IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Cloud Security Using Multilevel Encryption Algorithms

Miss Shakeeba S. Khan[1], Prof. Ms. R. R. Tuteja[2]

M.E. Scholar, Department of Computer Science & Engineering, PRMIT&R Badnera, Amravati, India[1]

Associate Professor, Department of Computer Science & Engineering, PRMIT&R Badnera, Amravati, India [2]

Abstract: Cloud generally relates with a set of hardware, storage of network, services, interfaces which are needed to combine and deliver the service for computing. The role of cloud is to provide the service for delivery of software, and storage of data on internet based on user demand. Because of these services cloud computing has become an important platform for companies to build their infrastructures upon. With growing publicity of cloud computing, related vulnerabilities or threats are also increasing because cloud services are often delivered by third party. So, security of the information in the cloud is the major issue for a cloud user. 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.

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

I. INTRODUCTION

Cloud Computing is the ability to access a pool of computing resources owned and maintained by a third party via the Internet. Cloud Computing performs the operation like distributed system where many computers can perform operation simultaneously.

Cloud is also used as a business solution for storage. It provides a vast amount of storage in all sectors like Government, Enterprise etc. Apart from government and enterprise one can also achieve storage of their personal data on cloud. So there is a need to protect Cloud data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the user's databases hosted by the Cloud provider.

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.

II. CHALLENGES AND ISSUES IN CLOUD COMPUTING

Security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully evaluated with respect to the security.

Current cloud environment is associated with numerous challenges as follows;

A. Governance

Governance implies management and oversight by the organization over procedures, standards and policies for application development and data technology service acquirement, also because the style, implementation, testing, use, and watching of deployed or engaged services.

B. Malicious Insiders

This threat is well known to most organizations. 'Malicious insiders' impact on the organization is considerable. Malicious insiders are the threat which has access to the data or information about the organization being a member of the organization. As cloud consumers application data is stored on cloud storage provided by cloud provider which also has the access to that data.

C. Data Integrity

Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exists.

D. Account or service Hijacking

This threat occurs due to phishing, fraud and software vulnerabilities. In this type attacker can get access to critical areas onto the cloud from where he can take permit and steeling important information leading to compromise of the availability, integrity, and also confidentiality to the services.

E. Insecure APIs

Anonymous access, reusable tokens or password, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring, and logging capabilities etc security threats may occur to organizations if the weak set of interfaces and APIs are used [11].

DOI 10.17148/IJARCCE.2016.5116

III.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. This will helps us in reduction of Virtualization vulnerability. For secure communication between the host domain and the guest domain, or from hosts to management systems, encryption technologies, such as Secure HTTP (HTTPS), encrypted Virtual Private Networks (VPNs), Transport Layer Security (TLS), Secure Shell (SSH), and so on should be used. Encryption will help prevent such exploits as man-in-the-middle (MITM), spoofed attacks, and session hijacking [5].

A. Advanced Encryption Standard (AES) 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 Feistel rounds [10]. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm as shown in figure 1.

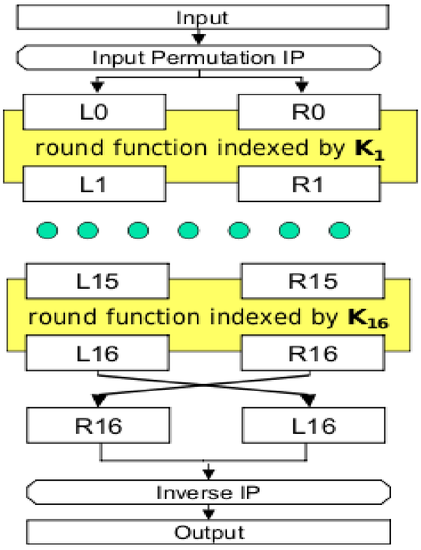


Fig. 1. Encryption with DES

DES performs an initial permutation on the entire 64 bit block of data. It is then split into two, 32 bit sub-blocks, L0 and R0 which are then passed into what is known as Feistel rounds [10]. Each of the rounds are identical and the effects of increasing their number is twofold - 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. 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. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. As well as these differences AES differs from DES in that it is not a Feistel structure. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key. The overall structure of AES can be seen in figure 2.

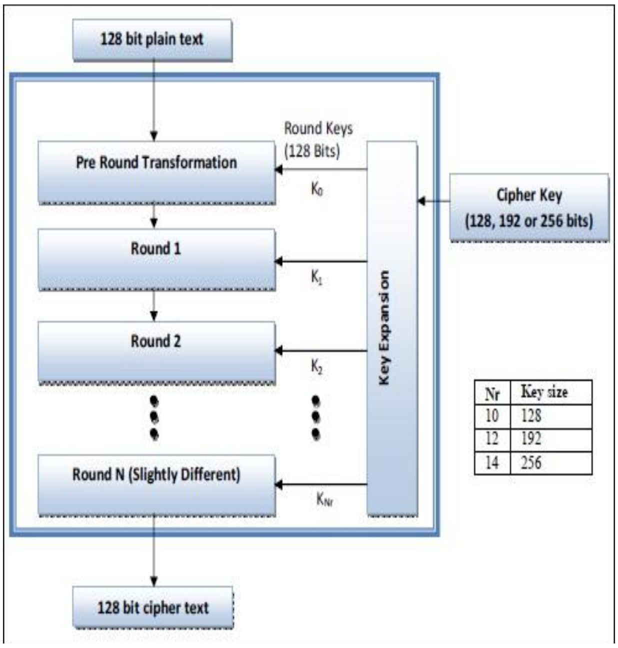
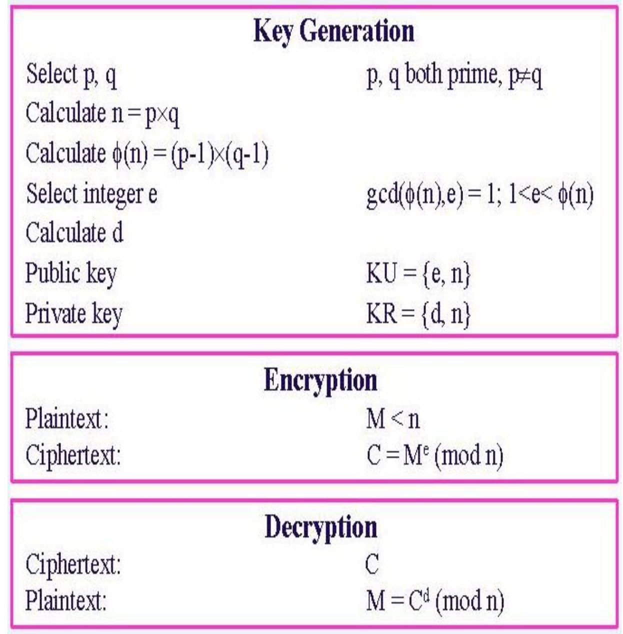


Fig. 2. Encryption with AES

C. 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 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. The process is shown in figure 3.

DOI 10.17148/IJARCCE.2016.5116



Key Generation

Select p, q	p, q both prime, p≠q
Calculate n = p×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. 3. 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.

D. *Homomorphic Algorithm*

Cloud consumer encrypts its data before sending to the Cloud provider, but each time he has to work on that will have to decrypt that data. The consumer will require giving the private key to the server to decrypt the data before to perform the calculations required, which might influence the confidentiality of data stored in the Cloud. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption); the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data. Homomorphic encryption is distinguishing, according to the operations that are performed on raw data.

- Additive Homomorphic encryption: additions of the raw data.
- Multiplicative Homomorphic encryption: products for raw data.

Rashmi Nigoti et.al [11] expalins DES algorithms, AES algorithm, RSA algorithm and Homomorphic algorithm for security of 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.

IV. 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 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. Also, you're able to quickly and easily recover files if they lose during a break-in, network breach or natural disaster.

DOI 10.17148/IJARCCE.2016.5116

- Use 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.

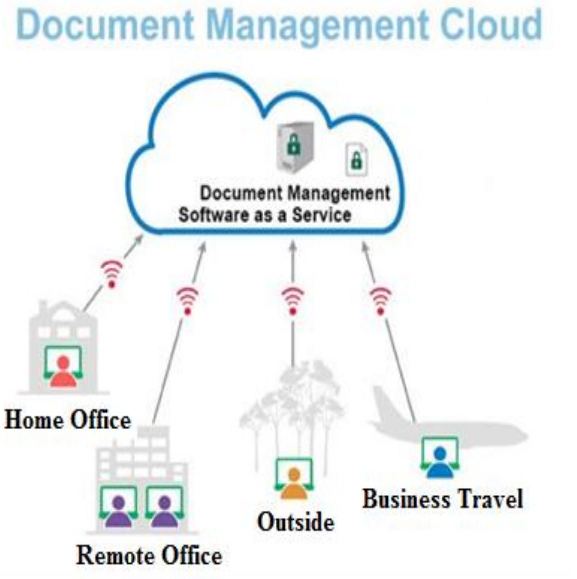

Document Management Cloud
Document Management Software as a Service
Home Office
Remote Office
Outside
Business Travel

Fig. 4. Architecture of Cloud-Based DMS

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;

- 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.

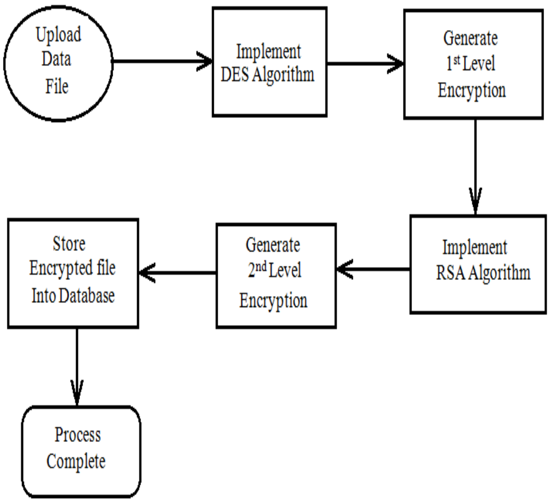

Upload Data File
Implement DES Algorithm
Generate 1st Level Encryption
Implement RSA Algorithm
Generate 2nd Level Encryption
Store Encrypted file Into Database
Process Complete

Fig.5. Block diagram of Multilevel Encryption

And while downloading 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 6.

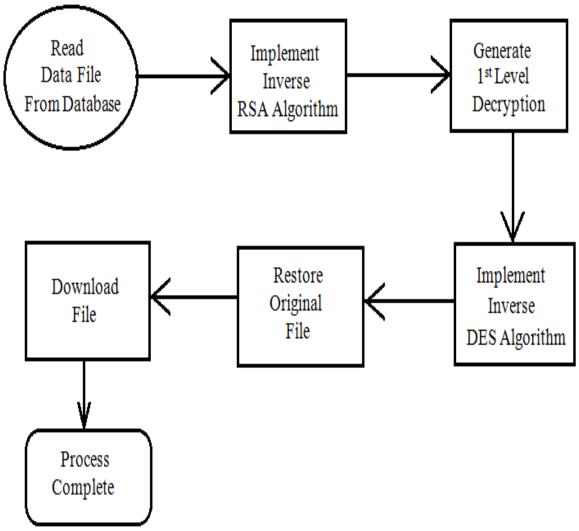

Read Data File From Database
Implement Inverse RSA Algorithm
Generate 1st Level Decryption
Implement Inverse DES Algorithm
Restore Original File
Download File
Process Complete

Fig. 6. Block diagram of Multilevel Decryption

As Shown in figure 6, 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

DOI 10.17148/IJARCCE.2016.5116

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.

V. 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

Following figures illustrates the implementation of multilevel encryption algorithms.

In figure 7 pdf files which uploaded on Cloud Based DMS are shown.

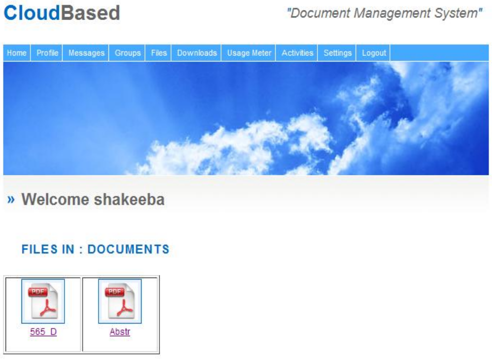
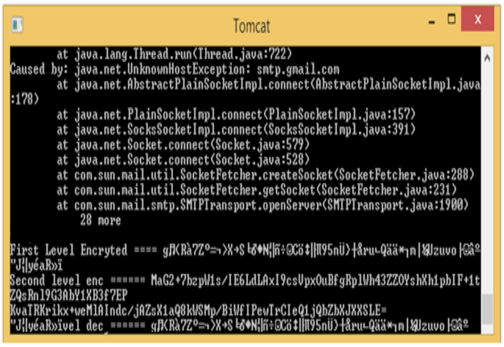


Fig. 7. User uploaded PDF Documents in Cloud Based DMS

Both the first level and second level encryption applied on the pdf files are shown in following figure 8;



```
        at java.lang.Thread.run(Thread.java:722)
Caused by: java.net.UnknownHostException: smtp.gmail.com
        at java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java
:178)
        at java.net.PlainSocketImpl.connect(PlainSocketImpl.java:157)
        at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:391)
        at java.net.Socket.connect(Socket.java:579)
        at java.net.Socket.connect(Socket.java:528)
        at com.sun.mail.util.SocketFetcher.createSocket(SocketFetcher.java:288)
        at com.sun.mail.util.SocketFetcher.getSocket(SocketFetcher.java:231)
        at com.sun.mail.smtp.SMTPTransport.openServer(SMTPTransport.java:1900)
            28 more

First Level Encryted ==== gЛ<Rà7Z°=¬>X→S ╘δ♦N¦|ñ÷©Cö‡||П95nÜ>╀åru└Qää*┐m|¾Uzuvo├©â º
"J¦|yéaR»ï
Second level enc ====== MaG2+7bzpW1s/IE6LdLAxI9csVpxOuBfgRplWh43ZZOYshXh1pbIF+1t
ZQsRnl9G3AbY1XB3f7EP
KvaTRKrikx+weMlAIndc/jAZsX1aQ8kWSMp/BiWfIPewTrCIeQ1jQbZbXJXXSLE=
"J¦|yéaR»ïvel dec ====== gЛ<Rà7Z°=¬>X→S ╘δ♦N¦|ñ÷©Cö‡||П95nÜ>╀åru└Qää*┐m|¾Uzuvo├©â º
```

Fig. 8. First and Second level Encrypted data of Pdf files shown on Tomcat server

VI. 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 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] 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] 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.

[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] KEAHEY, TSUGAWA, MATSUNAGA, FORTES, J. 2009. Sky Computing. Internet Computing, IEEE 13, 5, 43-51, 2009.

[15] NURMI, WOLSKI, GRZEGORCZYK, OBERTELLI, SOMAN, YOUSEFF, ZAGORODNOV, D. 2008. The Eucalyptus Open-source Cloud-computing System. Proceedings of Cloud Computing and Its Applications, 2008.

[16] 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.

[17] Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, “Modeling and Evaluation of Trust in Cloud Computing Environments” School of lnformation 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.

[18] 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.

[19] 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.

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

DOI 10.17148/IJARCCE.2016.5116