International Journal of Advance Engineering and Research Development
Scientific Journal of Impact Factor (SJIF): 4.72
Special Issue SIEICON-2017,April -2017
e-ISSN : 2348-4470 p-ISSN : 2348-6406

Data Security for Cloud Computing with Double Layer Encryption Algorithm based on DNA and AES

Megha D. Randeri[1], Mr. Sheshang D. Degadwala[2], Mrs. Kishori S. Shekokar[3]

[1]M.E. Student, Computer Department, Sigma Institute of Engineering.
[2]Assistant Professor, Computer Department, Sigma Institute of Engineering.
[3]Head of Computer Department, Sigma Institute of Engineering.

Abstract — *The emergence of cloud computing has made a tremendous impact on the Information Technology (IT) industry over the past few years. Cloud computing provides a new paradigm for hosting and delivering services over the Internet which moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. Although having the flexibility to gain access to data anywhere in the world, Cloud computing have many security challenges to protect multiple users' data. Privacy and security of cloud storage services are very important and become a challenge in cloud computing due to loss of control over data and its dependence on the cloud computing provider. Security issues like privacy, data security, confidentiality and authentication need to be considered in Cloud computing. In this paper, I present a double layer encryption algorithm based on DNA encoding with AES symmetric key algorithm to make cloud data more secure.*

Keywords- *Cloud Computing, AES Algorithm, RSA, Digital Signature, DNA Sequences.*

I. INTRODUCTION

Cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS)[6]. Although having flexibility to gain access to data from anywhere, Cloud computing has many security challenges to protect multiple users' data.

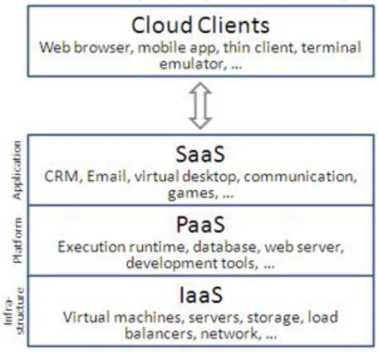

Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

Figure 1. Architecture of cloud system

As shown in the Figure 1 Architecture of cloud system consists of mainly 3 layers. First layer consists of client who stores the data into the cloud. The data can be in any form like files, client information, etc. The client will first register and gets the authentication access by login using their username and password. After login into the system user can store their confidential data into cloud by using the encryption technique which is AES based encryption. Second layer consists of application server which has cloud storage business logic layer and database. Cloud storage business logic layer consists of code which is used to connect the application to the database. So that the data passed into the application will be directly saved into the database. Third layer consists of third party storage server which usually contains the data that can be accessed by the third party agent of the cloud system. The data is stored confidentially by cloud owner[2].

II. LITERATURE REVIEW

There are many studies and researches performed to enhance the security of cloud computing storage and environment using encryption techniques. However, there has been a slight improvement in the results of these works comparing with the rapid growth of cloud. Here, I have conducted a Literature Review of five papers to compare the different encryption algorithms providing security to cloud data based on the factors like higher security and faster encryption process. Table 1 shows the comparative analysis of five papers.

Table 1. Comparative Analysis

Sr. No	Paper title	Authors name	Implementing Symmetric or Asymmetric Algorithms	Providing Optimal Solution for cloud security
1	Enhanced Data Security Model for Cloud Computing	1) Eman M. Mohamed 2) Hatem S. Abdelkader 3) Sherif El-Etriby	No Implementation	Yes
2	Enhancement of Security Mechanism for Confidential Data using AES-128, 192 and 256 bit Encryption in Cloud	1) Gaurav Raj 2) Ram Charan Kesireddi 3) Shruti Gupta	Symmetric AES with 128, 192 and 256 bit key length	Yes
3	A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services	1) Nasrin Khanezaei 2) Zurin Mohd Hanapi	Both asymmetric RSA and symmetric AES	Yes
4	Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing	1) Uma Somani 2) Kanika Lakhani 3) Manish undra	Digital signature with asymmetric RSA	Yes
5	A Double Layer Encryption Algorithm based on DNA and RSA for Security on Cloud	1) Karandeep Kaur	DNA algorithm with asymmetric RSA algorithm	Yes

In [1], Eman M. Mohamed, Hatem S. Abdelkader, Sherif El-Etriby proposed a model of three-layer system structure, in which the first layer is responsible for user authentication, the second layer is responsible for user's data encryption and the third layer is responsible for fast recovery of user data. They used NIST statistical tests to get the highest security encryption algorithm from eight algorithms namely RC4, RC6, MARS, AES, DES, 3DES, Two-fish and Blowfish. For case study they used Micro Instances of the Amazon EC2 family.

In [2], Gaurav Raj, Ram Charan Kesireddi and Shruti Gupta used the enhancement of AES encryption technique to encrypt the confidential data in the cloud. In that, confidential data will be encrypted, so that it reduces the time, space and cost. Based on the size of the data encryption is decided. For large data 128 bits key, for medium data 192 bits key and for small data 256 bits key is used for the encryption process. The implementation of AES encryption is done on Visual Studio with ASP.NET as a front end and the programming language used here is C.

In [3], Nasrin Khanezaei and Zurin Mohd Hanapi presented a framework for cloud storage system using a combination of RSA and AES encryption methods to share the data among users in a secure cloud system. RSA is an asymmetric cryptographic algorithm where as Advance Encryption Standard (AES) is symmetric cryptography algorithm. Their proposed method is simulated in .net framework as two different applications which re server and client.

In [4], As per Uma Somani, Kanika Lakhani and Manish Mundra, cloud computing has problem like security of data, file system, backups, network traffic and host security. They have proposed a concept of digital signature with RSA algorithm, to encrypt the data while transferring it over the network. Their proposed model solves the dual problem of authentication and security.

In [5], Karandeep Kaur has proposed an approach of double layer encryption method to ensure security in cloud. It is based on a popular cryptography algorithm RSA and Deoxyribonucleic Acid sequences, which is relatively novel technique.

III. PROPOSED ALGORITHM

The algorithm that has been proposed in this paper consists of a double layer security algorithm. DNA algorithm is used followed by AES algorithm to ensure double layer protection in cloud environment. DNA sequences have been proved a quite novel technique [5]. Among various encryption algorithms AES has been proved the most secured and also takes less time to encrypt. Initially, user data is converted to binary equivalent which is encoded by DNA encoding sequence. The encoded text is further encrypted using AES.

In the proposed algorithm, the data is converted into binary text, which is encoded using specified DNA encoding sequence. Further, that encoded text is encrypted using Advanced Encryption Standard (AES) algorithm resulting in the full secure cipher text.

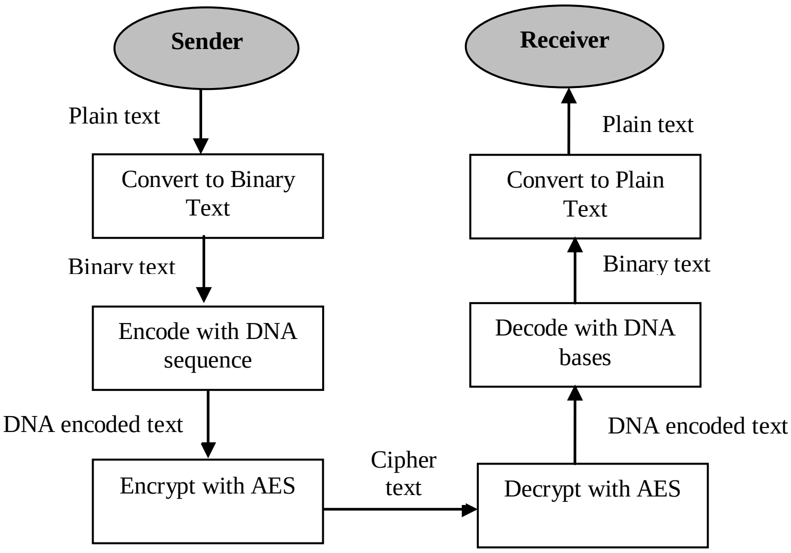


Figure 2. Proposed Algorithm

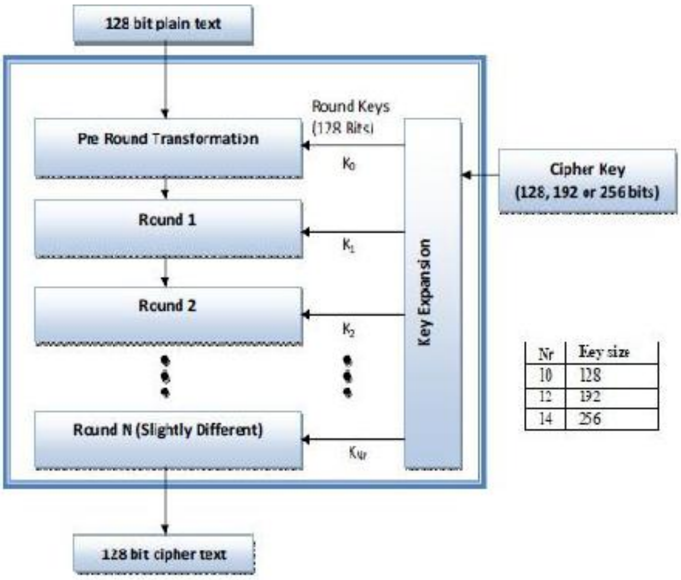
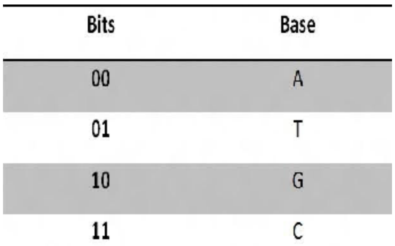


Figure 3. AES Encryption process [7]

DNA Algorithm

DNA is the starting point of all life species. DNA molecules contain stands of nucleotides which are named after the nitrogen base they are made of: Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). The DNA molecules have a double helix structure which is a combination of complementary strands A to T and G to C. These four bases can be represented by a combination of two bits as shown in Figure 4. [5]



Bits	Base
00	A
01	T
10	G
11	C

Figure 4. DNA Encoding [5]

IV. CONCLUSION

Cloud computing has been a new generation of communication because of its high flexibility and feasibility of access to IT resources. But security of cloud data is also a major issue. Depending on the cloud users' preference of the higher security or the performance of the algorithm, users can select the encryption techniques. Blowfish or DES or AES take the least time to encrypt data than others and ensure that data retrieve faster whereas AES is the highest security algorithm which takes less time to encrypt. In this paper a new double layer cryptographic technique has been proposed which combines the novel DNA algorithm with the most secure AES algorithm. The used DNA sequence is very hard to break.

REFERENCES

[1] Eman M. Mohamed, Hatem S. Abdelkader, Sherif El-Etriby "Enhanced Data Security Model for Cloud Computing" 2012 8th International Conference on INFOrmatics and Systems (INFOS2012).

[2] Gaurav Raj, Ram Charan Kesireddi and Shruti Gupta "Enhancement of Security Mechanism for Confidential Data using AES-128, 192 and 256 bit Encryption in Cloud" 2015 IEEE 1st International Conference on Next Generation Computing Technologies (NGCT-2015).

[3] Nasrin Khanezaei and Zurin Mohd Hanapi "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014).

[4] Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[5] Karandeep Kaur "A Double Layer Encryption Algorithm based on DNA and RSA for Security on Cloud" 2016 International Research Journal of Engineering and Technology.

[6] Balachandra Reddy Kandukuri, Ramacrishna PaturiV, Atanu Rakshi "Cloud Security Issues" 2009 IEEE International Conference on Services Computing.

[7] Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. R.K.Tiwari "An Approach towards Data Security in the Cloud Computing Using AES" June 2016 International Journal of Advanced Research in Computer and Communication Engineering.