.
srinivasan_gasc@gmail.com

ABSTRACT- Cloud computing provide users to store and process their data in third-party centres. It can be used for highly sensitive data that are necessarily needed to be secured and stored on clouds.It is used to securely store information or data into the cloud, by replicating and storing the data on multiple clouds. The proposed work plan is to eliminate the concerns regarding data privacy using multilevel cryptographic algorithms to enhance the Secure Data Storage and Sharing in Multi Cloud Computing Environment Using Multilevel Encryption Algorithms.

KEYWORDS
Cloud Computing, Secure Cloud Architecture, Public Cloud, Personal Cloud, Encryption, Data Integrity, Splitting.

INTRODUCTION

Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed Encryption. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud Computing performs the operation like distributed system where many computers can perform operations simultaneously. There is a need to protect Cloud data against unauthorized access.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 7, 2017 ISSN: 2348-6600
Reference ID: IJCS-187 PAGE NO: 1137-1144
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Cloud Computing Characteristics

1. Broad Network Access: cloud amenities can possibly gain access to over the network through the usage of standardized mechanism that hold up different users, like mobile phones, tablets, mainframes and work stations.
2. Self-service on Necessity: The user probably will make a judgment on the use of computing amenities such as server time and network storage, based on of their current needs, with no more communication with dissimilar service providers in cloud.
3. Combining of Computing Resources: In addition to classical virtualization, cloud computing uses in adding the capabilities of mechanization of services and multi-tenancy of users at shared information resources. Common use of the same technical resources is the vital feature of cloud computing.
4. High Elasticity: The client may simply rise or fall the capacities afforded using the current requirements. The capacities are limitless for the user.

EXISTING SECURITY SYSTEMS

Cryptography can help emergent acceptance of Cloud Computing by more security concerned companies. The first level of security where cryptography can help Cloud computing is secure storage. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms. Now a day's cryptography is considered as a combination of three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, and Hashing. In Cloud computing, the main problems are related to data security, backups, network traffic, file system, and security of host [2], and cryptography can resolve these issues to some extents. Consider an example, in the cloud consumer can protect its confidential data, then he has to encrypt his information before storing in the cloud storage, and it is advised not to save an encryption key on the same server where you have stored your encrypted data.

A. Data Encryption Standard (DES) Algorithm

The Data Encryption Standard (DES) [2] is a symmetric- key block cipher at the encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption.

B. Advanced Encryption Standard (AES) Algorithm

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. The AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 7, 2017 ISSN: 2348-6600
Reference ID: IJCS-187 PAGE NO: 1137-1144
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

C. RSA Algorithm

The RSA is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Mohammed A. Alzain et al. (2011) in MCDB: using Multi-Clouds to ensure security in Cloud Computing [6] have proposed a multi clouds database model and present the architecture of multi cloud database model and describe the layers and components.

PROPOSED SYSTEM

Nowadays Cyber Criminals can easily access data storage. In Personal Cloud Storage important data, files and records are entrusted to a third party, which enables Data Security to become the main security issue in Cloud Computing. In Cloud Storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task.

A. System Analysis

A document management system (DMS) is a system used to track, manage and store documents. Most are capable of keeping a record of the various versions created and modified by different users. Generally, Organizations or individual uses Premise-based document management system. But Premise-based document management systems are not reliable, they have following limitations:

- Initial investment is high.
- The logistics of capturing, storing, retrieving, indexing, sharing, and securitizing documents is complex.
- It needs software licenses, server modules, hardware and need to assign storage, databases, and web servers.
- Did not provide Top Level Security.

Because of these limitations, each and every organization is moving its data to the cloud based document management system, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc. In Cloud Storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 7, 2017 ISSN: 2348-6600
Reference ID: IJCS-187 PAGE NO: 1137-1144
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

resources authentication of stored data becomes a mandatory task.

B. System Architecture

The proposed system is designed to maintain security of files. The name of our system is "Cloud-Based Document Management System" or "Cloud-Based DMS". Our System provides Software-as-a Service (SaaS) document management solutions. Cloud-based DMS uses an enterprise's existing equipment eliminating the need for high-powered servers or complex onsite architectures. The following figure illustrates the architecture of cloud-based Document Management System (DMS).

The proposed system architecture focuses on the following objectives which are helpful in increasing the security of data storage.

Scalability: The system is scalable because it provides server, storage capabilities and collaboration from one to thousands of users.

Security: The cloud offers better security by using multilevel encryption. We can able to quickly and easily recover files if they lose during a break-in, network breach or natural disaster.

Uses of Web Browser:

Cloud-based DMS is available through a simple Web browser Internet connection. The system needs little or no software to install; no firewalls to configure; no backups to set up.

Storage and Backup: The system scrambled the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage using multilevel encryption algorithms.

C. Proposed System Design

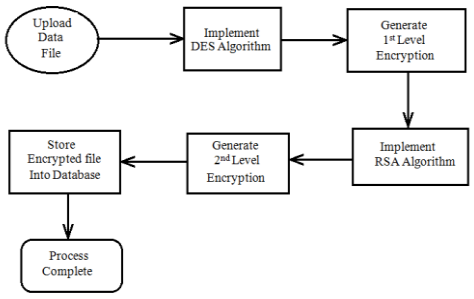
The proposed system "Cloud-Based DMS" is designed to maintain security of data files stored in cloud. This proposed system is a combination of two different security algorithms to eliminate the security challenges of Personal Cloud Storage. We have taken a combination of algorithms like: DES and RSA. DES (Data Encryption Standard) is a symmetric key algorithm, in which a single key is used for both encryption/decryption of data. Whereas RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. A user can upload data files such as text, mp3, images, pdf etc in Personal Cloud Storage. While uploading file DES and RSA Encoding schemes are used to encrypt data. The Block Diagram of proposed work at Multilevel Encryption is shown in following figure 5. As Shown in figure 5, the steps of Multi-level encryption will be as follows;

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 7, 2017 ISSN: 2348-6600
Reference ID: IJCS-187 PAGE NO: 1137-1144
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Upload the file. Now implementation of DES Algorithm takes place. The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The actual key used by DES algorithm for encryption is 56 bits in length. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds [7].

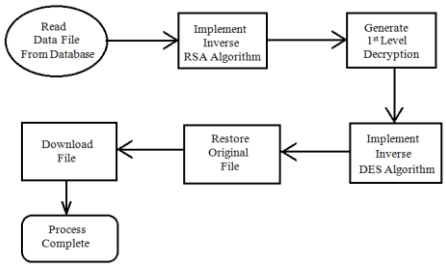
DES has 16 rounds, means the main algorithm is repeated 16 times to produce cipher text. As number of rounds increases, the security of system increases exponentially. The first level encryption is generated using DES algorithm. Now apply RSA algorithm [5] on encrypted output of DES algorithm to generate second level encryption. In RSA algorithm public key is used for encryption. RSA is a Block Cipher in which every message is mapped to an integer.

Once the data is encrypted using RSA algorithm, it will be stored in Database of Cloud Storage.



And while downloading file inverse DES and RSA algorithms are used to decrypt data. The

Block Diagram of proposed work at multilevel decryption is



For Data Security, the steps of Multi-level decryption will be as follows:

Inverse DES and RSA algorithms are used to decrypt data. First apply the Inverse RSA algorithm (decryption scheme) using private key. This algorithm will generate first level decrypt data. Now apply the DES decryption algorithm on first level decrypted data. DES decryption algorithm uses the same 56 bit length key for decryption. DES algorithm of decryption will generate Plain text. Now Plain Text will be displayed to the User.

In Our proposed System, implementation of the DES algorithm takes place to generate first level encryption. And then we apply the RSA algorithm on the encrypted output of DES algorithm to generate second level encryption. And same process takes place for decryption using inverse DES and RSA algorithms.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 7, 2017 ISSN: 2348-6600
Reference ID: IJCS-187 PAGE NO: 1137-1144
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Cloud service providers for storage of the data on the multiple clouds. Data splitting technique that splits the data required to store into slices for better security. Encrypting/Decrypting mechanisms that are employed over data at different stages of proposed schemes. User platform and data. Encrypting the data files that are to be stored on clouds.Splitting the data on the mobile according to the needs and comforts of the data owner as number of segments or size of files etc. Re-naming of the encrypted segments so as to make it difficult of any intruder to get access and control over the data slices. Assigning of the segments to the respective clouds as we are using multiple clouds so we have to assign each segment with a cloud on which it is stored. Distributing these segments to their respective clouds.

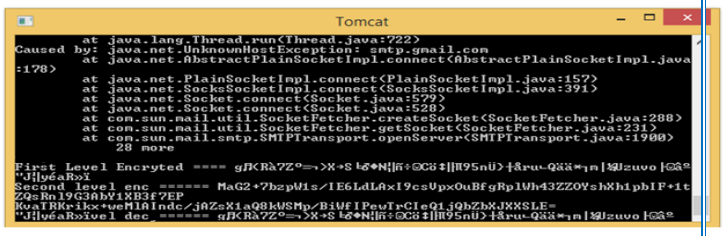
SYSTEM IMPLEMENTATION AND RESULTS

A. System Implementation: Implementation of algorithms has been done using HeidiSQL_3.2 IDE (Integrated Development Environment) with Java Server Pages.

Installation of MySQL5 and Apache Tomcat is necessary for our system, because Cloud Based DMS is a mysql database client made with jsp and connected to mysql database and hosted in Apache Tomcat Server.

B. Results: The following figures illustrate the implementation of multilevel encryption algorithms. In the figure, PDF files are uploaded on Cloud Based DMS.

In the above figure, User uploaded PDF Documents in Cloud Based DMS Both the first level and second level encryption applied on the pdf files are shown in following figure 8;



CONCLUSION AND FUTURE SCOPE

A. Conclusion

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons. So cloud security is must which will break the hindrance the acceptance of the cloud by the organizations. Encryption algorithms play an important role in data security on cloud. But these existing

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 7, 2017 ISSN: 2348-6600
Reference ID: IJCS-187 PAGE NO: 1137-1144
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

cryptographic algorithms are single level encryption algorithms. Cyber criminals can easily cracked single level encryption. Hence we propose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage. In our proposed work, only the authorized user can access the data. If some intruder (unauthorized user) tries to get the data directly from the database, he must have to decrypt the data at each level which is a very difficult task. It may be expected that multilevel encryption will provide more security for Cloud Storage than single level encryption.

B. Future Scope

We are working on betterment of decryption techniques. The decryption techniques must be more precise as compared to what we have presently. The applied multilevel decryption algorithm needs to be modified so as to improve the decryption of files. Thus in a nutshell, further experiments are required to confirm these justifications. In addition, firewall and VPN (Virtual Private Network) technology will be improved to protect data transfer. These are some justifications that are expected in the future, the future of cloud based DMS is not limited to these justification.

REFERENCES

[1] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram, "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033-3037, May-Jun 2012.

[2] 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.

[3] Dr.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, pp.571-575, May 2013.

[4] Kevin Curran, Sean Carlin, Mervyn Adams, "Security issues in cloud computing", Elixir Network Engg.38 (2011), pp.4069-4072, August 2011.

[5] 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.

[6] Neha Jain, GurpreetKaur, "Implementing DES Algorithm in Cloud for Data Security", VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 7, 2017 ISSN: 2348-6600
Reference ID: IJCS-187 PAGE NO: 1137-1144
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

[7] RandeepKaur, SupriyaKinger, "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.