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 5, May 2015

Designing of Hybrid RSA Encryption Algorithm for Cloud Security

Dr. Nandita Sengupta

Assistant Professor, Dept. of I.T., University College of Bahrain, Manama, Kingdom of Bahrain

ABSTRACT: Cloud system is providing many facilities to the users by providing Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS). Cloud system involves transferring data from client to server, server to client and processing, storage data in server. As a result of which, data needs to be protected while transferring through the network and in the server. Cloud system is an emerging technology in which security is the most challenging issue. RSA encryption algorithm is a very old encryption algorithm which may fail in maintaining security level of data in transit if the value of public key is achieved by the attacker. This paper suggests hybrid RSA encryption algorithm which makes the data difficult to decrypt for the attacker. Man in the middle attack will be minimized by applying this proposed hybrid RSA encryption algorithm for data transfer in cloud system.

KEYWORDS: Hybrid RSA algorithm; cloud security; encryption; decryption; Man-in-the-Middle Attack

I. INTRODUCTION

Distributed resources are provided by cloud provider but only disadvantage is the security threat in cloud. A few years before, hard disk, external hard disk, memory sticks were the only storage device for data or documents. In present scenario, internet based platform is providing the facility to store data or documents in remote server which is provided by cloud service providers, like Google, Microsoft, IBM etc. People can access, process, modify those resources whenever then need. Cloud computing [1–6] has become popular in almost all business sectors, like education, healthcare, government, finance. Even though so many advantages are provided by the cloud service providers, security is the major challenging issue in it. NIST defined four different types of cloud, private cloud, public cloud, hybrid cloud and community cloud considering deployment models of cloud. Each of these cloud system requires a robust mechanism for maintain security.

NIST listed a few objectives, like accountability, assurance, authentication, authorization, availability, confidentiality, integrity, non-repudiation for maintaining security in software system. Confidentiality can be maintained by applying a complex encryption algorithm even in public cloud, hybrid cloud for IaaS, PaaS and SaaS.

RSA encryption algorithm is one of the oldest and efficient public key algorithms which is used for encrypting data. But it has limitations in degree of security and time of computation. Proposed algorithm eliminates the first limitation, i.e., provides more security without affecting computation time much.

This paper has 7 sections in addition to introduction, reference and biography sections. Section 2 describes related work in the same subject whereas section 3 depicts RSA Public key Algorithm, section 4 explains Feistel algorithm, proposed hybrid RSA encryption is defined in section 5, section 6expresses analysis and results, section 7 concludes the paper with future work.

II. RELATED WORK

In [7]Rachna Arora et. al. discussed various security issues, mechanism and challenges of cloud computing. Authors of paper [8] presented cipher cloud where they showed 5 layers of security measurement for encrypting data for cloud. Before sending the data through media, data will be encrypted and data will remain stored in server as encrypted. In paper [9], an efficient implementation of RSA algorithm has been shown. Authors have used two public key pairs and the value of e will be calculated using some mathematical logic. They mentioned that there is no need to send the value of e directly. So, even the value of e is protected from the attack. While users need those data for their use, same will be

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 5, May 2015

decrypted after downloading. Authors of paper [10] provided security for three aspects, of security confidentiality, Integrity and authentication of data storage in the cloud. MD5 algorithmis proposed for integrity of the data. Confidentialitywill be maintained by providing Blowfish algorithm. RSA algorithmtakes care about the authentication. In paper [12], authors proposed public key cryptosystem RSA for providing security of data for cloud system. Authors of paper [13] proposed an improved RSA encryption algorithm for cloud security. In comparison to original RSA model, the number of key generation exponents has been increased.In paper [14], Hybrid Encryption algorithm(HE-RSA) has been proposed which is based on RSA Small-eand Efficient RSA. Authors mentioned that the reliability in cloud computing environments will be improved by using HE-RSA. This algorithm provides more security than RSA as dual encryption process has been applied. Authors have shown comparison between original RSA and HE-RSA for key generation, encryption and decryption time.

III. RSA ALGORITHM

In 1977, three scientists, Ron Rivest, Adi Shamir, and Len Adleman, developed RSA algorithm at MIT. RSA algorithm [15] has been named based on these three scientists. RSA applies public key approach for encryption. The two keys, the public key and the private key, are required for asymmetric public key encryption. Suppose the sender Alice wants to send message to the receiver Bob, then Bob has to generate a pair of keys, public key (PU_K) and private key (PR_K). Alice forms the cipher text (CT) based on the input of plain text (PT) and public key (PU_K). Plain text gets converted into decimal strings, block of numbers, PT_1,PT_2,..Eq (1) represents that cipher text is derived from the encryption function which works on those two inputs.

$$CT_1 = E(PU_K , PT_1) \quad \text{eq. (1)}$$

At the receiving end, Bob gets the Plain text (PT_1) back by decrypting the cipher text with the help of decrypting key which is private key (PR_K). Eq. (2) represents that plain text is derived from decryption function which needs two inputs, cipher text and private key.

$$PT_1 = D(PR_K, CT_1) \quad \text{eq. (2)}$$

Both plain text and cipher text are integers in RSA scheme and these integers are in between 0 and n-1 for some value of n. Encryption and decryption are expressed by using following equations, eq. (3) and eq. (4) respectively for RSA algorithm.

$$CT_1 = (PT_1)^e \bmod n \quad \text{eq. (3)}$$

$$PT_1 = (CT_1)^d \bmod n \quad \text{eq. (4)}$$

Alice, the sender, knows the value of e and n so that plain text (PT_1) can be encrypted to cipher text (CT_1). But only the receiver, Bob, knows the value of d and n so that cipher text (CT_1) can be decrypted by Bob to plain text (PT_1). Here, the public key is defined as $PU_K = \{e,n\}$ and private key is defined as $PR_K = \{d,n\}$. Key generation algorithm for RSA scheme is as follows

1. Select two prime numbers, s and t
2. Calculate n = st
3. Calculate $\varphi(n) = (s-1)(t-1)$
4. The value of e is selected in such a way that e is relatively prime to $\varphi(n)$ and less than $\varphi(n)$
5. Determine d such that de mod $(\varphi(n)) = 1$ and $d < \varphi(n)$

With the help of the algorithm, keys are generated, public key, $PU_K = \{e,n\}$ and private key, $PR_K = \{d,n\}$. Detailed RSA algorithm is shown in Fig. 1.

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 5, May 2015

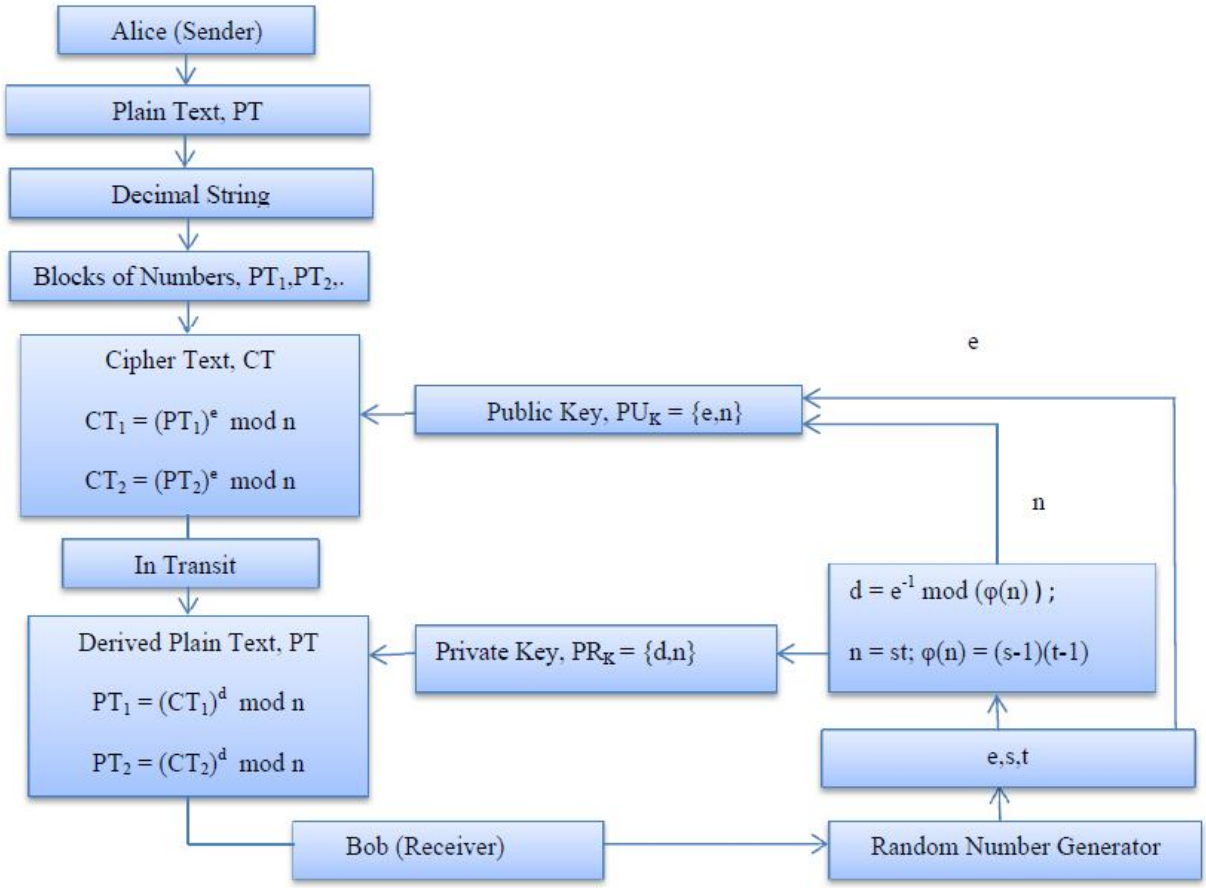

Fig.1. RSA Encryption Decryption

IV. FEISTEL CIPHERALGORITHM

A plaintext block of X length bits and a key K are considered as inputs of Feistel encryption algorithm [15]. The plaintext data is divided into two halves (X/2), and data is passed through n numbers of rounds of processing. After all the rounds, resultant data is combined to form cipher text. Each right half of data along with a key, different for each round, are used as an input of a function. Output of the function is considered as an input of xor operation to form the right half data for next round. Another input of xor operation is taken from left half of the data from previous round. Number of rounds can be different for implementation of the algorithm and this number is considered as a high number for effective implementation of the algorithm. Assume, data length is of X bits and it is divided into two halves. At i-th round, right half data is denoted as RHD_i and left half data is denoted as LHD_i. Where at starting, the value of i is 0. F function is applied on two inputs, RHD_i and K_i. Exclusive OR is applied on the output of F function and LHD_i to substitute the left hand half data for (i+1)-th round. Finally, (i+1)-th round left hand half data and right hand half data are formed by permutation, i.e. interchanging both the halves data immediately after substitution. Eq. (5) and eq. (6) represents (i+1)-th left hand half data and right hand half data respectively.

$$LHD_{i+1} = RHD_i \quad \text{eq. (5)}$$

$$RHD_{i+1} = EXOR\ (LHD_i\ ,\ F(RHD_i\ ,\ K_i)) \quad \text{eq. (6)}$$

The decryption process of Feistel algorithm works in the same way as opposite to the encryption algorithm. Keys work in reverse direction The whole encryption and decryption process is explained in Fig. 2a and Fig. 2b respectively where only 16 rounds are shown.

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 5, May 2015

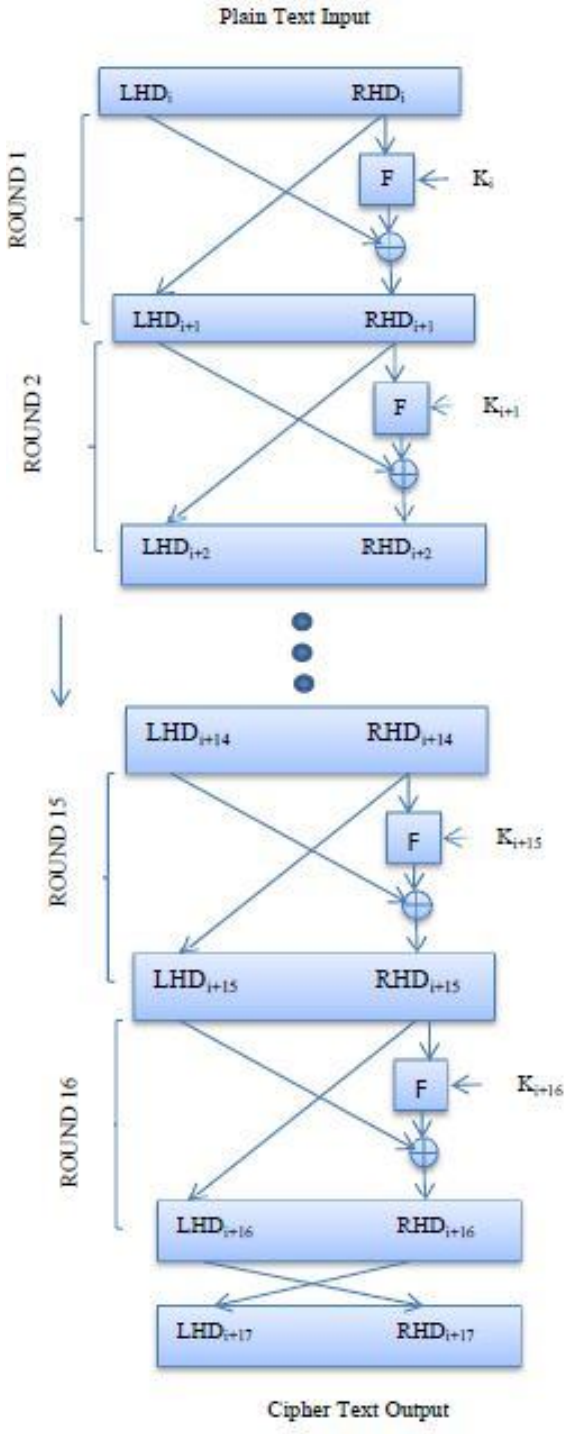

Fig.2a. Feistel Encryption Algorithm

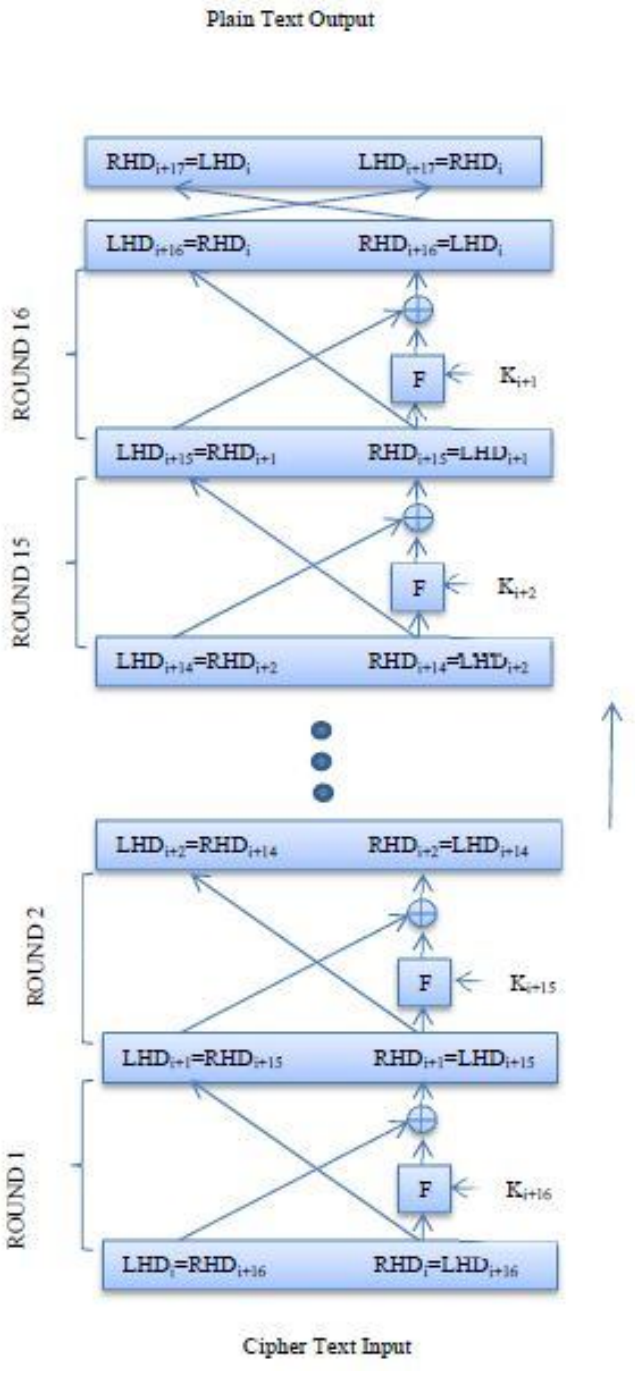

Fig.2b. Feistel Decryption Algorithm

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 5, May 2015

V. PROPOSED ALGORITHM

Hybrid RSA encryption algorithm is proposed in the paper for security of data in cloud system. In the first phase RSA Encryption algorithm will be applied and in the second phase Feistel encryption algorithm will be applied on the output data, i.e., cipher text of first phase. After final phase, encrypted data will be sent for transmission. As the proposed algorithm has two phases, probability of man-in-the-middle attack will be less. Encryption and decryption processes of the hybrid algorithm are shown in Fig. 3a and Fig.3b respectively.

Fig.3a. Hybrid RSA Encryption Algorithm Fig.3b. Hybrid RSA DecryptionAlgorithm

A. *Design Considerations:*

- Assume two prime numbers, s and t.
- The value of e should be selected maintaining some criterion to form public key for RSA Algorithm.
- The value of d should be determined maintaining some criterion.
- The number of rounds,m, should be considered for Feistel Encryption Algorithm.
- The value of key, K, should be chosen for Feistel Encryption Algorithm.

B. *Description of the Proposed Algorithm:*

Step 1: Select two prime numbers, s and t.
Step 2: Calculate n = st.
Step 3: Calculate $\varphi(n) = (s-1)(t-1)$.
Step 4: The value of e is selected in such a way that e is relatively prime to $\varphi(n)$ and less than $\varphi(n)$.
Step 5: Determine d such that $de \bmod (\varphi(n)) = 1$ and $d < \varphi(n)$.
Step 6: Keys are generated, public key, $PU_K = \{e,n\}$ and private key, $PR_K = \{d,n\}$.
Step 7: Encrypt plain text to first phase cipher text, $CT_{11} = E(PU_K , PT_{11})$
Step 7: Cipher text, CT_{11} is divided in two halves, LHD_i and RHD_i.
Step 8: $LHD_{i+1} = RHD_i$.
Step 9: Calculate $RHD_{i+1} = EXOR (LHD_i , F(RHD_i , K_i))$.
Step 10: The value of m is reduced by 1 and i = i+1.
Step 11: Repeat step 7 to step 10 till the value of m becomes 0.
Step 12: End of Hybrid encryption.

Output of this hybrid encryption algorithm is CT_{12}, cipher text, derived by two phases of encryption.

VI. ANALYSIS AND RESULTS

For doing the analysis, online software for RSA key generation [16] has been used for Phase 1. Results of RSA algorithm has been shown below.

Phase 1:

Plaintext:

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 5, May 2015

==========
The quick brown fox jumps over the lazy dog

Message: m
========== hex ====
7d0aef4913c19205f54904fc9439f84908f9a0c2f49e007a9bc2f99f07fc4916f28dc2f68a1cc54906f98fafff

Ciphertext: c = m^e mod n
========== dec ====
427101866301864286400748270672579576915353502845703756101941448079858976935357375870045567757
401879557673746794225222385212588971630898795757737775937185098540508371247232855702411867843
434783546714091123955935354722973034702358724579748797660389084613734345608925026845044706459
057229760553803565019296303683597240144650196946528576022589550207488764314461409610589620998
757150898326010108184814822674885474807841803707759747446205397449788948082831198932080542676
136032647191676933588455159388290907579975500802342374901962434505969769886155121574110737246
774543042841443988275969319872720216644615766182982988547 6

Phase 2: This cipher text from RSA algorithm has been considered as input data for Feistel algorithm and decrypted message has been found by using online tool [17] for Feistel algorithm. Final encrypted message, achieved from hybrid RSA algorithm is depicted inFig. 4.

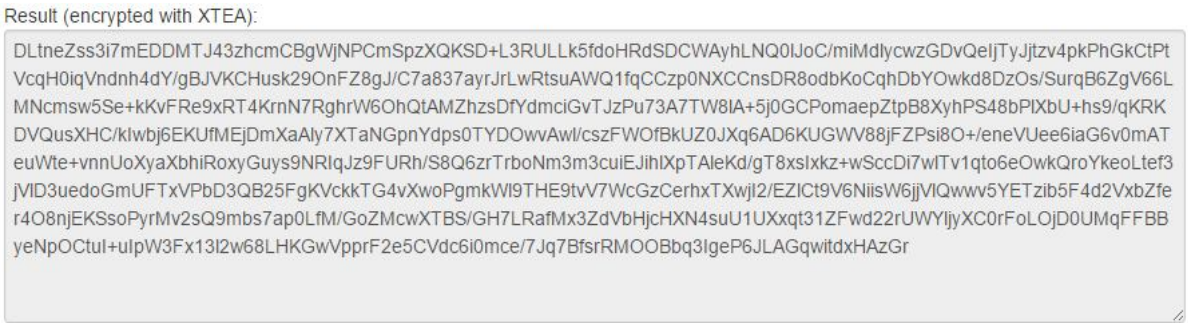

Fig.4.Final Cipher Text of Hybrid RSA Algorithm

VII. CONCLUSION AND FUTURE WORK

The analyzed results show the complexity of the hybrid algorithm which includes 2 phased encryption. As a result, if the attacker wants to get the information by decrypting the final encrypted message, will be difficult to get the correct plain text message. Only applying RSA algorithm, encrypted data for cloud does not maintain a high security level. As the value of public key is shared, i.e., the value of e is known, there is high possibility of determining the value of d and decrypt the encrypted data. So, proposed hybrid RSA encryption technique provides higher level of security than only RSA algorithm. Encryption of data for IaaS will secure the data from confidentiality but to maintain integrity of data in cloud, Secure protocol (like FTP with SSL, HTTPS, Secure Copy Program) transactions are required. Future work includes designing of such hybrid encryption which ensures data transmission through secured protocol.

REFERENCES

1. Sengupta, N. andHolmes, J.“Designing of Cryptography Based Security System for Cloud Computing”, Proceedings of CUBE 2013, IEEE, Pune, India,15th-16th November 2013.
2. Xiong, J., Liu, X., Yao, Z., Ma, J., Li, Q., Geng, K.,and Chen, S. P., “A Secure Data Self-Destructing Scheme in Cloud Computing”, IEEE Transactions on Cloud Computing, vol.2, no.4, pp.448,458, 2014.
3. Jamshidi, P., Ahmad, A.,and Pahl, C. P., “Cloud Migration Research: A Systematic Review”, IEEE Transactions on Cloud Computing, vol.1, no.2, pp.142,157, July-December 2013.

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 5, May 2015

4. Ficco, M.,and Rak, M., "Stealthy Denial of Service Strategy in Cloud Computing", IEEE Transactions on Cloud Computing, vol.3, no.1, pp.80,94, Jan.-March, 2015.
5. Zhang, Y., Liao, X., Jin, H.,and Min, G.,"Resisting Skew-Accumulation for Time-Stepped Applications in the Cloud via Exploiting Parallelism", IEEE Transactions on Cloud Computing, vol.3, no.1, pp.54,65, Jan.-March, 2015.
6. Chen, A. C., Won, M., Stoleru, R., Xie, G.G.,"Energy-Efficient Fault-Tolerant Data Storage and Processing in Mobile Cloud", IEEE Transactions on Cloud Computing, vol.3, no.1, pp.28,41, Jan.-March, 2015.
7. Arora,R.,Parashar,A.,"Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 3, Issue 4, pp.1922-1926, Jul-Aug 2013.
8. Kaur,M., Singh,R., "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing",International Journal of Computer Applications, Volume 70, No.18, May 2013.
9. Ayele,A. A., Sreenivasarao, V., "A Modified RSA Encryption Technique Basedon Multiple public keys", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2013.
10. Galli,H.,Padmanabham, P.,"Data Security in Cloud using Hybrid Encryption and Decryption", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 10, October 2013.
11. Dubey, A.K., Dubey, A.K., Namdev, M., and Shrivastava, S.S., "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment", Proceedings of 2012 CSI Sixth International Conference onSoftware Engineering (CONSEG), IEEE, 5-7 Sept. 2012.
12. Yellamma,P.,Narasimham,C., and Sreenivas,V., "Data security in cloud using RSA", Proceedings of 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 4-6 July 2013.
13. Saggar, S.,Datta, R., "An improved RSA Encryption Algorithm for Cloud Computing Environments: Two key Generation Encryption (2KGEA)", International Journal of Software and Web Sciences (IJSWS), 2013.
14. Moghaddam, F., Alrashdan, M.,and Karimi, O.,"A Hybrid Encryption Algorithm Based on RSA Small-eand Efficient-RSA for Cloud Computing Environments", Journal of Advances in Computer Network, Vol. 1, No. 3, September 2013.
15. Stallings, W.,"Cryptography and Network Security Principles and Practice", Prentice Hall.
16. Online free software for RSA key generation, http://www.mobilefish.com/services/rsa_key_generation/rsa_key_generation.php.
17. Online free software for Feistel encryption and decryption, http://www.tools4noobs.com/online_tools/xtea_decrypt/.

BIOGRAPHY

Dr. Nandita Sengupta(ngupta@ucb.edu.bh) has done her Bachelor of Engineering from IIEST formerly known as Bengal Engineering College,Shibpur,Calcutta University. She completed Post Graduate Course of Management in Information Technology from IMT. Later on she passed M Tech (Information Technology) from IIEST. She completed her PhD in Engineering (Computer Science and Technology) from IIEST. She has 25 years of working experience. 11 years she dedicated in industry. Last 14 years she is in academics and taught various subjects of IT. Presently she is working as Assistant Professor in University College of Bahrain, Bahrain. Her area of interest is Analysis of Algorithm, Theory of Computation, Soft Computing Techniques, Network Computing. She achieved "Amity Best Young Faulty Award" on the occasion of 9th International Business Horizon INBUSH 2007 by Amity International Business School,Noida in February,2007. She has around 25 publications in National and International conference and journals.