ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Security in Cloud Computing using Cryptographic Algorithms

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

M.E. Scholar, Dept. of Computer Sci. & Engg., PRMIT&R, Sant Gadge Baba Amravati University, India[1]

Associate Professor, Dept. of Computer Sci. & Engg., PRMIT&R, Sant Gadge Baba Amravati University, India[2]

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 third party provider who owns the infrastructure. Benefits of cloud storage are easy access means access to your knowledge anyplace, anyhow, anytime, scalability, resilience, cost efficiency, and high reliability of the data. Because of these benefits each and every organization 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 the treatments (calculations) and storage (databases hosted by the Cloud provider). In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using cryptographic algorithms to enhance the security in cloud as per different perspective of cloud customers.

KEYWORDS: Cloud Computing, Cryptographic Algorithm, Infrastructure, Internet, Security Issue.

I. 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 information and computer resources 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. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. 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 treatments (calculations) and 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 accomplished by cryptography. Cryptography, in modern days 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.

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 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

II. LITERATURE REVIEW

Cloud computing has been defined by US National Institute of Standards and Technology (NIST) [12] as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction ".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.

Brian Hay et. al [3] have focused on data authentication, data integrity, querying and outsourcing the encrypted data. Their research says that, the risks can arise at operational trust modes, resource sharing, new attack strategies. In operational trust modes, the encrypted communication channels are used for cloud storage and do the computation on encrypted data which is called as homomorphic encryption [6]. New attack strategies like Virtual Machine Introspection (VMI) can be used at virtualization layer to process and alter the data.

Kevin Curran et.al [4] mentions that Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud computing has become a variable platform for companies to build their infrastructures upon. If companies are to consider taking advantage of cloud based systems by storing their data in Cloud Storage they will be faced with the task of seriously reassessing their current security strategy.

Randeep Kaur et.al [5] mentions some of the notable challenges associated 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 that are believed to have long-term significance for cloud storage.

John C. Mace et.al [21] have proposed an automated dynamic and policy-driven approach to choose where to run workflow instances and store data while providing audit data to verify policy compliance and avoid prosecution. They also suggest an automated tool to quantify information security policy implications to help policy-makers form more justifiable and financially beneficial security policy decisions.

A. *Summary 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 survey there are many security techniques which are currently applied to cloud storage. Apart from this there are still too many areas which require further enhancements like more efficient algorithms can be developed which can increase the security level in the cloud storage.

III. EXISTING ALGORITHMS FOR CLOUD SECURITY

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, encryption algorithm [1] plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the 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].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

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 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.

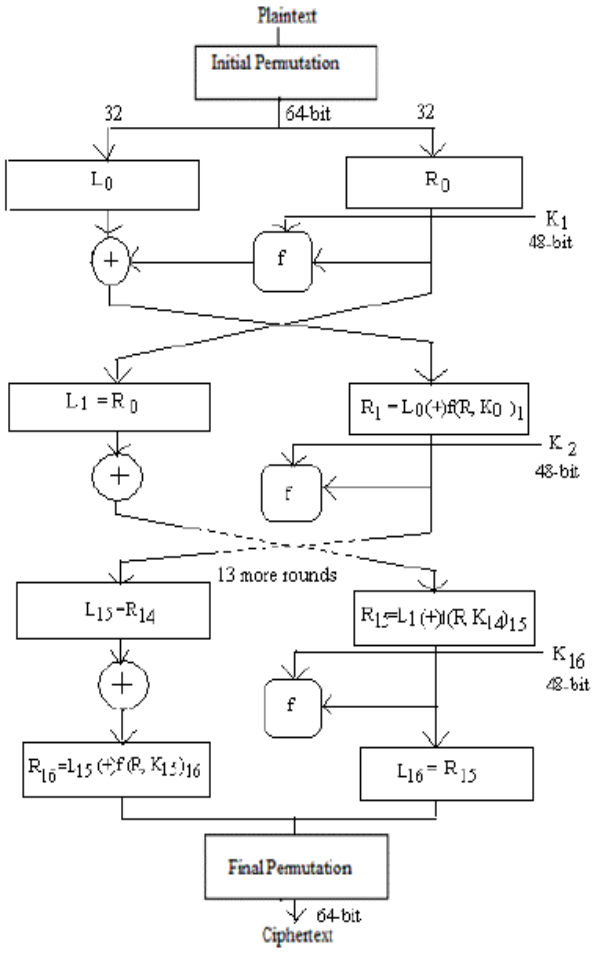

Fig. 1. Encryption with DES

DES performs an initial permutation on the entire 64 bit block of data. It is then split into two, 32 bit sub-blocks, L_0 and R_0 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 L_{15} and R_{15} output quantities are swapped to create what is known as the pre-output. This [R_{15}, L_{15}] 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.

The function f is made up of four sections:

- Expansion P-box
- A whitener (that adds key)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

- A group of S-boxes
- A straight P-box.

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 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 2.

Key Generation

Select p, q	p, q both prime, p≠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 [11], 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.

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

connected resources that comprise a cloud. To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task.

A. *Proposed System Design:*

The proposed system is designed to maintain security of text files only. This proposed system uses DES & RSA algorithm to generate encryption when user uploaded the text files in Cloud Storage and inverse DES & RSA algorithm to generate decryption when user download file from Cloud Storage, for increasing security.

The proposed system is designed to maintain security of text files only. The proposed system design focuses on the following objectives which are helpful in increasing the security of data storage.

1) For Encryption of text files:

- Upload Text file.
- Implementing the DES algorithm of Encryption to generate first level encryption.
- Implementing the RSA algorithm of Encryption to generate second level encryption.
- Store Cipher Text into Database.

2) For Decryption of text files:

- Read Cipher Text from Database.
- Implementing the RSA algorithm of Decryption to generate first level decryption.
- Implementing the DES algorithm of Decryption to generate Plain text.
- Display Plain Text to User.

B. *Proposed 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 Text file in Personal Cloud Storage. When 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 3.

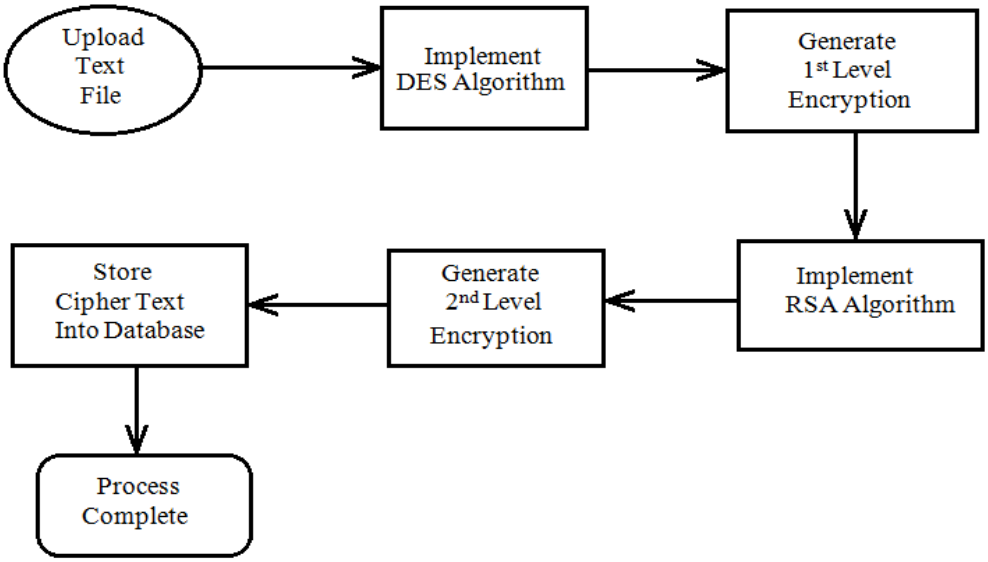

Fig. 3. Block Diagram of Multilevel Encryption

As Shown in figure 3, the steps of Multi-level encryption will be as follows;

- Upload the text 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

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 when 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 4.

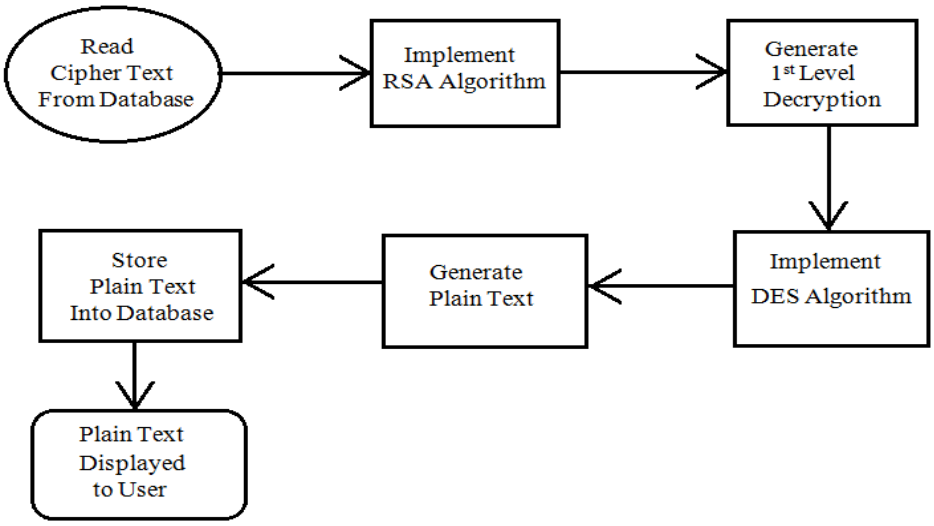

Fig. 4. Block Diagram of Multilevel Decryption

As Shown in figure 4, 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 decrypt 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 provide security for cloud storage data.

V. CONCLUSION

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 each and every organization 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Cloud Computing can become more secure using cryptographic algorithms. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms.
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.

As our proposed algorithm is a Multilevel Encryption and Decryption algorithm. Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is expected that using multilevel encryption will provide more security for Cloud Storage than using single level encryption.

REFERENCES

1. AL.Jeeva, Dr.V.Palanisamy And 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 and 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 and 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 and 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. L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security & Privacy Magazine, vol. 7, pp. 61-64, July2009.
9. 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.
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 and 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. G. Lin, D. Fu, J. Zhu, and G. Dasmalchi, "Cloud Computing: IT asa Service," IT Professional, vol. 11, pp. 10-13, Mar./Apr.2009.
14. Mandeep Kaur and Manish Mahajan, "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Vol. 2, pp.831-835, October 2012.
15. Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 3, pp.1922-1926, Jul-Aug 2013.
16. Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , "Cloud Computing System Based on Trusted Computing Platform", International Conference on Intelligent Computation Technology and Automation, Volume 1, pp.942-945, 2010.
17. Pearson, S., Benameur, A., Privacy, "Security and Trust Issues Arises from Cloud Computing", Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference, pp.693-702, 2010.
18. 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.
19. Puneet Jai Kaur, Sakshi Kaushal, "Security Concerns in Cloud Computing", Communication in Computer and Information Science Volume 169, pp.103-112, 2011.
20. 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.