Security in Cloud Computing using Cryptographic Algorithms

Miss Shakeeba S. Khan[1]M.E. Scholar, Dept. of Computer Sci. & Engg., PRMIT&R Badnera, Amravati, India

*Prof. Ms. R. R. Tuteja[2]*Associate Professor, Dept. Of Computer Sci. & Engg., PRMIT&R Badnera, Amravati, India

Abstract: Cloud Computing is a set of IT Services, for example network, software system, storage, hardware, software, and resources and these services are provided to a customer over a network. The IT services of Cloud Computing are delivered by cloud service provider who owns the infrastructure. Benefits of cloud storage are easy access means access to your knowledge anytime along with scalability, resilience, cost efficiency, and high reliability of the database. Because of these advantages and facilities each and every organization or company is moving its data to the cloud, 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. To secure the Cloud means secure databases hosted by the Cloud provider. In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using multilevel cryptographic algorithms to enhance the security in cloud as per different perspective of cloud customers.

Index Terms: Cloud Computing, Cryptographic Algorithm, Data Authentication, Data Integrity, Infrastructure, Internet, Security Issue.

1. INTRODUCTION

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to database information from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Because of these benefits each and every organizations are moving their data to the cloud. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the user data storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is achieved by cryptography. Cryptography, in modern days is considered mixture of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

Data cryptography mainly is the scrambling of the content of the data, such as text documents, images, pictures, audio, sounds, videos etc 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 storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms.

2. Literature review

Cloud computing has been defined by US National Institute of Standards and Technology (NIST) [12] as "a model for enabling trusted, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal difficulty or cloud provider reaction ". The NIST definition is one of the most accurate definitions of cloud computing and is hugely accepted in US government documents and projects.

Kevin Curran et.al [4] mentions that Cloud Computing is an architecture that focuses on a scalable platform so as to provide on demand computing resources and services. Cloud computing has become a variable platform for organizations to build their infrastructures upon.

Randeep Kaur et.al [5] mentions some of the important and risky challenges related with cloud Storage. The challenges are Security, Privacy and Lack of Standards which slow down services in the cloud.

Rashmi Nigoti et.al [11] defines some privacy and security-related issues which are significant for cloud storage.

A. Discussion on Literature Review

The literature review contains the definitions of cloud computing defined by US National Institute of Standards and Technology (NIST). The NIST definition is one of the clearest and most comprehensive definitions of cloud computing and is widely referenced in US government documents and projects.

A number of researchers have discussed the security challenges that are raised by cloud computing. It is clear that the security issue has played the most important role in hindering the acceptance of Cloud Computing.

For security purpose of cloud storage various encryption techniques are being analyzed by

researchers. As discussed in literature review there are many security techniques which are currently applied to cloud storage.

EXISTING SYSTEMS

In Cloud Storage the 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, encryption algorithm[1] plays a important role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using encryption key and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is known as asymmetric key encryption where two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption [6].

There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption algorithms which were implemented in research work are as follows;

A. ***Data Encryption Standard (DES) Algorithm***

The Data Encryption Standard (DES) [2] is a symmetric-key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). 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. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen rounds [10]. Each round uses a different 48-bit key known as round key generated from the cipher key according to a predefined algorithm as shown in figure

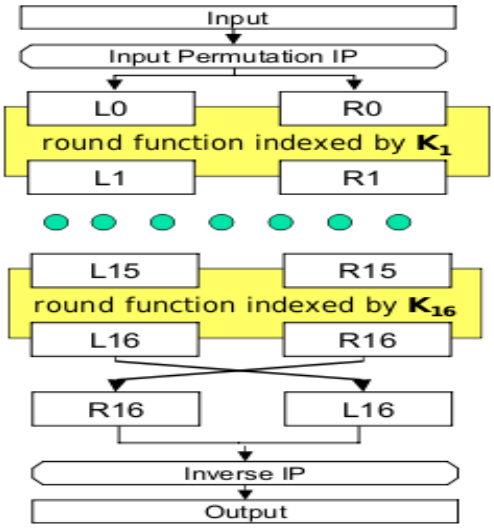

Fig. 1. Encryption with DES

DES performs an initial permutation on the entire 64 bit block of data. It is then divide into two, 32 bit sub-blocks, L0 and R0 which are then passed into what is known as rounds [10]. Each of the rounds are identical and the effects of increasing their number is such as - the algorithms security is increased and its temporal efficiency decreased. At the end of the 16th round, the 32 bit L15 and R15 output quantities are swapped to create what is known as the pre-output. This [R15, L15] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit cipher text.

B. ***RSA Algorithm***

The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm of asymmetric-key cryptography, involves a public key and a private key. The public key can be known to every member/user and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The process is shown in figure 2.

Key Generation

Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Fig. 2. RSA Algorithm

RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at encryption

$$C = M^e \bmod n$$

And at decryption side

$$M = C^d \bmod n.$$

Where n is a very large number, created during key generation process.

Rashmi Nigoti et.al [1], uses DES algorithm and RSA algorithm for providing security to cloud storage. In existing systems only single level encryption and decryption is applied to Cloud data storage. 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.

3. 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. The cloud provides all the benefits of an on-premise document management system; such as a content library, records of changes to each document and audit trails – but in a secure, online environment where authorized users access files at any time and from any device.

So, here we introduce a Cloud Based Data Management System (DMS) which provides security to documents using multilevel encryption algorithms. The main objective of Cloud Based DMS is the security of cloud data storage. To secure the cloud means secure the databases of the users stored in the cloud. And security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

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).

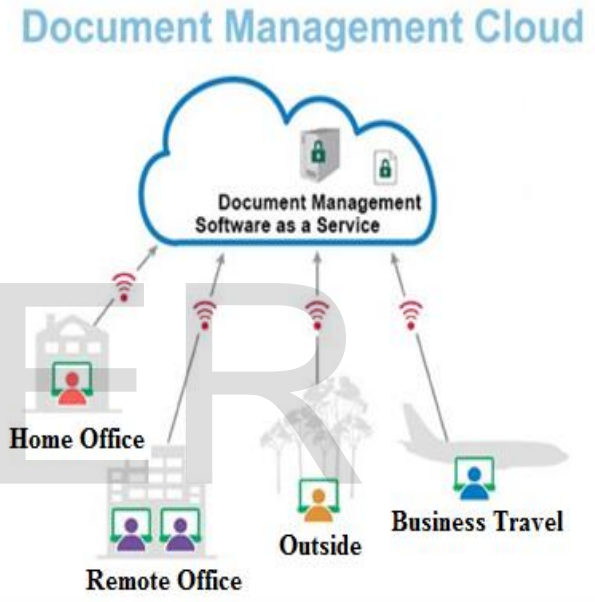

Fig. 3. Architecture of Cloud-Based DMS

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. Also, you're able to quickly and easily recover files if they lose during a break-in, network breach or natural disaster.
- Use of Web Browser:
  Cloud-based DMS is available through a simple Web browser Internet connection. 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 Algorithm*

We have proposed 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 files (e.g. Text, images, pdf etc)in Cloud-Based DMS. While uploading a 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 4.

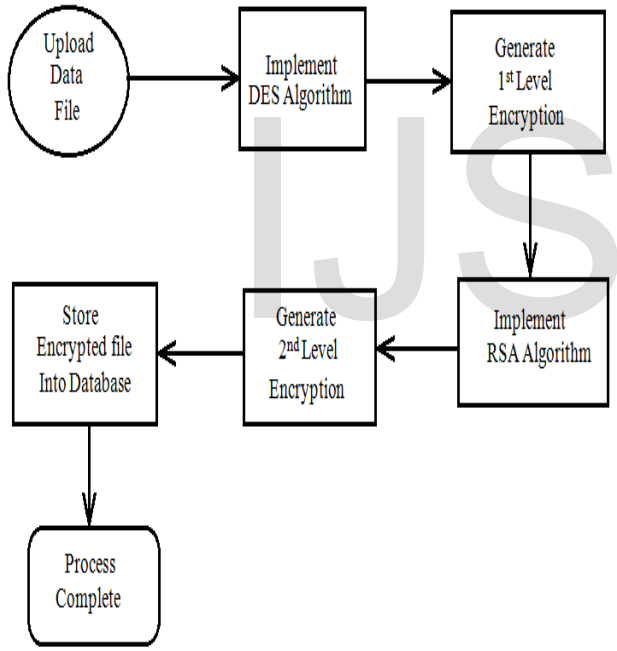

Fig.4. Block diagram of Multilevel Encryption

As Shown in figure 4, the steps of Multi-level encryption will be as follows;

- 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 [10].
- 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 [11] 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 of file inverse DES and RSA algorithms are used to decrypt data. The Block Diagram of proposed work at multilevel decryption is shown in following figure 5.

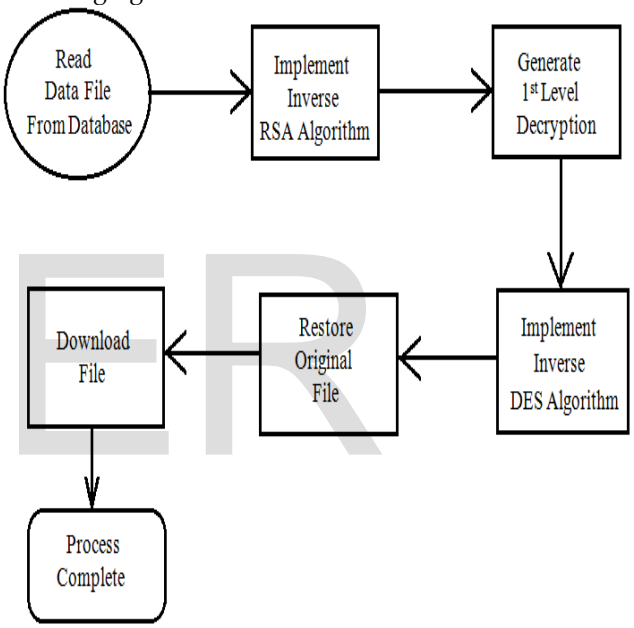

Fig. 5. Block diagram of Multilevel Decryption

As Shown in figure 5, 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. Means we applied multilevel Encryption and Decryption to cloud-based DMS for security purpose.

4. Conclusion

Cloud computing is the emerging field in the modern era. Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. As every organization is moving its data to the cloud, so there is a need to protect that data against unauthorized access, modification or denial of services etc. Cloud Computing can become more secure using cryptographic algorithms. But the existing 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 de-crypt 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.

5. 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] Rashmi Nigoti, Manoj Jhuria, 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.

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

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] S.C. Rachana, Dr. H. S. Guruprasad, "Emerging Security Challenges in Cloud Computing ", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3 Issue 2, pp.485-490, March 2014.

[9] Akhil Behl, "Emerging Security Challenges in Cloud Computing ", IEEE World Congress on Information and Communication Technologies, pp.217-222, 2011.

[10] G. Devi, M. Pramod Kumar, "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803, pp. 592-596, 2012.

[11] 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.

[12] Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication, NIST SP - 800-144, 80 pp., 2011.

[13] ERDOGMUS, "Cloud Computing: Does Nirvana Hide behind the Nebula? Software", IEEE 26, 2, 4-6, 2009.

[14] BERNSTEIN, D., LUDVIGSON, E., SANKAR, K., DIAMOND, S., MORROW, M. 2009. Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability. In Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference, pp.328-324, ICIW 2009.

[15] Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Modeling and Evaluation of Trust in Cloud Computing Environments" School of Information Science and Engineering, Northeastern University, Shenyang, P.R. China, Computing Center, Northeastern University, Shenyang, P.R. China, 3rd International Conference on Advanced Computer Control (ICACC 2011), 2011.

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

[17] 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.

[18] Puneet Jai Kaur, Sakshi Kaushal, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume 169, pp.103-112, 2011.

[19] Priyanka Arora, Arun Singh, Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing

Environment", World of Computer Science and Information Technology Journal, pp.179-183, 2012.

[20] L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security & Privacy Magazine, vol. 7, pp. 61-64, July2009.