International Journal of Database Theory and Application
Vol.8, No.3 (2015), pp.145-154
http://dx.doi.org/10.14257/ijdta.2015.8.3.12

A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks

Navdeep Singh and Pankaj Deep Kaur

Department of Computer Science
GNDU Regional Campus Jalandhar
Navvdeep.singh@gmail.com

Abstract

Any technology cannot be said perfect until it is free from any vulnerability. So whenever a new technology is introduced the security is the first feature that is countable. There are many famous technologies that are used for online data storage, accessing the data from any location and provide the online use of any software. Cloud computing is the same technology that provides the online data storage and the most important feature that it provides software on lease facility. If large data storage feature took into consideration then it must be said that if a user wants to store the data on cloud then the security of that data must be the first requirement of the user. In this paper an integrated approach is introduced to encrypt and decrypt the data before sending on cloud by using the two different techniques. And the performance analysis is done on the basis of different parameters to achieve the better performance and security.

Keywords: *DoS attacks, RSA, AES, Cloud Computing, Security*

1. Introduction

Cloud computing is the very famous technology that provides the facilities of large data storage and the use of software by paying for that [1]. Cloud computing provides the software as a service, platform as a service and infrastructure as a service facilities. Though many features are provided by cloud computing but there are still some holes regarding security. Among these holes we took the DoS attack [2] into the consideration in which an attacker send fake requests again and again to consume all the resources and when a legitimate request try to execute the process then system denies to process the same request because of un availability of resources [3]. In this paper an integrated approach is introduced to to prevent the fake request by double encryption of data so the fetching of data could be make difficult. Two algorithms, RSA and AES are used for that integrated approach. Before discussing the both algorithms simple encryption and decryption should be understand. Encryption is a technique in which a plain text is converted into a secrete text with the help of special key [4]. Key may be public or private. The secrete text is called as cipher text. And in the same way decryption is a technique in which the cipher text is decoded and the original message is obtained with the help of key. There are many algorithms available for the encryption and decryption but the most efficient technique is RSA and AES by the performance and response time. AES algorithm is the advance encryption standard which was developed by Joan Deaman and Vincent Rijmen [5]. Advance Encryption Standard is famous for its speed in both hardware and software implementation. With respect to AES, probably the most powerful single- key recovery methods designed so far are impossible differential cryptanalysis [6] and Square attacks [7].The AES method can be used for the data blocks of 128, 192, 256 bits in 10 to 14 rounds [8]. The number of rounds depends upon the size of the key. It can efficiently run on the small devices. This algorithm can be implemented in different steps. First of all a block of data is encrypted and the cipher is then settled to go through the

ISSN: 2005-4270 IJDTA

number of rounds. After that the final round is executed that corresponds to cipher text output of final round steps [9].

The next technique used for the encrypting the data is RSA algorithm. This technique was developed by Ron Rivest, Adi Shamir, and Leonard Adleman in **1977.** In this technique the message sender generates a public key to encrypt the message and a private key is generated by the receiver by using the secured database [10]. The attacker can be confused by this technique because the incorrect private key can still decrypt the data but that data will be in another form i.e. that will be not original message. This is a much complex technique. After generating the public and private keys, the process of encryption is started. In both encryption and decryption methods the functions are created related to the value of public and private keys [11].

The main focus of this paper is to combine these both techniques in such a way that the cipher created by the AES is can be used as encrypted data. And here a novel approach introduced here to protect the data on the cloud in such a way that the private key that is used to decrypt the data will also be encrypted using the RSA algorithm. The next step will cover the performance comparison of all the techniques covered in this paper on the basis of different parameters and technique is named as hybrid technique.

2. ComparativeParameters

2.1 Throughput

Throughput is the amount of the work a computer can do in a given period of time. It is a measure of comparative effectiveness of large computers that run programs concurrently

2.2 Performance

Performance is denoted by theamount of useful work accomplished by a computer system or computer network compared to the time and resources used. Depending on the context efficient performance depends on the shortest response time, high throughput, low utilization of computing resources, high availability etc

2.3 Overheads

Overheads are any combination ofexcess or indirect computation time, bandwidth, memory or other resources that are required to attain a particular goal.

2.4 Response Time

The amount of time between asingle interactive user requests being entered and receiving the application's response is known as response time

3. LiteratureSurvey

The Cloud Computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure and operational expenditure. In [12] the author focuses on technical security issues arising from the usage of Cloud services and especially by the underlying technologies used to build these cross-domain Internet-connected collaborations.

Denial of service (DoS) attacks has become a major threat to current computer networks. To have a better understanding on DoS attacks, this article provides an overview on existing DoS attacks and major defence technologies in the Internet and wireless networks. In particular, we describe network based and host based DoS attack techniques to illustrate attack principles. In [13] DoS attacks are classified according to

their major attack characteristics. Current counterattack technologies are also reviewed, including major defence products in deployment and representative defence approaches in research

Cloud computing is still in its infancy in regards to its software as services (SAS), web services, utility computing and platform as services (PAS). All of these have remained individualized systems that you still need to plug into, even though these systems are heading towards full integration. In [14] authors recreate some of the current attacks that attackers may initiate as HTTP and XML. We also offer a solution to trace back through our Cloud Trace Back (CTB) to find the source of these attacks, and introduce the use of a back propagation neutral network, called Cloud Protector, which was trained to detect and filter such attack traffic. In this paper the work was done on the detection of the attack and filtering of the attacked message within the short period of time.

In recent years network security has become an important issue. Encryption has come up as a solution, and plays an important role in information security system. Many techniques are needed to protect the shared data. The present work focus on cryptography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. In [15] authors implemented three encrypt techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. Experiments results are given to analyses the effectiveness of each algorithm

In [16] paper provides an overview of current cryptanalysis research on the AES cryptographic algorithm. Discussion is provided on the impact by each technique to the strength of the algorithm in national security applications. The paper is concluded with an attempt at a forecast of the usable life of AES in these applications.

In [17] paper introduces the concept and implementation of RSA algorithm for security purpose and to enhance the performance of software system using this algorithm. In this article study has done about RSA algorithm. This study includes what is RSA algorithm and why they are used in the field of Cryptography & Network Security. After doing several works on this topic we came to conclude that RSA algorithm is important to Network Security because they are the components (i.e. Encryption & Decryption key) which interact with the Security system. Without them the system will be useless as RSA are used to fire a particular Encryption & Decryption keys process because of which Security system is build.

4.Proposed Hybrid Technique

An integrated approach is developed to secure the data on the cloud using two different techniques. As the double encryption is provided by the system, then if the attacker tries to attack on the data, then it would be difficult to decode the data for the attacker. RSA is used after AES here because there is a big advantage of RSA algorithm i.e. if the attacker decrypts the data of RSA cipher then it will give the results but that results will be different from the original data. In this hybrid technique the following steps will be performed under the hybrid algorithm.

1. Key Generation
2. Data Encryption
3. Private Key Encryption
4. Private Key Decryption
5. Data Decryption

Step1. Key Generation: It is the very simple and basic step in which key is generated i.e. Public and private key. Public key is used by sender to encrypt the data and private key is used by the receiver to decrypt the data. But to decode the data at the receiver end,

the private key is sent by the sender to receiver including the cipher text. Here the technique is providing the encryption to the private key also to make the decryption more complex and to make the data secure on cloud. In this step suppose the private key say K is generated. This key is a simple key and let it to be stored on memory for further operations.

Step2. Data Encryption: AES is the technique that is very famous for its speed and security. So to encrypt the data following steps will be performed under AES (For 128-bit block)

- From the round keys get the set of the round keys
- To perform the round keys initialize the state of array and add the initial round key to starting array.
- Perform round = 1 to 9: Execute Usual Round.
  -Sub Bytes
  -Shift Rows
  -Mix Columns
  -Add Round Key using n rounds.
- Execute Final Round.
  -Sub Bytes
  -Shift Rows
  -Add Round Key, using n (10)
- Then the Corresponding cipher text chunk output of Final Round Step

Step3. Encrypting Private Key: Private key K is generated in the first step. In this step the private key encryption will be done to make the decoding of data more difficult. RSA technique will be used to encrypt the private key. Here are the following steps

- K representing the key as integer K €{0....n-1}
- Compute C= K^emod n

Step4. Private Key Decryption: before decrypting the encrypted data, the authenticated user at receiver end should have to decrypt the private key to obtain the original data. Here the following steps are:-

- Compute K=C^d mod n

Step5. Data Decryption: The decryption technique involves the reverse all the steps that have been used in data encryption technique like inversing shift rows, inversing the sub bites , adding round keys etc. The next step involves the XO ring the output of the previous two steps with four words from key schedule. And it does not involve the "Inverse mix columns" step.

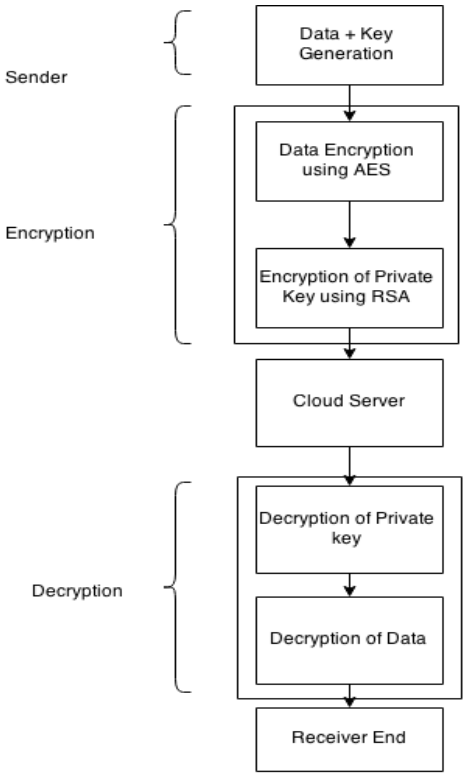

Figure 1. Architecture of Hybrid Technique

5. Experimental Results and Analysis

Experimental results for different algorithms like AES, RSA and the Hybrid technique proposed, are shown graphically and in tabular form on the basis of different parameters.

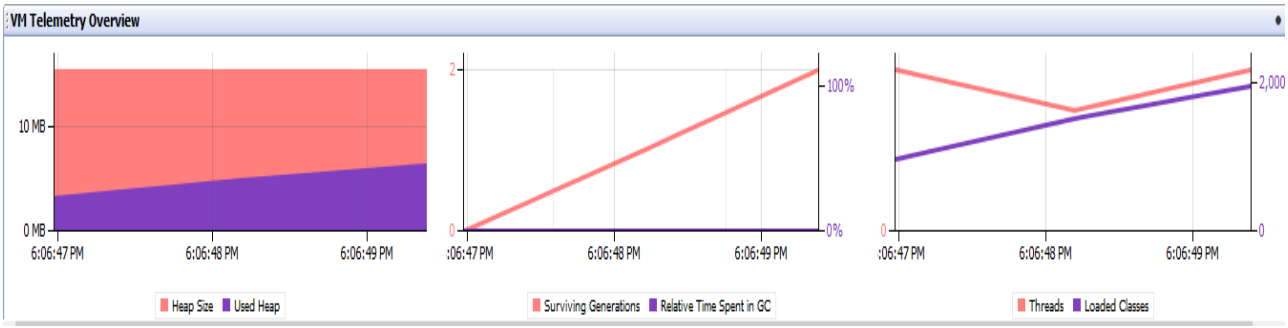

Figure 2. VM Telemetry Overview In the Form of CPU Performance in AES

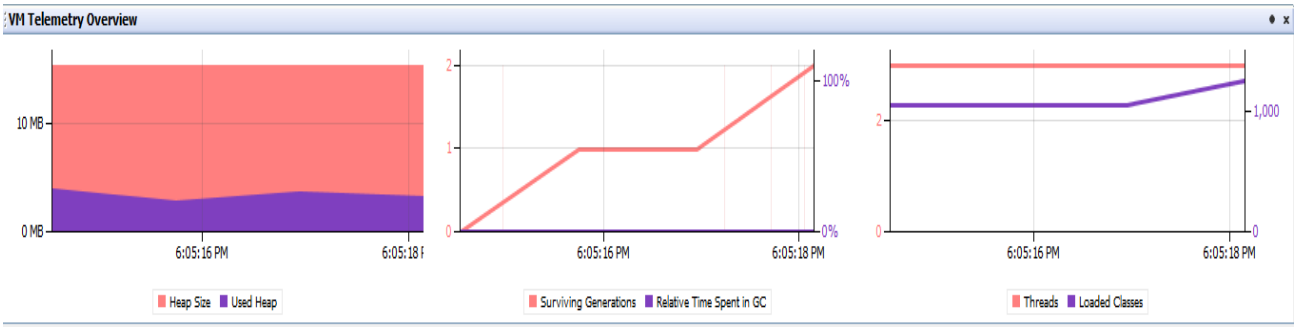

Figure 3. VM Telemetry Overview In the Form of CPU Performance in RSA

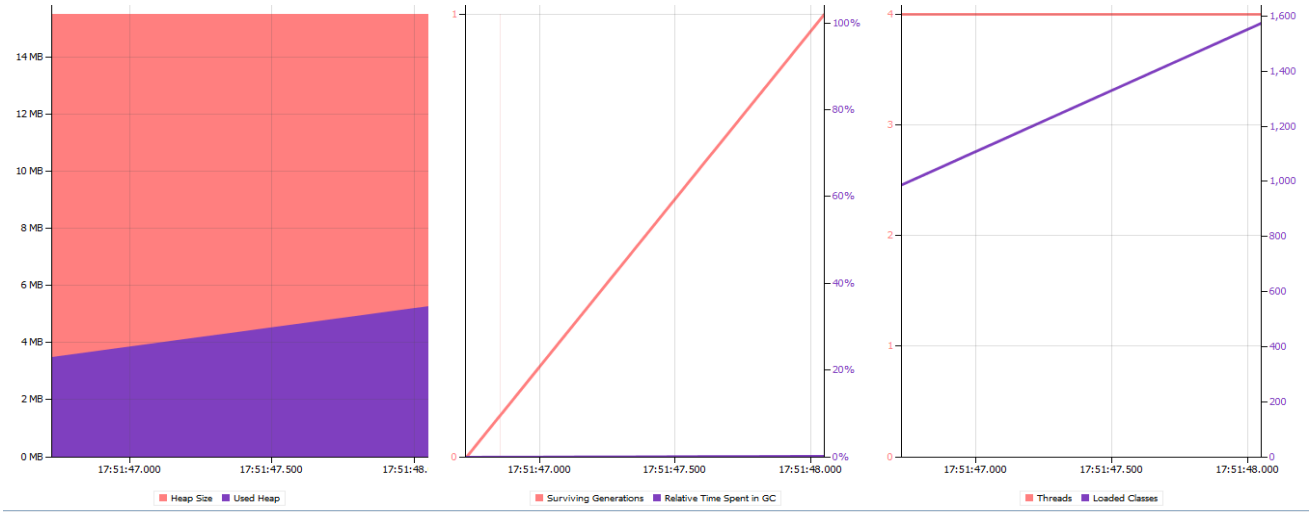

Figure 4 VM Telemetry Overview In the Form of CPU Performance in Hybrid Technique

5.1 Evaluation Parameters

There are some parameters on the basis of which the comparative analysis is done to check the performance, throughput, response time like parameters. There are some calculated values which have been used to make the evaluation graphs of different techniques by using different parameters.

Table 1. Comparison between AES, RSA and Hybrid Technique

S. No.	Data Packet Size	Algorithm	Execution Time(Sec)	Performance	Response Time(sec)
1	153	AES	1.5	High	1
		RSA	7.3	Lower	2.3
		Hybrid	8.2	Higher	0.89
2	868	AES	2.3	High	1.8
		RSA	8.3	Lower	4
		Hybrid	9	Higher	1

There is the graphical analysis of comparison between different algorithms on the basis of execution time and response time

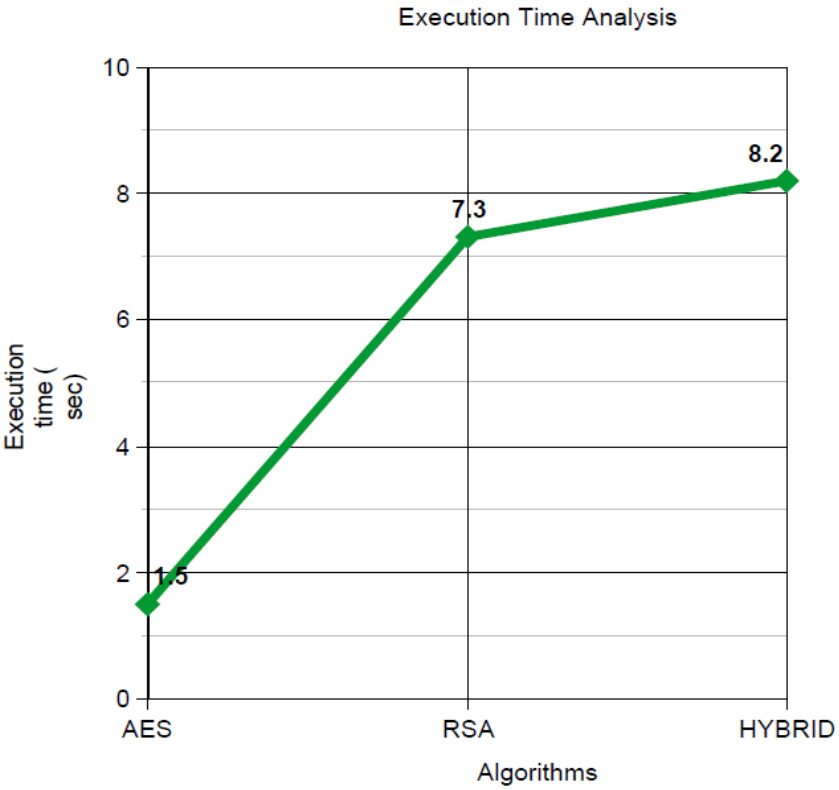

Figure5. Execution Time Analysis of Algorithms

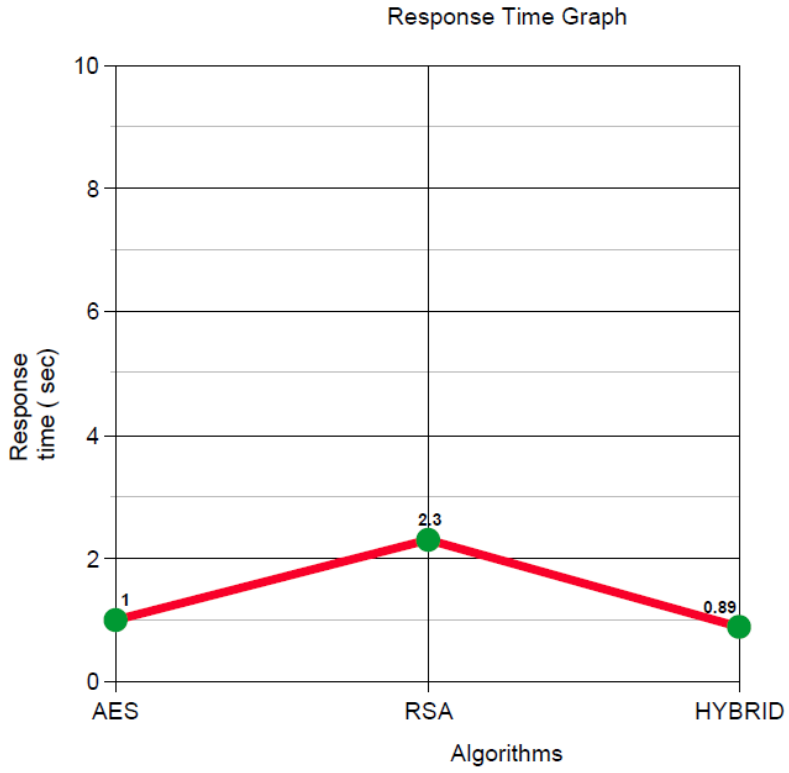

Figure 6. Response Time Graph

Simple Comparison Analysis between Above Three Techniques:-

Table 2. Simple Comparison between AES, RSA, Hybrid Technique

Attributes	**AES**	**RSA**	**HYBRID**
Developed	2000	1978	Proposed 2015
Key Size	128,192,156 bits	>1024 bits	Any key size of AES and RSA
Block Size	128 bits	512 bits minimum	Any block size same as AES or RSA
Ciphering and Deciphering	Fast	Slower	Faster
Scalability	Not Scalable	Not Scalable	Scalable
Encryption and Decryption	Moderate	Slow	Fast
Security	High	Least	Excellent
Key Used	Same	Same	Encrypted

6. Security of Cloud

Cloud computing is very famous technology. It's becoming very vast and many private and government companies owned their own clouds. In this paper a technique is proposed to prevent the data loss by much vulnerability. Very common attacks i.e. DoS attacks has been noticed on the cloud. Among all the XML attack [] is very common which can cause the decoding of data and it can change the message body. So the technique proposed here make difficult to decode the data on the cloud.

7. Conclusion

Security is very important feature for any technology. Using any technology will not be worth if it is not secure. In this paper a hybrid technique is proposed using two different techniques to provide the security to data on the higher level. This technique is beneficial in simple data transfer and storing the data on cloud. Some experimental analysis has been done on the basis of performance, execution time, response time and the CPU performance in VM telemetry view. Concluding all the different parameters the response time is low and performance of proposed technique is higher than the other two techniques and it is providing the higher security to the data. But only one drawback here is the execution time. The time taken to execute the whole process is higher than the other two techniques. But if any technology is secured then some compromises can also be done. On further discussion and more work can be done to lower the execution time.

References

[1] M. Zhou, R. Zhang, W.Xie, W. Qian& A.Zhou, "Security and privacy in cloud computing: A survey. In Semantics knowledge and grid (SKG)", 2010 sixth international conference, **(2010)**; Beijing, China.
[2] M. Zhou, R. Zhang, W.Xie, W. Qian, & A.Zhou, "Security and privacy in cloud computing: A survey. In Semantics knowledge and grid (SKG)", 2010 sixth international conference, **(2010)**; Beijing, China:IEEE.*"*
[3] Z. Muda, W. Yassin, M.N. Sulaiman, and N.I. Udzir, "Intrusion detection based on K-Means clustering and Naïve Bayes classification", 7th International Conference on Information Technology in Asia: Emerging Convergences and Singularity of Forms (CITA), 2011
[4] D.Delfs., and K. Helmut, " Introduction To Cryptography: Principles and applications", Second Edition, Springer Science & Business Media, **(2007)**; Germany.
[5] G.N.Shindeand H.S. Fade War, "Faster RSA algorithm for decryption using Chinese remainder theorem", ICCES, vol. 5, no. 4, **(2008)**, pp. 255-261.

[6] E.Biham, A. Biryukov and A. Shamir, "Miss in the middle attacks on IDEA and Khufu", *FSE'99*, volume 1636 of *Lecture Notes in Computer Science*, **(1999)**, pp. 124–138.
[7] J.Daemen, L. R. Knudsen, and V. Rijmen, "The Block Cipher Square", *FSE'97*, volume 1267 of *Lecture Notes in Computer Science*, **(1997)**, pp. 149–165.
[8] R.Pahal, V. Kumar in "Efficient Implementation of AES" Dept. ECE, SGISamalkha, Haryana, India, International Journal of Advanced Research in Computer Science and Software Engineering
[9] C.Ritika, S. Kuldeep, "Efficiency and Security of Data with Symmetric Encryption Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering,vol. 2, no. 8, **(2012)**, p. 1
[10] N. Y. Goshwe, Department of Electrical/Electronic Engineering University of Agriculture, Makurdi "Data Encryption and Decryption Using RSA Algorithm in a Network Environment" IJCSNS International Journal of Computer Science and Network Security, vol.13, no.7, **(2013)**.
[11] R.S.Jamgekar, G. Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", International Journal of Emerging Science and Engineering (IJESE), vol. 1, no. 4, **(2013)**.
[12] M. Jensen and N.Gruschka,On "Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, **(2009)**.
[13] Q.Guand P. Liu"Denial of Service Attacks", Department of Computer ScienceTexas State University; School of Information Sciences and TechnologyPennsylvania State UniversityUniversity.
[14] C. Ashle, Y. Xiang, W. Zhou and A.Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks", Journal homepage: www.elsevier.com/locate/jnca
[15] P. Mahajan & A.Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security vol. 13, no. 15,**(2013)**.
[16] A. Kaminsky[1], M. Kurdziel[2], S. Radziszowski[1], [1]Rochester Institute of Technology, Rochester, NY [2]Harris Corp., RF Communications Div., Rochester, "An Overview of Cryptanalysis Research for the Advanced Encryption Standard".
[17] P. S. Yadav, P. Sharma, K. P Yadav, "Implementation of rsa algorithm using elliptic curve algorithm for security and performance enhancement", International Journal of Scientific & Technology Research, vol. 1, no. 4, **(2012)**.

Authors

Navdeep Singh, he was born on Sept 8 1990 in Dasuya city District Hoshiarpur Punjab India. He completed his B Tech (CSE) from BCET Gurdaspur in year 2012 and Pursuing M.Tech in computer Science and Engineering GNDU Regional Campus Jalandhar, Punjab, India. Area of interest in technology is Cloud Computing, Security issues of Cloud Computing, Encryption and Decryption. Many research papers have been published of the author in the different conferences like IEEE and different Journals. He islooking forward to go for Doctorate in the same field to continue his research.