IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Optimizing Fully Homomorphic Encryption Algorithm using RSA and Diffie- Hellman Approach in Cloud Computing

Aparna Negi[1*], Anshika Goyal[2]

[1]Computer Science & Engineering, Faculty of Technology, Uttarakhand Technical University, Dehradun, India
[2]Computer Science & Engineering, Faculty of Technology, Uttarakhand Technical University, Dehradun, India

[*]*Corresponding Author: Aparnanegi8@gmail.com, Tel.:7251985575*

Available online at: www.ijcseonline.org

Accepted: 16/May/2018, Published: 31/May/2018

Abstract- Cloud computing is a technology where user can store their data and any application software on it. With the use of this technology user need not to worry about the cost of hardware installation and their maintenance cost. Hence, the cloud computing security becomes the current research focus. To secure the cloud data, Encryption Scheme is used. Different encryption techniques used for security purpose like Fully Disk Encryption and Fully Homomorphic Encryption. FDE encrypts the entire disk and FHE encrypts the particular functions. FHE is used to secure the cloud data from exploitation during the computation. In this research paper, FHE encryption scheme is optimized in which the Encryption Time, Probability of Attacks and Space Used by encrypted data is reduced using RSA and Diffie- Hellman Algorithm. RSA Algorithm is applied to improve performance of FHE schemes. The Diffie- Hellman algorithm is also applied for the secure channel establishment in the fully homomorphic encryption It has been analyzed that RSA algorithm based FHE performs well as compared to Diffie- Hellman algorithm.

Keywords-Cloud Computing, Diffie Hellman Algorithm, RSA Algorithm, Fully Homomorphic Encryption, Security

I. INTRODUCTION

Cloud Computing:
Cloud Computing is the environment which provides on-demand & convenient access of the network to a computing resources like storage, servers, applications, networks and the other services which can be released minimum efficiency way. Cloud is a design, where cloud service provider provides services to user on demand and it is also known as CSP stands for "Cloud Service Provider". It is a technique which gives a huge amount of applications under different-different topologies and each topology gives some new specialized services [20].

Service Models in Cloud Computing:
a) Software as a Service (SaaS): This is the capability of using applications which are running on cloud infrastructure. The users access these applications through internet connections.
b) Platform as a Service (PaaS): It gives the computational resources on which services and applications can be host and develop.
c) Infrastructure as a Service (IaaS): This is the capability of doing processing, storing and run software which is given to the consumer.

Deployment models of Cloud
a) Public Cloud: In this cloud, resources allocated are publically. Applications in this cloud are on pay-per-use basis. Public clouds can be managed by government organizations or business.

b) Private Cloud: In this cloud, resources are limited and used within an organization. It is more secure as employees in an organization can access the particular data only.

c) Hybrid Cloud: In this cloud, there is a combination of both Public and Private cloud. The services within the organization are control by the customer and resources which need to be delivered externally are controlled by the service provider.

d) Community Cloud: This cloud is used by those organizations which have same concerns like security requirements; mission or policy. This is managed by organizations within a community or by the third party auditor.

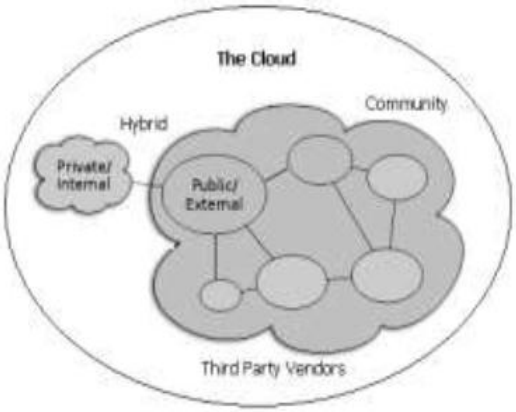

Fig.1 Deployment Model of Cloud

As a last paragraph of the introduction should provide organization of the paper/article (Rest of the paper is organized as follows, Section I contains the introduction of Cloud computing and its services and Deployment models. Section II contain the related work and brief description of research papers, Section III explain the methodology of research work with flow chart, Section VI describes results and discussions of all the experiment and results of experiment done in research work, and Section V concludes the research work with future directions and covers the complete thesis).

II. RELATED WORK

Geethu Thomas et al.(2010) in their paper titled on "Cloud Computing security using Encryption Technique" In this paper they presented that the cloud computing is very efficient technology or important field used for data storage due to its efficiency and flexibility.

Sean Carlin et al.(2011) in their paper titled on "Cloud Computing Security" In this paper cloud computing is the distributed architecture that centralizes the resources of server on a scalable platform which provides services on demand. Various cloud deployment models are discussed i.e. public, private and hybrid. The main security issues and risks are discussed; sharing of resources is one of them.

Dawn Song et al.(2012)in their paper titled on "Cloud Data Protection for the Masses" proposed that the data-protection-as-a-service where different services are provided for protecting data. Two techniques have discussed i.e. FDE (Full Disk Encryption) and FHE (Fully Homomorphic Encryption). There is a comparison in these techniques on the basis of key management, sharing, and ease of development, maintenance, aggregation and performance.

Deyan Chen et al.(2012) in their paper titled on" Data Security and Privacy Protection Issues in Cloud Computing" In this paper it describes data security and privacy protection issues occurred in cloud computing in all the stages of data life cycle. There are seven stages of data lifecycle: Generation, use, transfer, share, storage, archival, destruction. They have discussed some current solutions like fully homomorphic technique, data integrity, client-based privacy management tool, etc.

Dr Nashaat el-Khameesy et al.(2012) in their paper titled on "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" In this paper suggests a methodical application of "defence in depth" security technique that can help all security risks in networked storage. More important is defence in depth based networked storage security policy provides a comprehensive framework to toward future attacks as the current technologies are more clearly understood.

Simarjeet Kaur(2012) in their paper titled on "Cryptography and Encryption In Cloud Computing" proposed that the various data encryption schemes like homomorphic encryption, searchable and structured encryption, Identity based encryption, signature based encryption etc. are discussed.

Anjana Chaudhary et al.(2014) in their paper titled on "Security in Cloud Computing by using Homomorphic Encryption Scheme with Diffie-Hellman Algorithm" stated that the secure channel should be established two users to transfer the data. Only authorized users can encrypt or decrypt the data. For encryption and decryption of data, basic homomorphic encryption scheme is used along with Diffie-Hellman algorithm.

Peidong Sha et al.(2016) in their paper titled on "The Modification of RSA algorithm to Adapt Fully Homomorphic Encryption Algorithm in Cloud Computing" proposed that the RSA is partially homomorphic cryptosystem, based on the features of the RSA algorithm, we design a encryption system, this encryption system firstly discriminates whether the values of the public key and private key generated during the encryption process contain prime number, then combines with the Pascal's triangle theorem and RSA algorithm model and inductive methods to construct a new cryptosystem that meets homomorphic computation of some operations on cipher texts. Thus the new cryptosystem satisfies fully homomorphic encryption in cloud computing.

III. METHODOLOGY

In this section, all the functions for the coding are written in the MATLAB. Several inbuilt functions of MATLAB are used for the implementation of different steps of the algorithm. First we will establish a path between the User node to Cloud node. The image file containing the secret plain text that will be encrypted to cipher text using RSA and Diffie-Hellman algorithm.

Parameters used to analyze performance

1. Execution Time : The execution time is the time which is taken to execute the algorithm.

Execution time = End of clock- start of clock

2. Probability of attacks :- The probability of attack is the probability value of the attacks.

Probability = no. of vulnerabilities in the algorithm

3. Space Used :- The space utilization is the parameter which count number of buffers used by the algorithm.

Space used = time* buffer used per unit time

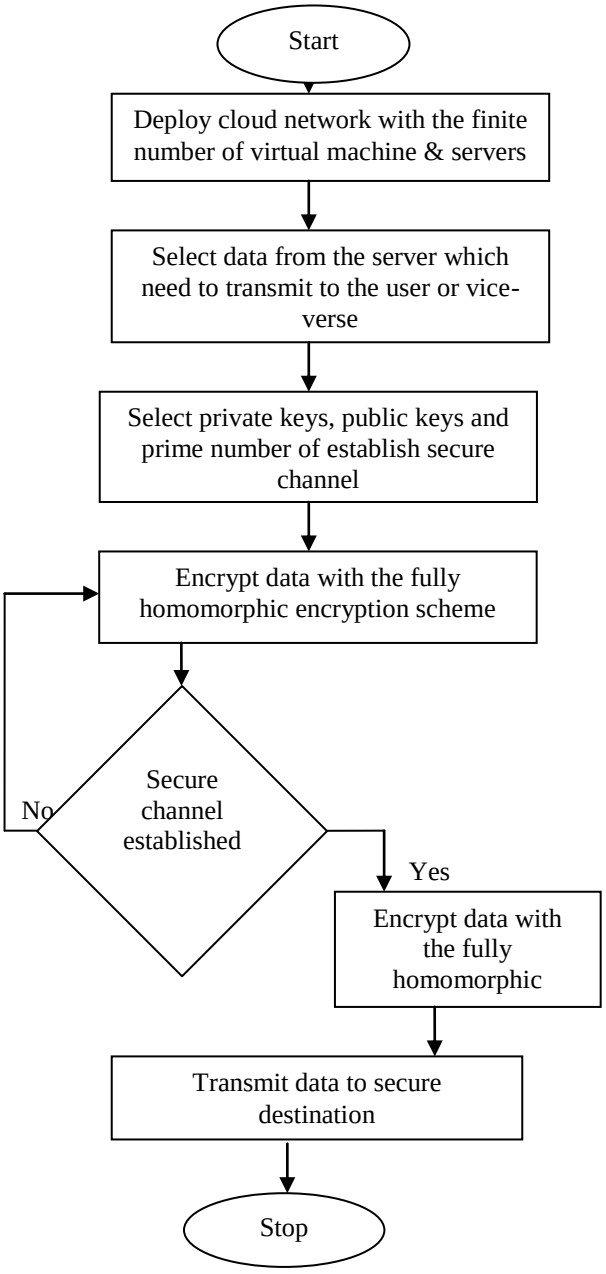

Fig.2 Flow Chart of RSA Algorithm in FHE

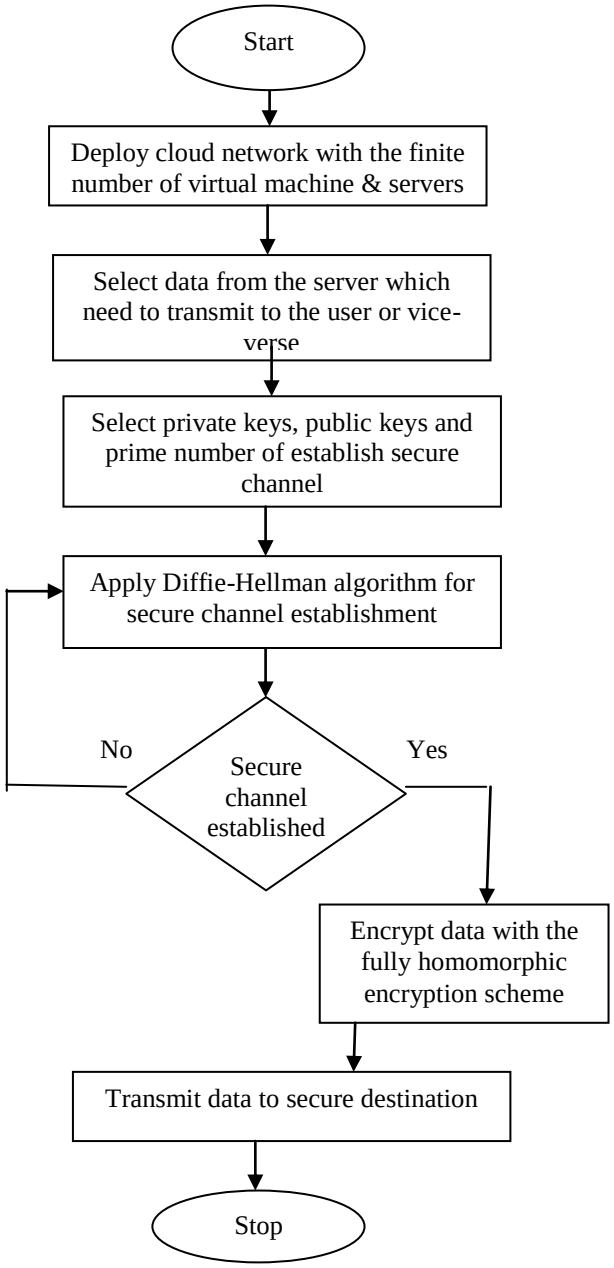

Fig.3 Flow Chart of Diffie- Hellman in FHE

Pseudo Code of RSA Algorithm

1**.** Let two large random prime integers: p and q.

2. Calculate n and φ(n) where, n = pq and φ(n) = (p-1)(q-1).

3. Choose an integer e, range: 1<e<φ(n) and gcd (e, φ(n))=1where gcd stands for greatest common denominator**.**

4. Compute d, range: $1<d<\varphi(n)$ such that: $ed \equiv 1 \pmod{\varphi(n)}$

Where,

- There are two keys i) the public key is (n,e)

  ii) the private key is (n,d)
- P, q and φ(n) are the private values.
- e is used as public or encryption exponent
- d is used as private or decryption exponent.

Pseudo Code of Diffie-Hellman Algorithm

Steps:

1. Alice and bob agree on a huge prime number p and a generator g. it would not matter to both if someone listen it as they are using insecure communication.
2. Alice chooses a random integer $xA < p$. Similarly Bob chooses $x_B < p$ both of them kept secret from everyone. These are their "Public key".
3. Alice "public key" is $y_A \equiv g^{x}{}_A \pmod p$ and sends it to Bob using insecure communication. Bob's "public key" is $y_B \equiv g^{x}{}_B$ and sends it to Alice. Here $0 < y_A < p$, $0 < y_B < p$.

   As discussed above, sending these public keys with insecure communication is safe because it would be difficult to calculate x_A from y_A or x_B from y_B, same as the powers of 2 above.

4. Alice computes $z_A \equiv y_B{}^{x}{}_A \pmod p$, Bob computes $z_B \equiv y_A{}^{x}{}_B \pmod p$. Here $z_A < p$, $z_B < p$.

   But $z_A = z_B$, since $z_A \equiv y_B{}^{x}{}_A \equiv (g^{x}{}_B)^{x}{}_A = g^{(x}{}_A{}^{x}{}_B{}^{)} \pmod p$ and similarly $z_B \equiv (g^{x}{}_A)^{x}{}_B = g^{(x}{}_A{}^{x}{}_B{}^{)} \pmod p$. So this value is their shared secret key. They can use it to encrypt and decrypt so that rest of their communication becomes faster.

   In this calculation, notice that the step $y_B{}^{x}{}_A \equiv (g^{x}{}_B)^{x}{}_A$ involved replacing $g^{x}{}_B$ by its remainder y_B, (in the reverse direction) here we were using the "as often as you want" principle.

IV. Results and Discussion

The results and discussion contains the results of the RSA and Diffie-Hellman algorithm. The performance of RSA and Diffie-Hellman algorithms are compared in terms of execution time, probability of attacks and space utilization. It has been analyzed that RSA Algorithm performs well in terms of all parameters.
Comparison of these algorithms are shown in the form of following graphs:

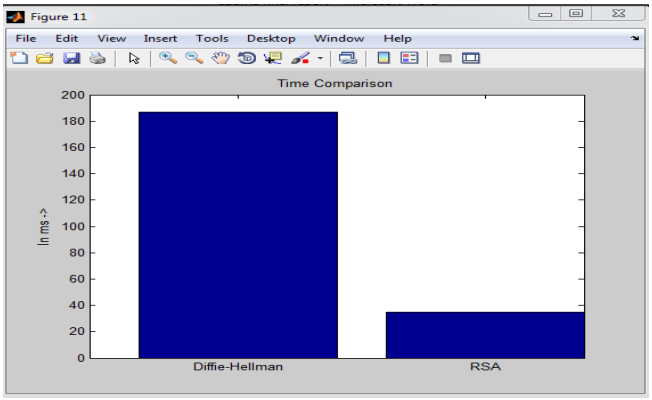

Fig.4 Comparison graph of Execution Time

Figure 4 shows the Execution Time graph of the Diffie-Hellman algorithm is compared with the RSA algorithm in the form of bar graphs.

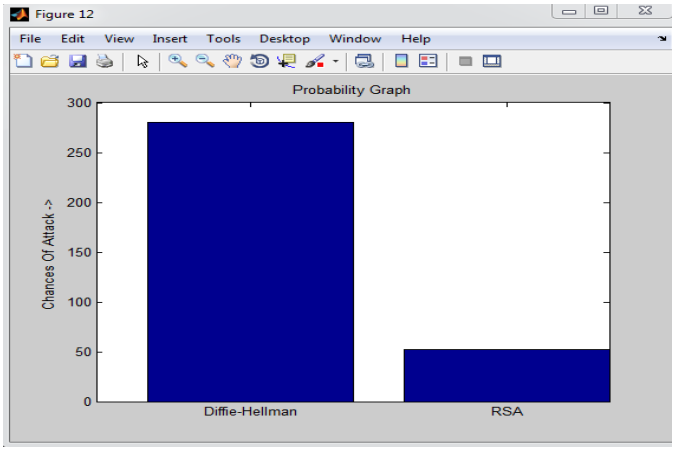

Fig.5 Comparison graph of probability of attacks

Figure 5 shows the Probability of attacks graph of the Diffie-Hellman algorithm is compared with the RSA algorithm in the form of bar graphs.

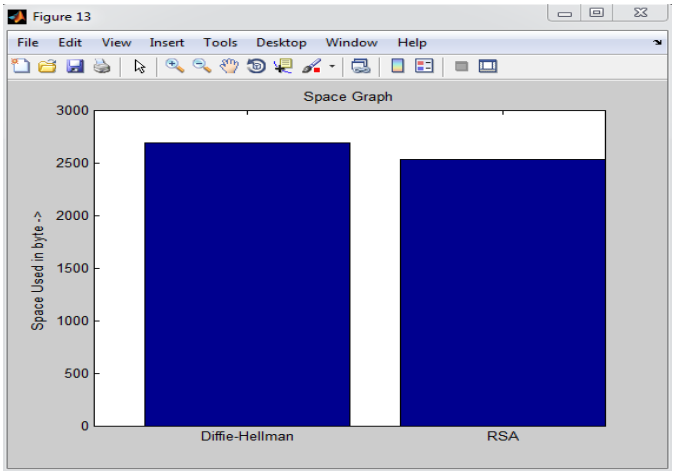

Fig.6 Comparison graph of Space Used

Figure 6 shows the Space Used graph of the Diffie-Hellman algorithm is compared with the RSA algorithm in the form of bar graphs.

Table 1: Qualitative Comparison of the algorithms

PARAMETERS	RSA	DIFFIE-HELLMAN
Ephemeral Keys	Generating ephemeral keys for RSA is extremely difficult.	Generating ephemeral keys for Diffie-Hellman is extremely easy.
Security	Relies on the difficulty of integer factorization.	Relies on the difficulty of discrete logarithm.
Encryption Cost	Encryption is cheaper.	Encryption is expensive.
Public Key Encoding	Public key is smaller to encode.	Public key is bigger to encode.
Strength	RSA 1024 bits is less robust than Diffie-Hellman.	Diffie-Hellman 1024 bits is much more robust.
Authentication	Authenticates only the sender.	Authenticates both the sender and the receiver.
Attacks	Susceptible to low exponent, common modules and cycle attack.	Susceptible to man-in-the-middle attack.

After analyzing it conclude that RSA algorithm is more secure, more reliable and more practically used algorithm available today in comparison to Diffie- Hellman algorithm. It is much faster as compare to less secured algorithms.

Table 2: Quantitative Comparison of the algorithm

Factors	Diffie-Hellman	RSA
Execution time	40 seconds	21 seconds
Space Utilization	2600 buffers	2400 buffers
Probability	92 percent	45 percent

It shows the comparison of RSA and Diffie- Hellman algorithm on following parameters as Execution Time, Probability of attacks and Space Used. After analyzing the graph it conclude that the execution time, probability of attacks and space used of RSA algorithm is much less than he Diffie- Hellman algorithm.

V. CONCLUSION AND FUTURE SCOPE

In this research work, the diffie-hellman algorithm is applied for the secure channel establishment in the fully homomorphic encryption. The RSA algorithm is also applied to improve performance of fully homomorphic encryption schemes. The performance of the RSA and Diffie-Hellman algorithms are compared in terms of execution time, probability of attacks and space utilization. On the basis of graphs shown in Fig 3, Fig 4 and Fig 5 respectively, the execution time of the RSA algorithm is less as compared to the diffie-hellman algorithm, the probability of attacks in the RSA algorithm is less as compared to diffie-hellman algorithm and the space utilization of RSA algorithm is less as compared to diffie-hellman due to less complexity. It has been analyzed that RSA algorithm performs well as compared to diffie-hellman algorithm. The hybridization of RSA algorithm is the efficient algorithm than the hybridization of diffie-hellman for the secure channel establishment. This work mainly focuses on the security of two parties so that data should be protected from various unauthorized users. In future, RSA algorithm will be further improved for OTP generation in the network. The RSA algorithm can be compared with other symmetric algorithms to analyze its reliability on Fully Homomorphic Encryption basis.

REFERENCES

[1] http://www.google.com/sans.org/rr/encryption/algorithm.php the Diffie-Hellman Algorithm Riley Lochridge April 11, 2003

[2] Craig Gentry, 2009,"full homomorphic encryption scheme"

[3] John Harauz ,Lori M. Kaufman,Bruce Potter," Data Security in the World of Cloud Computing " IEEE Security and Privacy July 2009. pp. 61-64

[4] van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V (2010) Fully homomorphic encryption over the integers. In Gilbert, H., ed.: EUROCRYPT. Volume 6110 of Lecture Notes in Computer Science., Springer

[5] Geethu Thomas, 2010,"Cloud Computing security using Encryption Technique"

[6] Sean Carlin, Kevin Curran, 2011 "Cloud Computing Security" International Journal of Ambient Computing and Intelligence, pp 14-19

[7] Shui Han, Jianchuan Xing, 2011 "Ensuring Data Storage Through A Novel Third Party Auditor Scheme in Cloud Computing" IEEE computer science & Technology, pp 264-268

[8] Dawn Song, Elaine Shi, 2012 "Cloud Data Protection for the Masses" IEEE Computer Society, pp 39-45

[9] Deyan Chen, Hong Zhao, 2012" Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering, pp 647-651

[10] Deepanchakaravarthi Purushothaman[1] and Dr.Sunitha Abburu[2] ,2012" An Approach for Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1.

[11] Dian-Yuan Han, Feng-qing Zhang, 2012 "Applying Agents to the Data Security in Cloud Computing" International Conference on Computer Science and Information Processing(CSIP), pp 1126-1128

[12] Dr Nashaat el-Khameesy,Hossam Abdel Rahman, 2012 "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" vol-3

[13] Simarjeet Kaur, 2012 "VSRD-IJCSIT, Vol. 2 (3), 2012, 242-249. Cryptography and Encryption In Cloud Computing, pp 242-249

[14] Young-Gi Min, Hyo-Jin Shin and Young-Hwan Bang, 2012 "Cloud Computing Security Issues and Access Control Solutions" Journal of Security Engineering, pp 135-140
[15] Yu, Z., Wang, C., Thomborson, C., Wang, J., Lian, S., & Vasilakos, A. V. (2012). A novel watermarking method for software protection in the cloud. Software: Practice and Experience, 42(4), 409-430.
[16] Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore, 2013 "Cloud Computing Security" International Journal on Recent and Innovation Trends in Computing and Computation, pp 36-39
[17] Bhavna Makhija, Vinit Kumar Gupta, 2013 "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, pp 341-345
[18] Barron, C., Yu, H., & Zhan, J., 2013 "Cloud Computing Security Case Studies and Research". Proceedings of the World Congress on Engineering 2013 Vol II
[19] Sanjoli Singla, Jasmeet Singh, 2013 "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013, pp 2232-2235
[20] Punithasurya K, Esther Daniel, Dr. N. A. Vasanthi, 2013 "A Novel Role Based Cross Domain Access Control Scheme for Cloud Storage" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013, pp 942-946
[21] Vimmi Pandey, 2013 "Securing the Cloud Environment Using OTP" International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4
[22] Anjana Chaudhary, Ravinder Thakur, Manish Mann, 2014 "Security in Cloud Computing by using Homomorphic Encryption Scheme with Diffie-Hellman Algorithm "International Journal of Advanced Computational Engineering and Networking Volume-2, Issue-10, Oct-2014, pp 2320-2106
[23] Peidong Sha, Zhixiang Zhu, 2016 "The Modification of RSA algorithm to Adapt Fully Homomorphic Encryption Algorithm in Cloud Computing" IEEE CCIS2016
[24] Matlab Tutorial by Tutorials Point https://www.tutorialspoint.com/matlab/matlab_overview.htm
[25] Will Garner "Diffie-Hellman Key Exchange" ppts.

Authors Profile

Ms.Aparna Negi completed Bachelor of Computer Science and Engineering from Uttarakhand Technical University, Dehradun in 2016. She is currently pursuing Master of Technology under Uttarakhand Technical University, Dehradun, India.

Mrs.Anshika Goyal is currently working as Assistant Professor in Department of Computer Science & Engineering, Faculty of Technology, Uttarakhand Technical University, Dehradun, India.

