INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue5)

Available online at: www.Ijariit.com

Implementing Multiple Security in the Cloud Environment

Anuradha[1], Dr. Suman Sangwan[2]

DCRUST, Murthal, Sonepat

ABSTRACT: Cloud computing is continuously evolving and considered next generation architecture for computing. Typically, cloud computing is a combination of computing resources accessible via internet. Historically, the clients or the organizations store data in data centers with firewall and other security techniques to protect data against intruders. However, in cloud computing, since the data is stored anywhere across the globe, the client organizations have less control over the stored data. To build the trust for the growth of cloud computing, the cloud providers must protect the user data from unauthorized access and disclosure. Here in this work hybrid approach of encryption techniques and the storage of data are considered in the cloud system. The main advantage of the hybrid scheme is to provide more security in the cloud.

Keywords: Data Encryption, cloud computing, Encryption algorithms, security etc.

I. INTRODUCTION

Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure, and customize applications online. It offers online data storage, infrastructure and application. The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud.

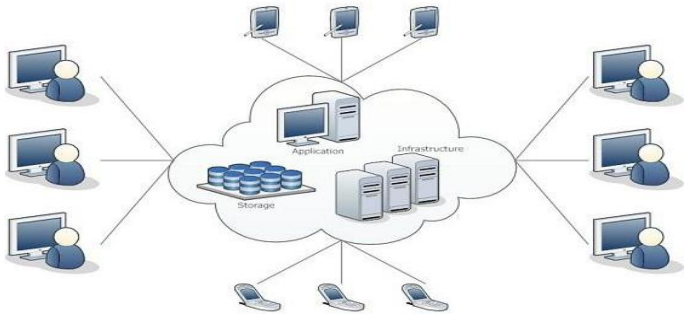

Figure 1: Cloud Computing

The cloud makes it possible for users to access information from anywhere anytime. It removes the need for users to be in the same location as the hardware that stores data. Once the internet connection is established either with wireless or broadband, user can access services of cloud computing via hardware. This hardware could be a desktop, laptop, tablet or phone.

1.1 *Cloud Service Model*

There are basically three types of service model in the cloud which are having features of application, software and hardware sharing resources in a cloud. These three service models are given below:-

Infrastructure as a service: In IaaS clients get access to infrastructure for deploying their stuff in the cloud. This service does not control or manages the infrastructure. In fact this manages or controls the Operating system, storage, applications. Here client is not control the cloud infrastructure but controls the operating system, storage, limited users and controls of host firewalls.

Platform as a service: In platform as a service generally user deploys and controls their applications in a cloud. In this user never ever manages the servers and the storage. Here client is not able to control the cloud infrastructure for example servers, operating systems, data storage, network connections but controls the deployed cloud applications and hosting configurations.

Software as a service**:** In software as a service we basically use the provider applications. In this user never ever manage or controls the network, operating system and applications. Here client does not control the cloud infrastructure for example operating system, storage, servers and the limited users cloud based application setting. It generally provides services to the users or the service providers provide virtualization abilities. Multiple types of services are provided by the service interface.

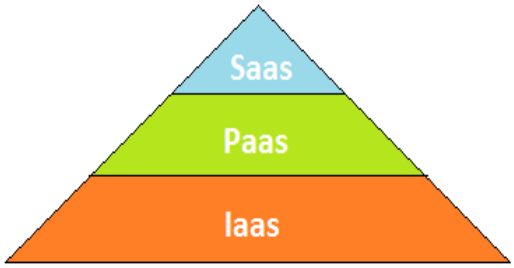

Figure 2: Cloud Models or Layers [2]

Interest of researchers in cloud computing is growing rapidly. It is believed that storage, networking and the computing all focus on horizontal scalability of virtualized resources rather than on single node performance. Moreover:

1. Applications software needs to scale up rapidly as well as scale down, which is a new requirement in the cloud. Such software also needs a pay-for-use licensing model to match needs of cloud computing.

2. Infrastructure software must be aware of the fact that it is no longer running on bare metal but on VMs. Moreover, metering and billing need to be built in from the start.

3. Hardware systems should be designed at the scale of a container (at least a dozen racks), which will be of the minimum purchase size. Processors should work well with VMs and flash memory and should be added to the memory hierarchy. LAN switches and WAN routers must improve the bandwidth and the cost.

II. LITERATURE SURVEY

Many encryption algorithms have been developed and implemented in order to provide more secured data transmission process in cloud computing environment, such as, DES, AES etc. The experimental environment consists of the cloud network, server and the client. The encryption algorithms are different in many fields such as block input size, key size, and speed-up of the encryption transformation. In this review paper following literature is used which mainly on data encryptions in public cloud are computing:-

Ln[2] Jasleen Kaur et al. represented the encryption algorithms which do not provide any authentication check for the clients but the survey security is the most weakest area of this research paper. It also increases the ease of use of data in a public cloud.

Ln[6] K. Sudha et al. presented that the encryption of original data before outsource it using advanced encryption techniques and retrieve the original data by using coordinate matching algorithm. It also provides more security to the original data.

Ln[7] Shakeeba S. Khan et al. proposed a cryptographic algorithms for security in cloud computing. The proposed plan is to eliminate the concerns in data privacy for enhancing cloud's security in different cloud customers. In this research paper if some intruder gets a valid key that he/ she can easily gets the data intentionally.

Ln[8] Ramalingam Sugumar et al. proposed a symmetric encryption algorithm which is used to secure a outsource data in a public cloud storage. This proposed algorithm minimizes time for the encryption and decryption. And the cloud should not access data stored in cloud storage server.

Ln[9] Hasan Omar Al- Sakran represented a scheme which minimize communication overhead and computations on client and server sides. And the issues of this research paper of a untrusted client and another one is the outsourced data and the data owner's application software to a cloud provider.

Ln[10] Dr. Nandita Sengupta presented a hybrid RSA Encryption algorithm for the cloud security in which a proposed hybrid RSA algorithm provide a higher level of security but cannot maintains a integrity of data in a public cloud.

Ln[11] V.Masthanamma et al. proposed a RSA encryption algorithm which is used to enhance the security of cloud and it also increases the security of data and consumes less time and the less cost. But the disadvantages of this work are a fake public key algorithm, key generation complexity, security needs and the low speed.

Ln[12] Alycia Sebastian et al. represented data security issues in public cloud. The data in cloud identify and discuss security risks associated with it and analyzes its solution strategies. For maintaining a secure environment it requires a shared responsibility of cloud providers and the customers.

III. PROPOSED WORK

In this work, an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud is proposed. By utilizing the symmetric token with dynamic verification of resource usage, the proposed scheme achieves the security and integrity of data storage on clouds. Moreover, when data corruption has been detected during the storage resource usage then the proposed scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving client. By using encryption techniques on password and security key, client feels more secure on a cloud because here even admin also don't know the password of any of his client.

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in the proposed work further provides the localization of data error.
2. Unlike most prior works for ensuring remote data integrity, the proposed scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
3. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colliding attacks.

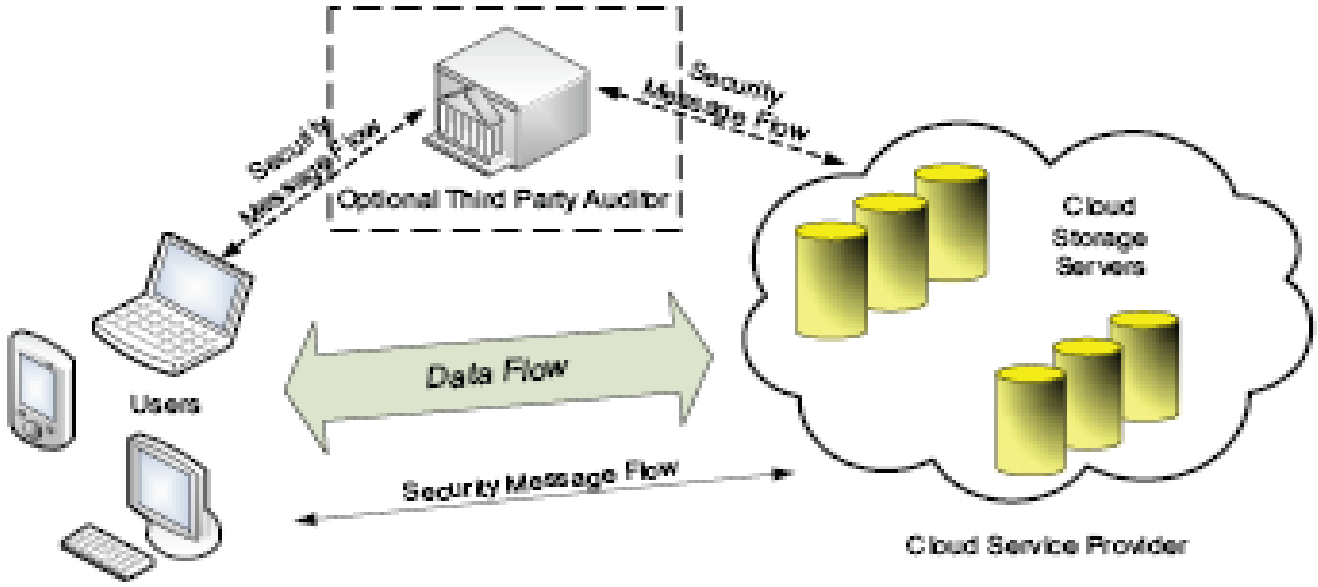

Figure 3: Cloud data storage architecture

IV. RESULT AND DISCUSSION

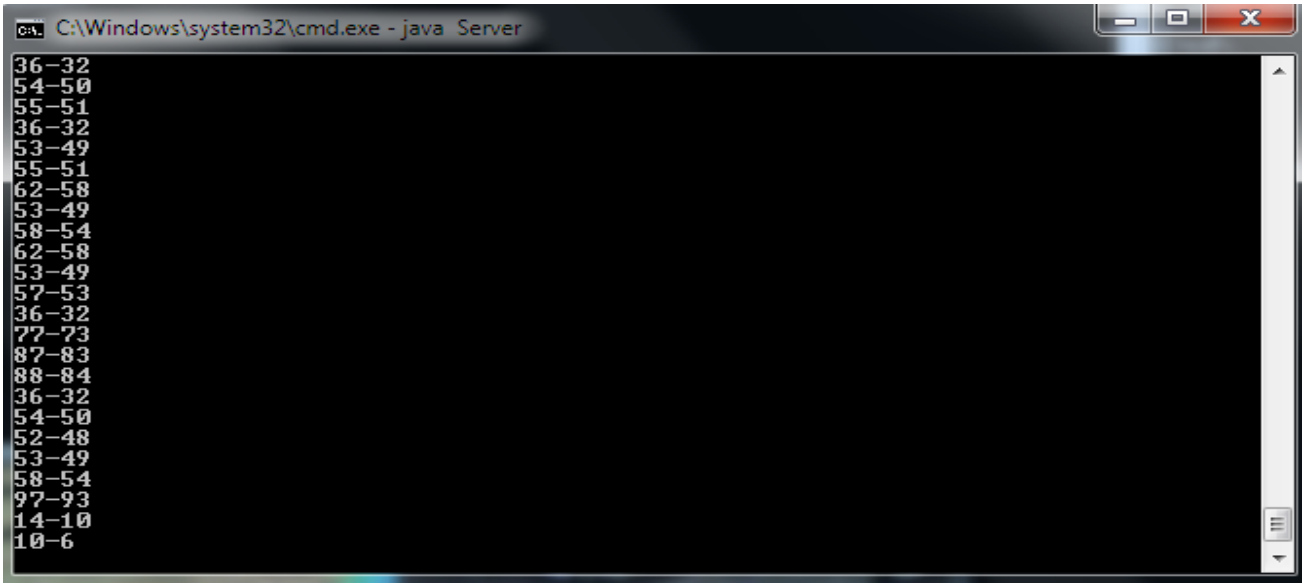

Figure 4: Data is passed using encryption algorithm

The figure 4 as given above shows how the data is passed using encryption algorithm for the security purpose in the cloud environment.

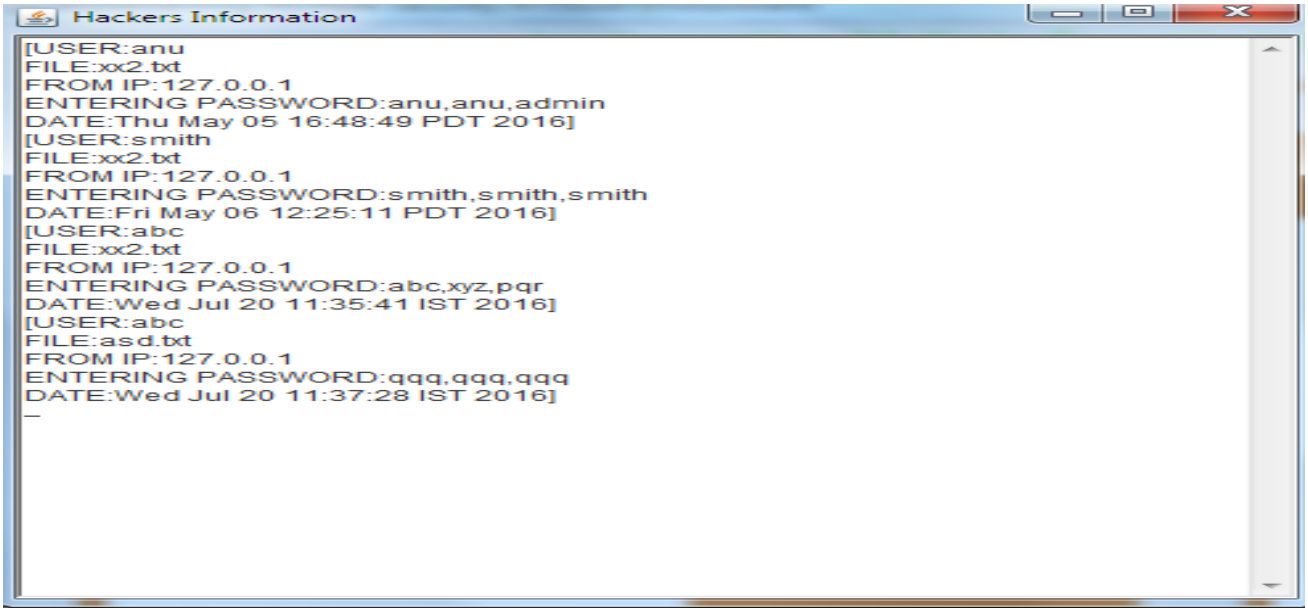

Figure 5: Hacker information on server side

In figure 5, all the hacker information with their username, file name which they want to hack, IP address of the hacker, three passwords which he/she tried to access any file, date and time of the hacking is stored in a text file on a server side.

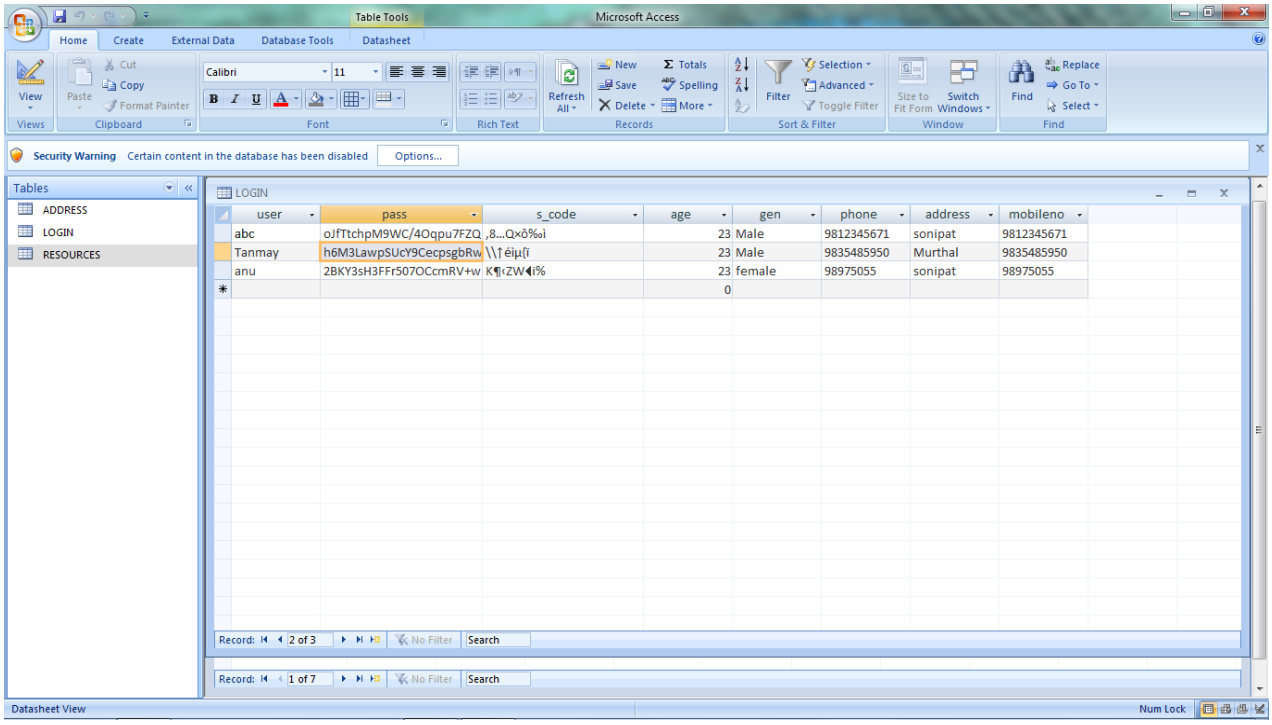

Figure 6: Password and security key saved in database using DES and AES encryption techniques.

V. Conclusion

In this research work two encryption algorithms one is advanced encryption algorithm (AES) and another one is data encryption algorithm (DES) are combined together to reach to the conclusion. The proposed work uses a hybrid algorithm that is based on password

and security key. By using hybrid algorithm on the security key and the password, client feels free from his/her fear that the administrator on the server side know the password because in this case even administrator doesn't know the security key and the password of any of his client. The password and the security key both are saved in a database in encrypted form.

In the presented work, the administrator also provides security in his/her resources by using the concept of true or false token in his/her resources. The resources which are authorized can be used by the client. If any client who is not allowed to use a particular resource, in that cases all his/her information is stored on the server side. The information stored on the server side is like username of a client, his IP address, password which he/she tries on a cloud, file name which he/she wants to hack and even the date and time of the hacker client.

The proposed algorithm can be made more flexible and reliable in future. By using more algorithms, more features and security can be added and more improved performance can be achieved in future. The presented work is defined mainly based on hacker attack; in future some other improvement can be done in the communication reliability.

REFERENCES

[1] Singla. Sanjoli, and Singh. Jasmeet, "Cloud data security using authentication and encryption technique," Global Journal of Computer Science and Technology 13.3, 2013.

[2] Kaur. Jasleen, Ms Anupma Sehrawat, and Ms Neha Bishnoi, "Survey Paper on Basics of Cloud Computing and Data Security." International Journal of Computer Science Trends and Technology (IJCSTT), 2014.

[3] Singhrova, Anita. "A host based intrusion detection system for DDoS attack in WLAN." Computer and Communication Technology (ICCCT), 2011 2nd International Conference on. IEEE, 2011.

[4] Gupta, Shikha, and Suman Sangwan. "Load Balancing in Cloud Computing: A Review." International Journal of Science, Engineering and Technology Research (IJSETR), June 2015

[5] Rani, Amita, and Mayank Dave. "Weighted load balanced routing protocol for MANET." Networks, 2008. ICON 2008. 16th IEEE International Conference on. IEEE, 2008.

[6] K. Sudha, B. Anusuya, P. Nivedha, A. kokila, "International Journal of Advanced Research in Computer Science and Software Engineering." Volume 5, Issue 1, 2015

[7] Khan, Miss Shakeeba S., Prof. R. R. Tuteja, "International Journal of Innovative Research in Computer and Communication Engineering", Volume 3, Issue 1, 2015

[8] Sugumar, Ramalingam, and Sharmila Banu Sheik Imam. "Symmetric encryption algorithm to secure outsourced data in public cloud storage."Indian Journal of Science and Technology 8.23 (2015):1.

[9] Al-Sakran, Hasan Omar. "ACCESSING SECURED DATA IN CLOUD COMPUTING ENVIRONMENT." International Journal of Network Security & Its Applications 7.1 (2015): 19.

[10] Sengupta Dr. Nandita., "International Journal of Innovative Research in Computer and Communication Engineering, Volume 3, Issue 5, 2015.

[11] V. Masthanamma, Preya G. Lakshmi., " International Journal of Innovative Research in Science Engineering and Technology", Volume 4, Issue 3, 2015.

[12] Gupta Diksha., Chakraborty Partha Sarathi., Rajput Pragya., "Cloud Security using Encryption Techniques", "International Journal of Advanced Research in Computer Engineering & Technology(IJARCET)", Volume5, Issue2, February 2015.

[13] Sharmila, R., "Secure retrieval of files using homomorphic encryption for cloud computing", "International Journal of Research in Engineering and Technology", 2014.

[14] Boopathy, D., and M. Sundaresan. "Data encryption framework model with watermark security for Data Storage in public cloud model." Computing for Sustainable Global Development (INDIACom), 2014 International Conference on IEEE, 2014.

[15] Khachatrian, Gurgen and Melsik Kyureghyan. "A New Public Key Encryption System Based on Permutation Polynomials." Cloud Engineering(IC2E), 2014 IEEE International Conference on IEEE, 2014

[16] Hu, Chengyu, et al. "Public-key encryption for protecting data in cloud system with intelligent agents against side-channel attacks." Soft Computing (2015):1-14.

[17] Luo Wenjum, Tan Jianming., "IEEE CCIS", 2012

[18] Long, Bin, et al. "On Improving the Performance of Public Key Encryption with Keyword Search" Cloud and Service Computing (CSC), 2012 International Conference on IEEE, 2012

[19] Arapinis, Myrto, Sergiu Bursuc, and Mark Ryan. "Privacy supporting cloud computing: Confichair, a case study." Principles of Security and Trust. Springer Berlin Heidelberg, 89-108, 2012.

[20] Renu S, Hasna Parveen O H, "International Journal of Advanced Research in Computer and Communication Engineering", Volume4, Issue 2, February 2015

[21] Sur, Chul, et al. "Certificate-based proxy re-encryption for public cloud storage." Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on. IEEE, 2013

[22] Liang. Kaitai, et al. "DFA-based functional proxy re-encryption scheme for secure public cloud data sharing." Information Forensics and Security, IEEE Transactions on 9.10:1667-1680, 2014.

[23] Tseng Fu-Kuo., Chen Rong-Jaye, Lin Bao-Shuh Paul, "IEEE International Conference on Trust, Security and Privacy in Computing and Communication", 2013

[24] Parkash G L, Dr. Manish Prateek, Dr. Inder Singh, "International Journal of Engineering and Computer Science", Volume3, Issue 4, Pg. 5215-5223, April 2014

[25] Sangwan, Suman, Parvinder Singh, and R. B. Patel, "Uivh-algorithm for semless mobility in heterogeneous wireless network." Proceedings of the CUBE International Information Technology Conference. ACM, 2012

[26] Kuyoro S. O., Ibikunle F. & Awodele O., "International Journal of Computer Networks (IJCN)" , Volume (3) : Issue (5) : 2011

[27] M N Manas., Nagalakshmi C., G. Shobha., "International Journal of Advanced Research in Computer and Communication Engineering", Vol. 3, Issue 4, April 2014

[28] Sajjad Hashemi., "International Journal of Security, Privacy and Trust Management (IJSPTM)",Vol 2, No 4, August 2013.

[29] Gampala, Veerraju, Srilakshmi Inuganti, and Satish Muppidi. "Data security in cloud computing with elliptic curve cryptography." International Journal of Soft Computing and Engineering (IJSCE) 2.3 : 138-141, 2012.

[30] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis."International journal of emerging technology and advanced engineering 1.2 : 6-12, 2011

[31] Sugumar, Ramalingam, and Sharmila Banu Sheik Imam. "Symmetric encryption algorithm to secure outsourced data in public cloud storage."Indian Journal of Science and Technology 8.23, 2015.

