www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 18897-18906

Review on Security Management in Cloud computing

Gouri Ajeev [1], Karthik Karunakaran [2], Arpita Gaur[3], Priya G[4]
[1]Undergraduate, VIT University
[2]Undergraduate, VIT University
[3]Undergraduate, VIT University
[4]Assistant Professor in dept. of CSE, VIT University
School of Computer Science and Engineering, VIT University, Vellore, India

Abstract

The basic ideas involving cloud computing were first came into picture in 1960, when John McCarthy stated that "computation may someday be organized as a public utility". But the concept of Cloud computing started drawing attention of the IT world until recently. It is changing the focus of enterprises. It has become a part of normal work flow for thousands of users on the internet. Cloud computing gained attention due to many of its salient features such as reduced storage cost, ‘pay per use’ policy, the growing technology of visualization, SOA (Service Oriented Architecture) and also because of development in internet security. Cloud security is one of the major challenges in cloud computing. This paper focuses on various cloud security issues and methods to enhance the security of data storage and processing in the clod environment. The definition of cloud computing and some of its features are also discussed in this paper.

Keyword*:* Cloud Computing, Cloud Security, Cloud Security Issues, Encryption, Decryption.

Introduction

Cloud computing is a very easy method through which we can get access to shared pool of resources, which can be configured and released with minimal effort. National Institute of Standards and Technology (NIST), has defined Cloud Computing as follows: Cloud computing is a model for enabling ubiquitous, 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.[1]”The consumers are provided with capabilities related to IT as “service”, instead of product produced using internet. To get inexpensive computing infrastructures that are on-demand and also gives a good quality of service levels, cloud computing serves all these needs. Including security is a major struggle for many developers. In other cases, providing security with currently affordable technological capabilities is very hard for the developers [2].

Cloud computing gives us the power to move the work done on client side to some unseen cluster over the internet. Maintaining database and applications for the users to access it through a network independently on a remote network is the work of a Cloud Service Provider (CSP).

Service Models of cloud computing

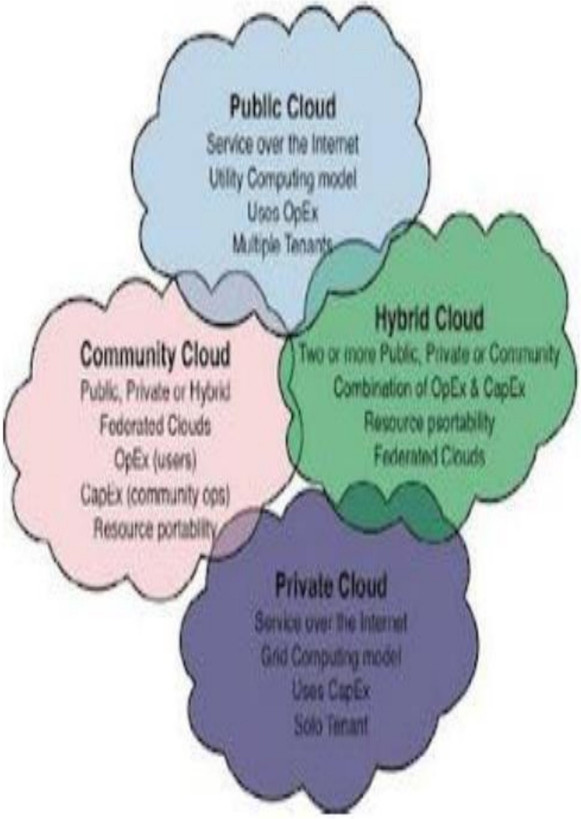
According to NIST’s cloud computing definition, it has three service models software as a service, platform as a service and infrastructure as service and four deployment models private cloud, public cloud ,hybrid and community cloud.[31] If a customer needs any service first he has to send a request to a service provider.[31]

DOI: 10.18535/ijecs/v5i11.31

1. Software as a Service (SaaS): Software as a Service consists of software running on the provider's cloud infrastructure, delivered to multiple clients on demand through a thin client such as a browser over the Internet. User need not install any software for running. Common examples are Google Docs and Salesforce.com.

2. Platform as a Service (PaaS): It provides a running environment for any application. Developers are given the flexibility so that they can develop applications on provider's platform. Storage, database, and scalability are the main services provided. Common examples are Google App Engine.

3. Infrastructure as a Service (IaaS): The service provider provides the entire hardware as a service and is responsible for maintaining, running and housing it. The client pays as per the usage of services. IaaS provides on demand access to resources (networking, servers and storage), which could be accessed via a service API. Common examples are Flexiscale, AWS: EC2 (Amazon Web Services).



Cloud Computing Deployment Models

Depending on infrastructure ownership, there are four deployment models.[5]. The security issues start with these four deployment models

1. The Public Cloud .Public cloud is the one which dynamically provisions the resources on a self service basis over internet. Large organizations usually are the owners.(e.g.
Amazon, Google's AppEngine and
Microsoft Azure). In terms of privacy issues and security, this would be the most cost effective model since the provider's infrastructure normally traverses many national boundaries. [6].

2. The Private Cloud*:* In its predominant use of virtualization, this model varies from the traditional data enter. Since the users will have to buy, build and manage, hey have been criticized such that they do not benefit from lower capital costs and less hands on

DOI: 10.18535/ijecs/v5i11.31

management. Private cloud attracts enterprises especially in safety critical organization and missions.

3. The Community Cloud: A community may have organizations which can all share this type of cloud infrastructure, and any of these organization can be responsible to manage it or a third party can also manage it. A common example is the Open Cirrus Cloud Computing Testbed, which is a collection
of Federated data centres across six sites spanning from North America to Asia.

4. The Hybrid Cloud: Of all the models discussed above, hybrid can be a combination of two or (or all). Standardization of APIs has led to easier distribution of applications across different cloud models.

We are dealing with many issues like multi tenancy, data loss and leakage, easy accessibility of cloud, identity management, unsafe API's, inconsistencies in service level agreement, patch management, internal threats etc. in cloud computing. [3] This paper mainly focuses on the major security issues in cloud computing and the mechanisms and algorithms that are adopted in the security management in cloud computing.

SECURITY ISSUES IN CLOUD

In cloud computing security issues are the major threats faced today. Recent research have discussed about the increasing number of threats in cloud computing. This is the reason that new security algorithms and techniques are being developed and existing ones are being improved.

Major threats faced are: [7]

- Data security breaches
- Fake credentials and breach in authentication.
- Hacking of interfaces
- Unauthorised API
- Exploitation of vulnerable sections of the system
- Account trafficking and hijacking
- Hostile insiders
- Complete data loss
- Dos attacks

Security algorithms and techniques to counter these threats exists and in this paper discusses about the comparison of these techniques in detail.

DETAILED DESCRIPTION OF COMMON ENCRYPTION ALGORITHMS

Encryption of data is done with the help of keys. The encryption and decryption of the user data is done through the same key values. This type of algorithms can be termed as cryptographic algorithms. There are a lot of cryptographic algorithms available in market, which can be used for security purposes. Some frequently used encryption algorithms are being analysed herein this paper.

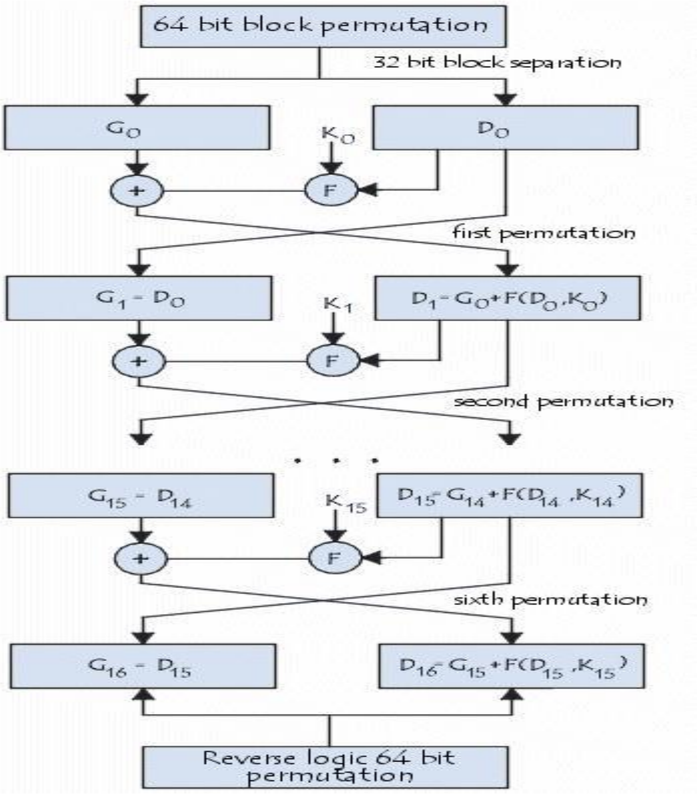
- **RIVEST-SHAMIR- ADLEMAN(RSA)**

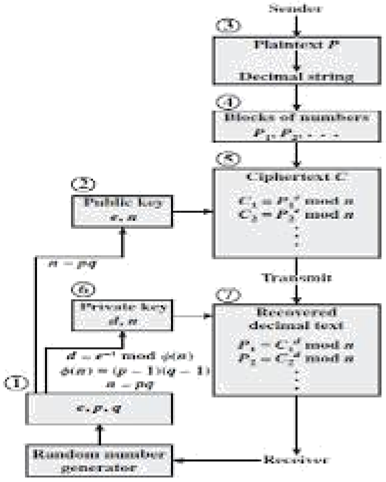
  The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977. The basic technique was first discovered in 1973. The RSA algorithm is the most popularly used public key cryptography algorithm in the world. It can be used to encrypt any data message without exchanging any secret key to the receiver.

The algorithm performs the encryption with two random numbers to create the needed public keys and private keys. These keys are used for encrypting and decrypting the data at the sender’s end and receiver’s end respectively. Sender encrypts the message which is required to be sent across the channel using the receiver’s public key and when the message arrives at the receiver’s side, the receiver can decrypt the encrypted message using their separately generated private keys [8] [9].

- **DATA ENCRYPTION STANDRAD (DES)**

The Data Encryption Standard is an old algorithm which is not recently used. And it is a symmetric-key method of message encryption. DES encrypts and decrypted the data using the same private key, so both the sender and the receiver must be aware of the key and use the same private key. It was initially developed by IBM, but was later acquired by NIST. DES encryption method is block cipher technique. In this technique blocks of data consisting of 64 bits can be encrypted and decrypted by using a 64 bit key[10][11]. Even though DES is considered to be old fashioned and old-timer, it is used by the finance and marketing sectors and other industries around the globe to protect their real time online web services and applications [12] [13].





- **TRIPLE DES**

Triple-DES encryption uses a triple-length DATA key. This key is comprised of three 8-byte DES keys to encrypt 8 bytes of data.

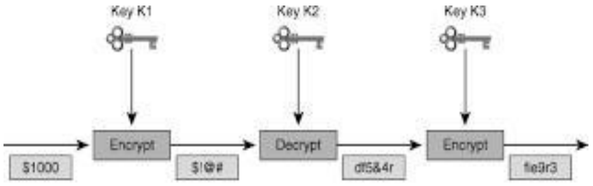
- Initially encrypt the data using the first key.
- Next decipher the encrypted data using the second key.
- Then lastly encipher the current decrypted message using the third and final key.

The procedure is reversed to decrypt data that has been encrypted using the triple-DES security algorithm:

- First decipher the data which has been received using the third key.
- Then encipher the decrypted data using the second key.
- Finally decipher the current result using the initial key.

So the total number of bits for the combined key size will be 168 bits. The complete process of TDES involves three 64-bit keys (Key1, Key2, and Key3) in the EDE model [14].

When the 3-DES the 3-times iteration process is applied to increase the encryption level and as the level of encryption increases, the average time also increases. This is considered as the major drawback in 3-DES. The 3DES algorithm is one of the slowest techniques. It is slower than most of the other block cipher methods [15] [16].



- EDE (Encrypt-Decrypt-Encrypt) Method – 3DES-EDE Method:
  - Data is encrypted using K1.
  - Data is decrypted using K2.
  - Data is encrypted using K3.
- If K1 = K3, Key Yields 112-Bit Key Length
- If K1 ≠ K3, Key Yields 168-Bit Key Length

- **Advanced Encryption Standard (AES)**

AES is a relatively new and latest encryption technique suggested by NIST to replace the old and outdated DES algorithm in 2001. AES algorithm has a huge advantage over the rest of the algorithms in the market,
it can be used to support any data of multiple combinations (128 bits). And the keys used in this technique are of various lengths (128, 192, and 256 bits).

The security process in AES system involves 10 rounds for 128-bit keys initially, and then it has to go through 12 rounds for 192-bit keys, and lastly 14 rounds for 256-bit keys in order to obtain the final encrypted text or to get back the original plain text, that is the initial message. AES allows data length of size 128 bits that can be split into four operational blocks [15].

The output has to go through nine rounds and during each of these nine round it has to go through four transformation.

- Substitution of bytes
- Shifting of rows
- Mixing of columns
- Addition of round key

And in the last and ultimate round (Round 10), the Mixing of columns transformation is not performed [16].

Decryption is the reverse process of encryption and uses the opposite of the functions used during the encryption process.

- Inverse Substitution of bytes
- Inverse shifting of rows
- Inverse mixing of columns [17].

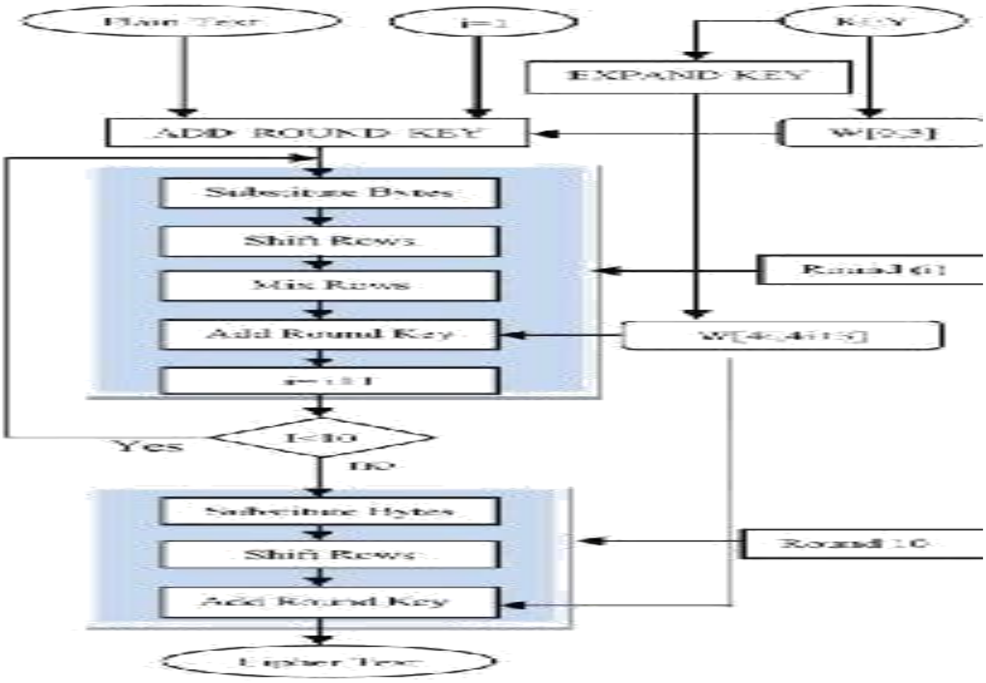
characters. This is the recent area of interest where ASCII characters are also encrypted and decrypted along with the Unicode characters [18].

Binary code segment is split into several sections for which accordingly DNA digital loading is performed. As BDEA algorithm can be used for Unicode character set too, hence a whole wider range of cloud service users can be reached and serviced easily.

MULTI-LEVEL ENCRYPTION

This method of encryption is much more complex and secure than previously existing security algorithms as it goes through multiple level of encryptions. Using this method of encryption the user can choose the security depth. This provides a lot of flexibility to the users and this way the users can change the security measures according to their need [19].

There are two methods in this technique. The first method is the Rail fence cipher algorithm that will use for Transposition and the other one is the Caesar cipher for substitution. In this method it is difficult to understand the cipher text compared with the other techniques [20].

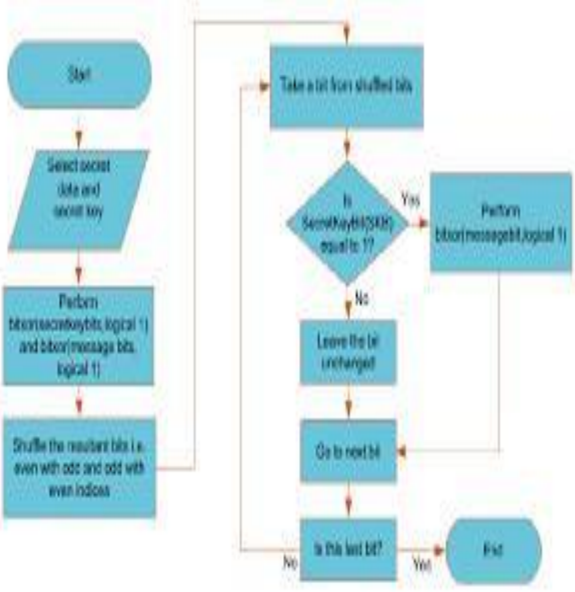


- **BI-DIRECTIONAL DNA ENCRYPTION**

Bidirectional DNA encryption algorithm (BDEA) is applied to counter the data security threats in cloud computing services and environment. Bidirectional DNA encryption algorithm can cipher Unicode characters as well as ASCII

COMPARITIVE STUDY OF SECURITY ALGORITHMS

The following table gives the comparative study about the different security algorithms widely used in the market in recent times [21] [22] [23].


Start
Select secret data and secret key
Perform bitxor(secretkeybits,logical 1) and bitxor(message bits, logical 1)
Shuffle the resultant bits i.e. even with odd and odd with even indices
Take a bit from shuffled bits
Is SecretKeyBit(SKB) equal to 1?
Yes
Perform bitxor(messagebit,logical 1)
No
Leave the bit unchanged
Go to next bit
Is this last bit?
No
Yes
End

FACTORS	RSA	DES	3DES	AES
CREATE	Rivest, Shamir	IBM in	IBM in	Rijmen

D BY	and Aldeman in 1978	1975	1978	and Daemen in 2001
KEY LENGTH	Depends in no. of bits	56 bits	168 bits or 112 bits	128, 192 or 256 bits
ROUND(s)	1	16	48	10, 12 or 14
BLOCK SIZE	Variable	64 bits	64 bits	128 bits
CIPHER TYPE	Asymmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
SPEED	Slowest	Slow	Very Slow	Fast
SECURITY	Least secure	Not secure enough	Adequate security	Excellent security

CONCLUSION AND SCOPE OF FUTURE WORK

This paper discusses about the popular encryption algorithms. The use of internet has increased exponentially in the last decade. And in the recent years the use of cloud computing services has been the most sought after service. The users store their data on cloud servers and this data is being transmitted nearly around the globe to be stored in multiple locations. So the need for secured data transmission over the network has increased.

In this research paper a survey on existing encryption/encoding algorithms/techniques has been done. And with all the analysis we can come to the conclusion that all the techniques available in the current market is useful for encrypting Real-time data. Each technique is unique and useful in its own way, which might be suitable for different applications based on the specific requirements of that particular application. And each technique has its own advantages and disadvantages.

Based on the research done and literature survey it is found that AES is the most efficient in terms of speed, time, avalanche effect and throughput. And we can also come to the conclusion that the security level of all the above discussed algorithms can be enhanced and improved by used multiple security algorithms simultaneously. If more than one algorithm is applied at a time then the security provided by the technique is improved by a considerable margin.

And our future work will involve use of combination and enhancement of these algorithms. And multiple security algorithms will be applied either in a sequential or parallel fashion to create a more secure and safe mode of transmission of data.

References

[1]. Peter Mell, Timothy Grance "The NIST Definition of Cloud Computing"
NIST Special Publication 800-145.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 25:599616, 2009. [3]SachdevAbhaThakral, and MohitBhansali. "Addressing the Cloud Computing Security Menace." IJRET, Volume 2, Issue 2, pp. 126-130, Feb 2013.

[4] R. Buyya, S. Pandey, and C. Vecchiola, Cloudbus toolkit for market-oriented cloud computing, in Proceedings 1st International
Conference on Cloud Computing (CloudCom 09), Beijing, 2009, pp. 3_27.

[5] Tharam Dillon, Chen Wu and Elizabeth Chang, Cloud Computing: Issues and Challenges, 2010 24th IEEE International
Conference on Advanced Information Networking and Applications, 1550-445X/10.

[6] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the
clouds: A 32Berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-
2009-28, 2009.

[7] Jaspreet Singh, Sugandha Sharma, "
Review on Cloud Computing Security Issues and Encryption Techniques"

[8] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's",
International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 386-391, July 2012.

[9] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121, 2011 [10]Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari,
"Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical,
Electronics and Computer Science, pp. 1-5, 2012.

[11] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, pp. 106-111, January 2011.

[12] Tingyuan Nie, Chuanwang Song and Xulong Zhi, "Performance Evaluation of DES and Blowfish Algorithms", IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), pp. 1-4, 23-25 Apr 2010.

[13] Shashi Mehrotra Seth, Rajan ishra,
"Comparative Analysis of Encryption Algorithms for Data Communication",
International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.

[14] E. Thambiraja, G. Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 226-233, July 2012

[15] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in
Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.

[16] Aized et al "Encryption Techniques For Cloud Data Confidentiality",
International Journal of Grid Distribution Computing Vol.7, No.4 (2014)

[17] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha, "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System", International Journal of Multidisciplinary Research, Vol.1 Issue 4, pp. 143-151, August 2011.

[18] Zilhaz Jalal Chowdhury, Davar
Pishva and G. G. D. Nishantha, "AES and Confidentiality from the Inside Out", the
12th International Conference on Advanced Communication Technology (ICACT), pp. 1587-1591, 2010.

[19] Amit "Enhancing Security in Cloud Computing Using Bi-Directional DNA
Encryption Algorithm" Springer 2015

[20] Dr.A.Padmapriyaet "Cloud Computing: Security Challenges &
Encryption Practices", Volume 3, Issue 3,
March 2013

[21] S. Pavithra and Mrs. E. Ramadevi, "Performance Evaluation of Symmetric Algorithms", Journal of Global Research in Computer Science, Volume 3, No. 8, pp. 43-45, August 2012.

[22] Shashi Mehrotra Seth, Rajan ishra,
"Comparative Analysis of Encryption Algorithms for Data Communication",
International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.

[23] Priyanka Arora, Arun Singh and Himanshu Tiyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and InformationTechnology Journal (WCSIT), Vol. 2, No.
5, pp. 179-183, 2012.

[24] V.K. Zadiraka & A. M. Kudin, "Cloud Computing In Cryptography And Steganography", in Cybermetics and Systems Analysis, Vol.49, No. 4, July-2013, UDC 681,3;519,72;003,.26.

[25] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan & Bhavani Thuraisingham,
"Security Issues for Cloud Computing" in International Journal of Information Security and Privacy, 4(2),39-51, April-June 2010.

[26] Rashmi Nigoti, Manoj Jhuria & Dr.
Shailendra Singh," A Survey of Cryptographic algorithms for Cloud Computing. In International Journal of Emerging Technologies in Computational and Applied Sciences(IJETCAS), ISSN(print) 2279-0047, ISSN(online):2279-0055.

[27]Patidar , S "Survey on cloud computing" , in Advanced computing and communication technologies , IEEE , Jan- 2012..

[28] M. Vijayapriya, "Security algorithm In Cloud Computing: Overview"/International Journal of Computer Science & Engineering Technology(IJCSET)

[29] L. Singh and R. K. Bharti, "Comparative perfomance analysis of cyptographic algorithms", International journal of advanced research in computer science and software engineering (IJARCSSE), vol. 3, no. 11, **(2013)**.

[30] R. L. Rivest, "The RC5 Encryption Algorithm", MIT laboratory for C.S,
Cambridge.

[31] Priya .G, Jaisankar N ,"*A Reputation Based Trustworthy System For Cloud Environment*"in International Journal of pharmacy and Technology,Vol 8,No 3 ,pp No: 16702-16708, September 2016.