IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Data Security using RSA Algorithm in Cloud Computing

Santosh Kumar Singh[1], Dr. P.K. Manjhi[2], Dr. R.K. Tiwari[3]

Research Scholar, Department of Computer Applications, Vinoba Bhave University, Hazaribag, India [1]

Assistant Professor, University Department of mathematics, Vinoba Bhave University, Hazaribag, India [2]

Professor, HOD CSE, R.V.S College of Engg & Tech., Jamshedpur, India [3]

Abstract: Cloud computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. In today's era, it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud Computing stores the data and disseminated resources in the open environment, security has become the main obstacle which is hampering the deployment of Cloud environments. Even though the Cloud Computing is promising and efficient, there are many challenges for data security as there is no vicinity of the data for the Cloud user. To ensure the security of data, we proposed a method by implementing RSA algorithm. After implementing RSA Algorithm, we have also analyzed the performance of our algorithm based on three parameters namely Time Complexity, Space Complexity and Throughput. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required user places a request for the data to the Cloud provider, Cloud provider authenticates the user and delivers the data.

Keywords: Cloud Computing, Data Security, RSA algorithm, Encryption, Decryption, Time complexity, Space complexity, Throughput.

I. INTRODUCTION

Cloud computing is the key driving force in many small, medium and large sized companies [1-2], and as many cloud users seek the services of cloud computing, the major concern is the security of their data in the cloud. Securing data is always of vital importance and because of the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services. Every cloud service(s) seeker either an individual or a company should ask the right questions to the cloud provider before hosting their data or applications on the cloud. Prospective cloud providers should let you know; Are they financially sound? Do they have good security policies and procedures in place? Is the infrastructure meant to host your data shared with lots of other users, or will it be segregated by virtualization? As many companies move their data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures. Computer based security measures mostly capitalizes on user authorization and authentication. Cloud computing has three delivery models named as Saas, Iaas, Paas and four deployment models such as private cloud, public cloud, hybrid cloud and community cloud. As many cloud users seeks the services of cloud computing, the major concern is the security of their data in the cloud [3]. Data security is always of vital importance and plays an important role in trust worthiness of computing [4]. Due to the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important [5]. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services [6]. Security and privacy are always a major concern in cloud computing environment [7]. Some of the security issues are Privacy and Confidentiality, Data integrity, Data location and Relocation, Data Availability, Storage, Backup and Recovery [8-9].

The security of data is the prime responsibility of cloud provider. So, for efficient data security we need a mechanism that provides secure data encryption as well as secure shield against data theft. Different researches have focused on the fact that user generally has to access large volumes of data from the cloud in a secured manner. We need some algorithm that will help in efficient and speedy secured data access. In this study we do research on data security issues in cloud and provide a mechanism which ensures data security in cloud in an efficient way. Rest of the paper organized in following manner: In Section II, we are introducing the concept of RSA algorithm, Data Security Issues in the Cloud as well as related work. Detailed proposed work presented in section III. In section IV, we have presented proposed work implementation. Finally Section V concludes the paper.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

II. RSA , DATA SECURITY ISSUES IN THE CLOUD AND RELATED WORK

A. RSA (Ron Rivest, Adi Shamir and Len Adleman)

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret as shown in Fig. 1. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977.

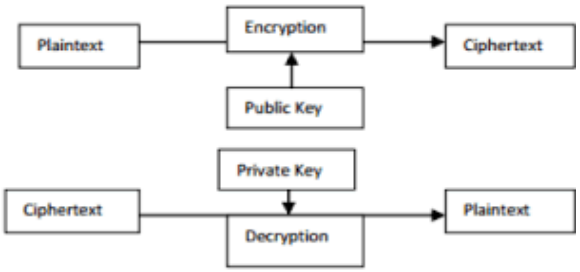

Fig. 1. Public Key Cryptosystem

In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data to the Cloud provider then Cloud provider authenticates the user and delivers the data.

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps: 1. Key Generation 2. Encryption 3 Decryption.

B. Data security issues in the cloud

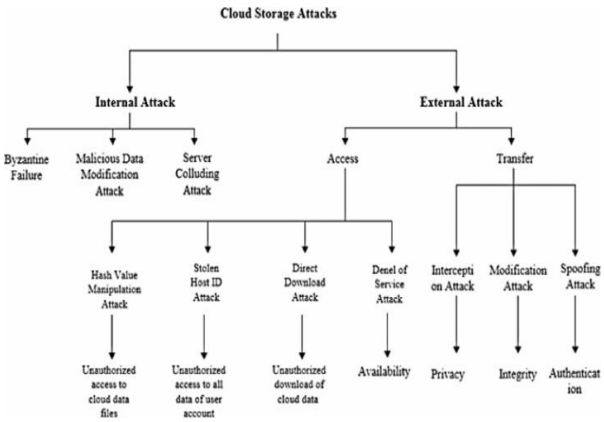

Fig. 2 Cloud Storage Attacks

Cloud storage attacks shown in Fig. 2, which raise the data security issues in the cloud, which are as follows:

Privacy and Confidentiality: Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.

Data integrity: With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place. For compliance purposes, it may be necessary to have exact records as to what data was placed in a public cloud, when it occurred, what virtual memories (VMs) and storage it resided on, and where it was processed. When such data integrity requirement exists, the origin and custody of data or information must be maintained in order to prevent tampering or to prevent the exposure of data beyond the agreed territories (either between different servers or different networks).

Data location and Relocation: Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information.

Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others' resources. Data Availability: Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult. Storage, Backup and Recovery: When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

C. Related Work

We provide some related work in the area of cloud computing security and cryptographic algorithm used in cloud computing security. Malakooti, et al [10] proposed a model which is based on the scrambling algorithm and multilevel encryptions. They have designed, implemented, and tested their security model on the image type of information that is to be stored on the cloud environment. Arockiam, et al [11] proposed technique which emphasizes on improving classical encryption techniques by integrating substitution cipher and transposition cipher. Both substitution and transposition techniques have used alphabet for cipher text. In their proposed algorithm, initially the plain text is converted into corresponding ASCII code value of each alphabet. Yang Xu, et al [12] proposed an agent-aid model by combining multi-agent system and decision-making theory toward working load balancing problem in large clouds. In their work, they put forward a novel model to balance data distribution to improve cloud computing performance in data-intensive applications, such as distributed data mining. Mohamed, et al [13] makes evaluation for selected eight modem encryption techniques namely RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish through their software to select the most suitable and the highest security encryption algorithm for secure cloud computing architecture. Tirthani, et al [14] have contemplated a design for cloud architecture which ensures secured movement of data at client and server end. They used the non-breakability of Elliptic curve cryptography for data encryption and Diffie Hellman Key Exchange mechanism for connection establishment. Their proposed encryption mechanism uses the combination of linear and elliptical cryptography methods. It has three security checkpoints named as authentication, key generation and encryption of data. Veerraju Gampala, et al [15] explores data security of cloud in cloud computing by implementing digital signature and encryption with elliptic curve cryptography. In their work authentication and encryption for secure data transmission from one cloud to other cloud is presented that requires secure and authenticated data with elliptic curve cryptography. Their proposed work contains steps like key generation, signature generation, encryption algorithm, and decryption algorithm with signature verification.

III.PROPOSED WORK

In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it [16-17]. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required user places a request for the data to the Cloud provider, Cloud provider authenticates the user and delivers the data. In proposed work, we have to implement RSA algorithm and then analyse its performance based on different parameters such as Time complexity, Space complexity and throughput. The proposed work will be carried out using Eclipse IDE with Java to get the results for different evaluation parameters. The implementation of RSA algorithm involves following steps:

- Key Generation
- Encryption
- Decryption

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only. RSA uses modular exponential for encryption and decryption. 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 n is a very large number, created during key generation process.

Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps: 1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.

2. Compute n = a * b.

3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).

4. Chose an integer e, such that $1 < e < Ø(n)$ and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.

5. Now determine d as follows: $d = e^{-1} (\text{mod } Ø(n))$ i.e., d is multiplicate inverse of e mod Ø(n).

6. d is kept as Private-Key component,

So that d * e = 1 mod Ø(n).

7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).

8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps: 1. Cloud service provider should give or transmit the Public- Key (n, e) to the user who wants to store the data with him or her.

2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.

3. Data is encrypted and the resultant cipher text (data) C is $C = m^e (\text{mod } n)$.

4. This cipher text or encrypted data is now stored with the Cloud service provider.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Decryption:
Decryption is the process of converting the cipher text (data) to the original plain text (data).
Steps: 1. the cloud user requests the Cloud service provider for the data.
2. Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data by computing, $m = C^d \pmod n$.
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

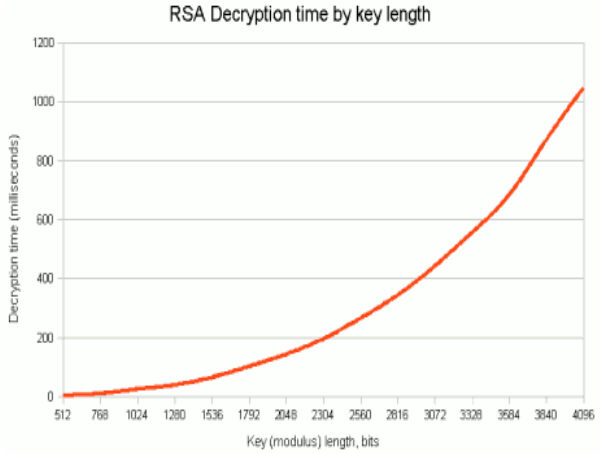

Fig. 3 RSA Decryption time by key length

If we want to increase the throughput we have to decrease the Private Key length as shown in Fig. 3.

We are taking some sample data and implementing RSA algorithm over it.

Key Generation:
1. We have chosen two distinct prime numbers a=61 and b=53.
2. Compute n=a*b, thus n=61*53 = 3233.
3. Compute Euler's totient function, Ø(n)=(a-1)*(b-1), Thus Ø(n)=(61-1)*(53-1) = 60*52 = 3120.
4. Chose any integer e, such that 1 < e < 3120 that is coprime to 3120. Here, we chose e=17.
5. Compute d, $d = e^{-1} \pmod{Ø(n)}$,
Thus $d=17^{-1} \pmod{3120} = 2753$.
6. Thus the Public-Key is (e, n) = (17, 3233) and the Private- Key is (d, n) = (2753, 3233). This Private-Key is kept secret and it is known only to the user.

Encryption:
1. The Public-Key (17, 3233) is given by the Cloud service provider to the users who wish to store the data.
2. Let us consider that the user mapped the data to an integer m=65.
3. Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user. $C = 65^{17} \pmod{3233} = 2790$.
4. This encrypted data i.e., cipher text is now stored by the Cloud service provider.

Decryption:
1. When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid).
2. The cloud user then decrypts the data by computing, $m = C^d \pmod n = 2790^{2753} \pmod{3233} = 65$.
3. Once the m value is obtained, user will get back the original data.

IV. IMPLEMENTATION

In this section we have to implement RSA algorithm and then analyse its performance based on different parameters such as Time complexity, Space complexity and through put. We will program the algorithm in Eclipse IDE with Java to get the results for different evaluation parameters and then we can use Matlab to plot the results for these parameters.

We have evaluated our algorithm on parameters such as Time complexity, Space complexity and throughput which will help us to analyse the efficiency of algorithm.

Time Complexity: Time complexity is commonly calculated by counting the total operations performed by the system where each operation takes a fixed amount of time. An algorithm performance time may vary with different input size therefore it is a common practice to express the time complexity in worst case denoted as T (n).

For instance the algorithm with T(n)=O(n) has linear time complexity whereas T(n)=O(n^2) is nonlinear and T(n)=O(2^n) is exponential. In our case we have computed the time complexity by varying the Private Key length of the RSA algorithm and finding the required execution time for each Private Key length.

The time complexity of RSA is analysed by varying the private key length in bits and noting the execution time for each key length. A summary of the different key lengths in bits and their execution time is shown in Table 1.

Table 1 Time Complexity

Private key length(bits)	Time in (ms)
64	86.00
128	91.33
256	110.33
512	142.67
1024	363.67
2048	2748.67

Space complexity: Apart from Time complexity, space complexity is also an important measure to judge the performance of an algorithm. It is the amount of memory which the algorithm needs for performing its computations.

A good algorithm keeps the amount of memory as small as possible. The way in which the amount of storage space

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

required by an algorithm varies with the size of the problem it is solving. Space complexity is normally expressed as an order of magnitude, e.g. O(N^2) means that if the size of the problem (n) doubles then four times as much working storage will be needed.

We have analysed the space complexity between private key length which is in bits and run time memory consumed by system. A summary of the different Private Key length in bits and run time memory taken by the system is given below in table 2.

Table 2. Space Complexity

Private Key Length (Bits)	Run Time Memory
128	345128
256	347224
512	347320
1024	348040
2048	348608
4096	349488
8192	351048

Throughput: In communication systems throughput is the rate of successful data delivery over a noisy communication channel. Throughput is usually measured in bits per second and sometimes we measure it in terms of packets per second.

We have calculated the throughput of the algorithm by dividing the total data in bytes by encryption time. Higher the throughput higher is the efficiency of the system.

Table given below gives us the comparison between the throughput and the message signal. We have calculated the throughput for 32, 64,128 and 256 bytes of messages. In any cryptographic algorithm, it is essential to understand the size of the input and the size of output as this is one of the important property of an avalanche effect.

Larger the size of the Cipher text compared with the Plaintext, more secure is the Cipher text against any Brute-Force attack. The table 3 below gives us the throughput for different data length.

Table 3: Throughput

	Throughput for different Private Key Length				
Data Bits	128 bits key length	256 bits key length	512 bits key length	1024 bits key length	2048 bits key length
32	205.13	186.04	136.75	102.56	48.854
64	457.14	372.09	256	205.13	71.99
128	914.28	684.49	514.056	315.27	182.33
256	1641.02	1361.70	1094.02	684.49	443.67

When we analyse the data from the above table we see that there is a tradeoff between through put and Private Key length. If we want to increase the throughput we have to decrease the Private Key length

V. CONCLUSION

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.
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 if he captures the data also, he can't decrypt it and get back the original data from it. We have evaluated its performance based on different parameters such as space complexity, time complexity and throughput. We have observed each efficiency parameter in detail by varying message packet length and private key length of our encryption scheme. By studying the obtained results we can say that RSA encryption algorithm is a feasible solution for secure communication in cloud computing.

REFERENCES

[1] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for Cloud Computing". The University of Texas at Dallas, USA, International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.
[2] Anup R. Nimje, "Cryptography in Cloud-Security Using DNA (Genetic) Techniques", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue5, pp.1358-1359, Sept- Oct2012.
[3] Engr: Farhan Bashir Shaikh, Sajjad Haider, "Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, 11-14 December 2011
[4] Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, www.ijera.com, Vol. 3, Issue 4, pp.1922-1926, Jul-Aug 2013.
[5] Danish Jamil, Hassan Zaki, "Cloud Computing Security", International Journal of Engineering Science and Technology IJEST, ISSN: 0975-5462, Vol. 3 No. 4, pp. 2672-2676, April2011.
[6] Dr. P. Dinadayalan, S. Jegadeeswari, Dr. D. Gnanambigai, "Data Security Issues in Cloud Environment and Solutions", World Congress on Computing and Communication Technologies 2014.
[7] Natan Abolafya, Secure Documents Sharing System for Cloud Environments, Master of Science Thesis Stockholm, Sweden 2012.
[8] Abdullah Al Hasib, Abul Ahsan Md. Mahmudul Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography", Third International Conference on Convergence and Hybrid Information Technology, 2008.
[9] Cloud Security Alliance, (2009) Security Guidance for Critical Area of Focus in Cloud Computing V2.1. [Online]. Available: https://cloudsecurityalliance.org/csaguide.pdf, accessed on Feb 2012.
[10] Dr. Mohammad V. Malakooti, Nilofar Mansourzadeh, "A Robust Information Security Model for Cloud Computing Based on the Scrambling Algorithm and Multi-Level Encryption", Proceedings of the International conference on Computing Technology and Information Management, Dubai, UAE, 2014, Islamic Azad University, UAE branch, Dubai, UAE.
[11] Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.
[12] Yang Xu, Lei Wu, Liying Guo, Zheng Chen, Lai Yang, Zhongzhi Shi, "An Intelligent Load Balancing Algorithm Towards Efficient

Cloud Computing", AI for Data Center Management and Cloud Computing: Papers from the 2011 AAAI Workshop (WS-11-08).

[13] Eman M.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby, "Enhanced Data Security Model for Cloud Computing", the 8th International Conference on Informatics and Systems (INFOS2012) 16 May, Cloud and Mobile Computing Track.

[14] Neha Tirthani, Ganesan R, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography", School of computing Science and Engineering, VIT, Chennai campus.

[15] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[16] Li Dongjiang, Wang Yandan, Chen Hong, "The research on key generation in RSA public- key cryptosystem", Department of Computer Science, North China Electric Power University, Beijing, China, Fourth International Conference on Computational and Information Sciences 2012.

[17] Ahmed E. Youssef, Manal Alageel, "A Framework for Secure Cloud Computing", Dept. of Information Systems, King Saud University, Riyadh, 11543, KSA.

BIOGRAPHY

Santosh Kumar Singh is a Research Scholar in the Department of Computer Applications, Vinoba Bhave University, Hazaribag, Jharkhand, India. He received M. Phil (Computer Science) degree in 2011 and Master of Philosophy Dissertation entitled "study on the network security & network topology". He Qualified Doctoral (Ph.D) Eligibility Test 2014 of Vinoba Bhave University, Hazaribag. His research interests are Cloud Computing, Parallel and Distributed Computing etc. He is currently working on Cloud Computing Security.