International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 5, Issue 1, 2018, PP 1-8
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
DOI: http://dx.doi.org/10.20431/2349-4859.0501001
www.arcjournals.org

Elaborating Security Algorithms in Cloud Environment

Shaffy Bansal[1], Dr. Gagandeep Jagdev[2]

[1]*Research Scholar, M.Phil. (Comp. Appl.), Guru Kashi University, Talwandi Sabo (PB)*

[2]*Dept. of Comp. Science, Punjabi University Guru Kashi College, Damdama Sahib (PB)*

***Corresponding Author:** ***Dr. Gagandeep Jagdev**, Dept. of Comp. Science, Punjabi University Guru Kashi College, Damdama Sahib (PB), India.*

Abstract: *The security of data is the primary concern of every organization today irrespective of its size. The large organizations responsible for managing bigger monetary information, bio-data and other relevant information are losing their valuable information or data in motion or in rest to unauthorized parties, hackers, or competitors. When such data gets into the hands of malicious persons, the organizations lose millions of rupees. Today the data protection has become vital for businesses. The data or information should be encrypted or scrambled in such a manner that even if it gets into the hands of hackers or unauthorized users, it becomes useless for them. The scrambling of plaintext delivers a safe and nice significance for secured data and communication. With the expansion of LAN, MAN, and WAN, the computer network is exposed to unauthorized people providing them access to attack personal and organizational data in network and cloud environment. Every organization and individual desires that security and privacy of their data should be maintained. This can be achieved by applying cryptographic algorithms on such critical data in cloud environment. This research paper studies the different encryption/decryption algorithms responsible for security of data placed in cloud. The paper shows the implementation of AES algorithm on 256-bit key size.*

Keywords: *AES, DES, encryption/decryption, RSA, 256-bit.*

Abbreviations: *AES, DES, RSA*

1. INTRODUCTION

Whenever one decides to travel from his/her source to destination, he/she boards a bus or a train. After taking a ticket, the person hold back to his/her seat till the destination is reached. Similarly other passengers in the bus or train takes their particular tickets as per their individual destinations and it hardly bothers one where they go. Same is the story in case of cloud computing. Cloud computing is very similar to such a bus or a train which carries data and information for multiple and different users and permits them to access its service at minimal cost. The term "Cloud" originated from a network design that was utilized by concerned network engineers to represent the location of different network devices and inter-connection among them [1, 5]. The Fig. 1 below displays the set up involved in cloud computing.

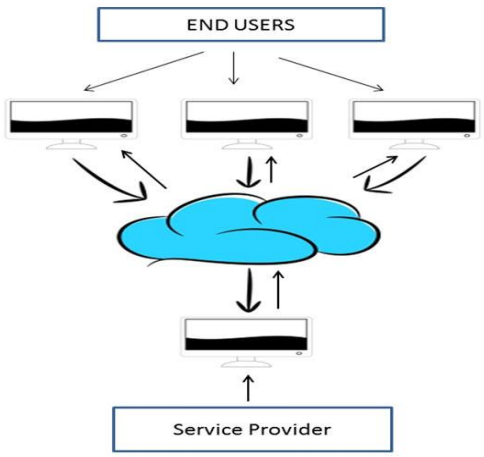

Fig1. *The figure depicts the setup of cloud environment*

As the number of computer and mobile user's increase, the demand for data storage has increased in all fields. No matter whether organization is small scale or large scale, they flourish on the basis of value and quality of their data. It is because of this that organizations invest heavily to maintain the worth of this data. But all this requires a strong storage hub and IT support. Not all businesses can manage the high cost involved in building in-house IT frame and maintain back up support services. For such situations, the cloud computing is a cheaper solution. In fact, because of its capability in storing data, computation and minimal maintenance cost, cloud computing has attracted even bigger businesses as well. The hardware and software demand is decreased from the user's side. The user has to only run cloud computing systems interface software and the cloud network tekes care of the rest. Some of the popular cloud services which is almost used by everyone are mail services like Hotmail, yahoo or gmail etc. When we access our email, our data is stored on cloud server and not on our own machine. The technology working behind the cloud is invisible. It doesn't matter whether cloud services are using HTTP, PHP, JSP, Ruby or any other specific technologies, user can simply connect to the cloud system from his/her desktop, mobile or laptop. The Fig. 2 shows the detailed scenario of working of cloud computing [2, 3, 13].

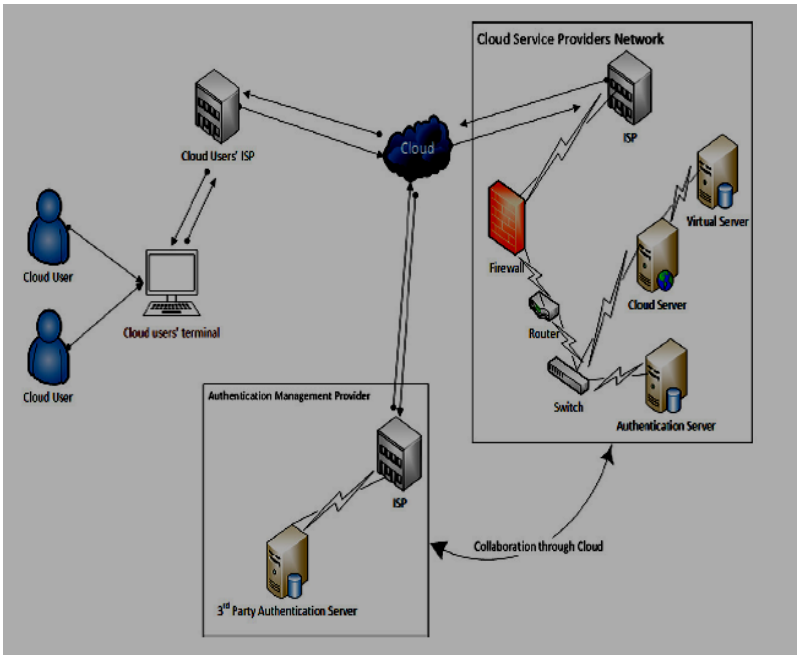

Fig2. *The figure shows the detailed view of authentication process involved in cloud computing*

Example - Google Cloud

Google is a search engine that offers all kind of information that is accessible and useful for the users. Google is offering numerous applications to their customers, applications that are helping them to reduce the consumption of the energy and carbon emission. Cloud computing can support an unlimited number of applications and Google Enterprise is offering some of them to their customers [4, 12].

The services offered by Google Enterprise are mentioned below.

- Google Apps - The service includes applications as e-mail, calendar, spreadsheets, and documents.
- Vault service - This service offers solution for mail security, archiving and encryption.
- Enterprise search.
- Earth and Maps - This service is offering tools to visualize information and direction about different places.
- Chromebooks - The service is used for delivering the power of the web.

Google Cloud Platform represents all the products of cloud computing offered by Google , that are using the same infrastructure as the one that Google is using for products offered to end-users, like: Google Search , YouTube.

Google Cloud Platform is composed of many products, where each of it has its own interface, command-line tool and API (Fig. 3).

- Google App Engine is a SaaS for web applications.
- Google Compute Engine is an IaaS that allows users to enable the virtual machine when needed.
- Google Cloud Storage allows users to store files online.
- Google Cloud DataStore offers storage for non-relational data that has a REST API.
- Google Cloud SQL is a MySQL database that exists on Google Cloud infrastructure.
- Google BigQuery is used to analyze data and is using SQL-like queries for dealing with big data in seconds.
- Google Cloud Endpoints is used for developing services within App Engine that can be accessed from IOS, Android and JavaScrip clients.
- Google Cloud DNS represents a DNS service that can be found in the infrastructure of Google Cloud.

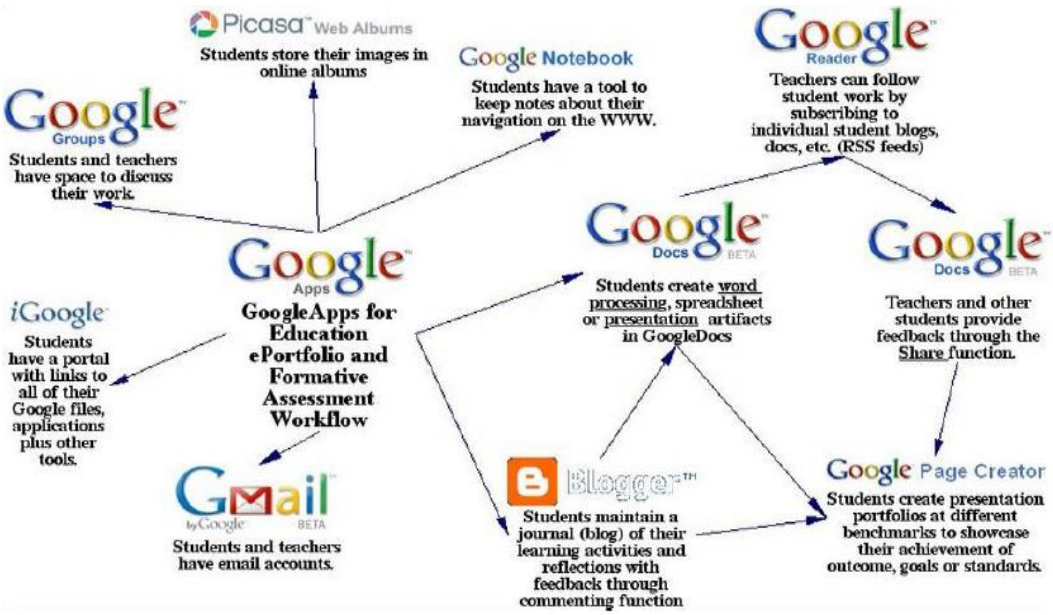

Fig3. *The figure shows the Google Cloud*

2. ALGORITHMS RESPONSIBLE FOR CLOUD SECURITY

In cloud environment, the individual's data is stored in and accessible from multiple distributed and connected resources. The security remains primary concern when the matter is of providing secure communication from distributed and connected resources. This task is accomplished by encryption algorithms. The encryption algorithm converts the data (plain text) into scrambled form (cipher text) using "the key" which is held by the user. This encryption is classified into two broad categories; Symmetric key encryption and Asymmetric key encryption. The symmetric encryption makes use of single key to encrypt and decrypt data. On the other hand, the asymmetric key makes use of two keys – private and public; public key is used for encryption and private key is used for decryption [1, 5].

The prominent cryptographic algorithms used for security of cloud environment are discussed as under.

2.1. RSA (Rivest Shamir Adleman)

The RSA algorithm is named after its three originators Ron Rivest, Adi Shamir, and Leonard Adleman. It is constructed on the property of positive integers. RSA makes use of modular exponential for carrying out the process of encryption and decryption. RSA algorithm involves a public key and a private key. The purpose of public key is to encrypt messages and is known to everyone. The private key comes into play while decrypting the messages. Messages encrypted by

public key can only be decrypted via private key. The Fig. 4 below shows the process involved in RSA algorithm [6, 7].

The details of variables utilized in description of working of RSA algorithm as shown in Fig. 2 are mentioned as under.

e – Refers to public key

d – Refers to private key

M – Refers to plain text

C – Refers to cipher text

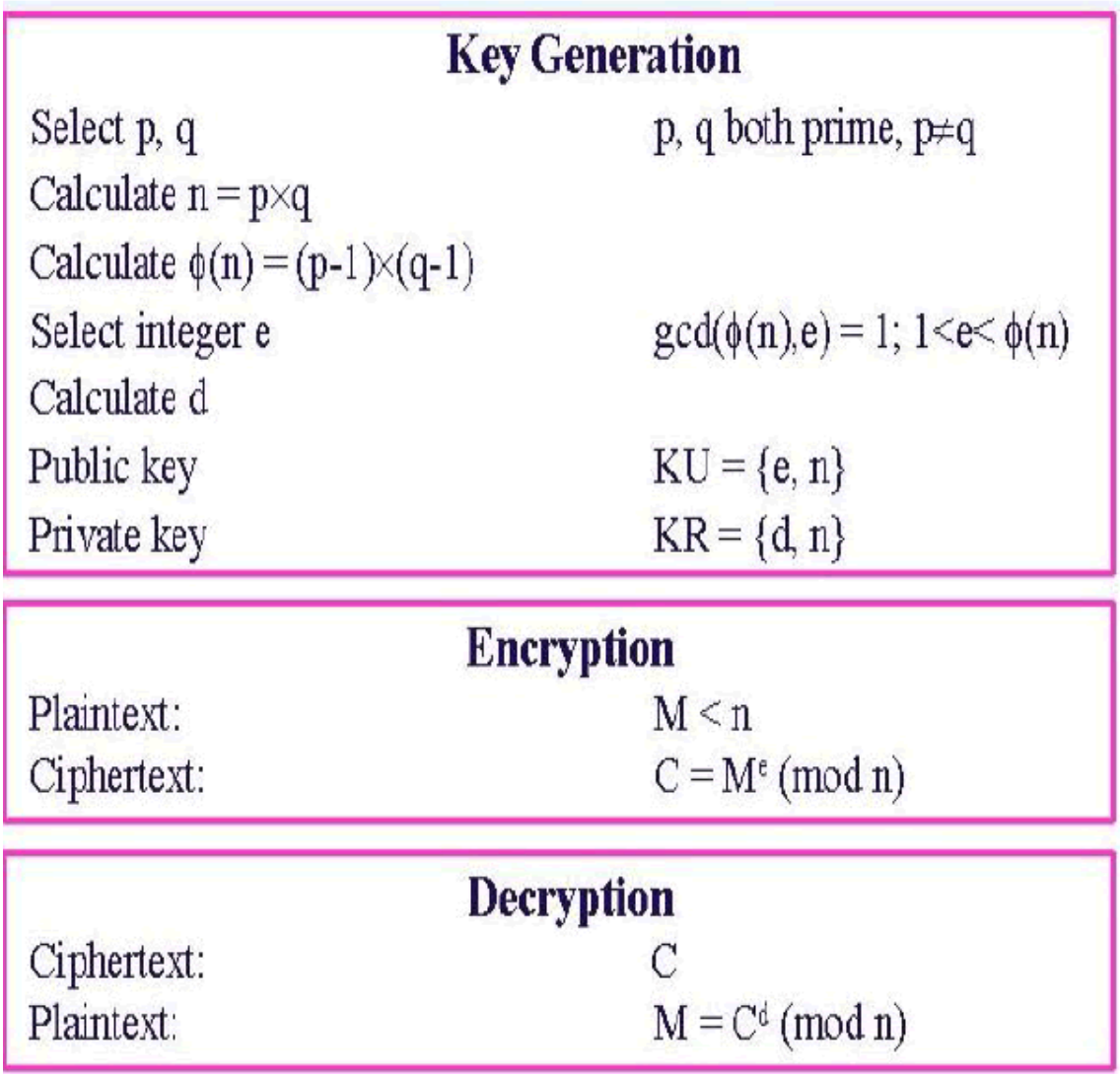

Fig4. *The figure depicts the working of RSA algorithm*

The result at the decryption side is calculated as under.

C = Me mod n

M = Cd mod n

Where n is a large number created during key generation process.

2.2. DES (Data Encryption Standard)

DES was developed in 1977 and was the first encryption standard recommended by NIST (National Institute of Standards and Technology). DES involves 64 bits key size and 64 bits block size. Since the time of its advent, DES has encountered many attacks which proved it as an insecure block cipher [1, 8].

Algorithm for DES:

Function DES_Encrypt (M, K)

Where M = (L, R)

M ← IP (M)

For round ←1 to 16 do

K ←SK (K, round)

L ←L xor F(R,Ki)

swap(L, R)

end

swap (L, R)

M ←IP^{-1}(M)

return M

End

2.3. Triple – DES

This algorithm was developed as an enhancement to DES and was developed in 1998. The modification conducted in 3-DES was that encryption was conducted 3 times to increase the encryption level. The 3-DES is a 64-bit block size with 192 bits key size. It has low throughput and low performance in terms of power consumption when compared with DES. Because of its triple phase encryption characteristics, it requires more time as compared to DES [5, 9].

Algorithm for Triple – DES

For j = 1 to 3

{

Cj,0= IVj

For i = 1 to nj

{

Cji = $E_{KEY3}(D_{KEY2}(E_{KEY1}(Pj, iCj, i-1)))$

Output Cj, i

}

}

2.4. AES (Advanced Encryption Standard)

The development of AES algorithm began on January 2nd 1997 and was completed on September 12th 1997 under the flag of NIST (National Institute of Standards and Technology). AES is a block cipher and is also known as Rijndael algorithm. This algorithm runs on variety of computer processors and hardware's. The complex internal structures of AES ensures very secure algorithm and till date it has no known weaknesses. The key length in AES can be 128, 192, or 256 – bits. The algorithm is constructed of variable block sizes of 128, 192, and 256 – bits [10, 11].

AES algorithm does its computations on bytes and not on bits. Therefore it treats, 128 bits of a plaintext as 16 bytes. These 16 bytes are organized in a matrix of order 4*4. The number of rounds in AES are variable as they depend on length of the key. AES performs 10 rounds for 128-bit key, 12 rounds for 192-bit key and 14 rounds for 256-bit keys. Each round makes use of 128-bit round key, which is computed from the original AES key.

3. CONTRIBUTION AND IMPLEMENTATION

The research paper depicts the implementation of AES algorithm using Java as a development tool. The Fig. 3 shows the entered plain text in the input box. If the number of bytes in plain text are below or upto 16 bytes, 128-bit encryption is activated. But if the number of bytes in plain text exceeds 16 bytes, the 256-bit encryption is activated. The Fig. 5 are shows the generated symmetric key.

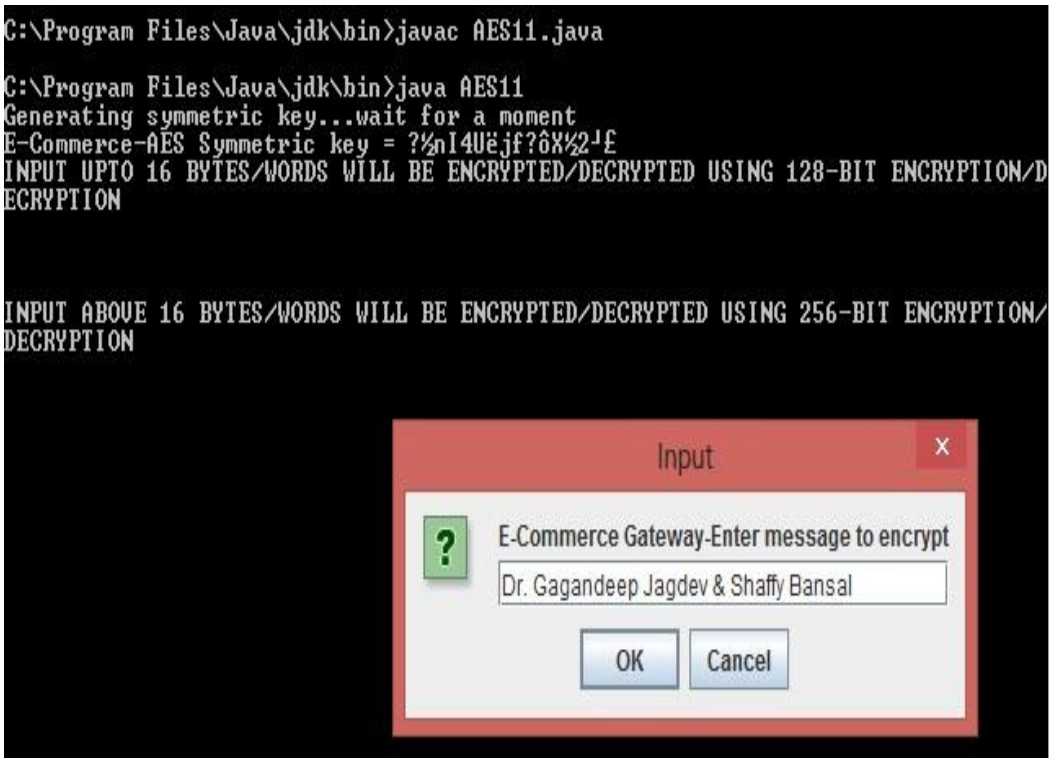

Fig5. *The figure shows the plain text to be encrypted using AES algorithm*

Fig. 6 shows the date and time of beginning of the encryption process and the encrypted text i.e. cipher text. The Fig. 4 also depicts the date and time at which the encryption process ended and displays the total time involved in the encryption process.

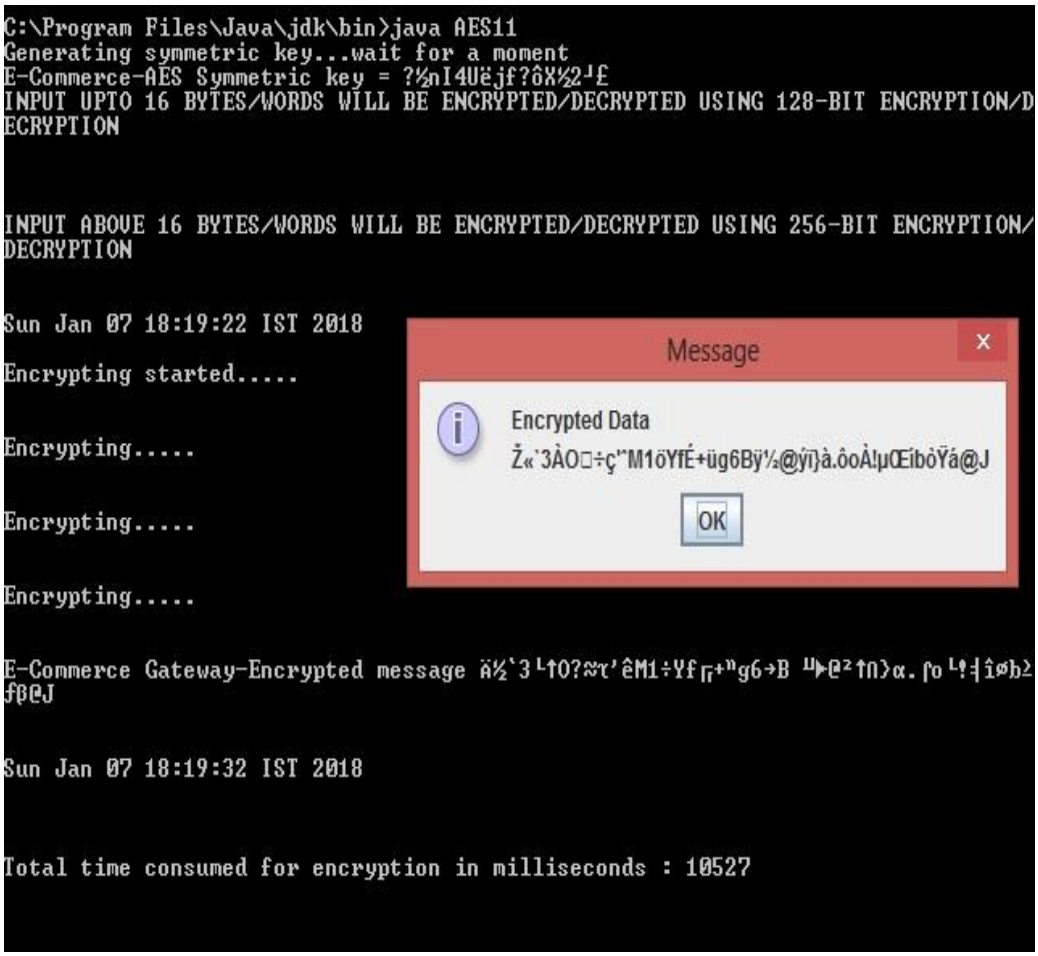

Fig6. *The figure depicts the encrypted text after the completion of encryption process*

Fig. 7 shows the choice to either terminate the operation (Press 1) or to initiate back the decryption process (Press 2). On initiating the decryption process, we get back the plain text from the cipher text after the application of appropriate key. The "Message Box" displays the plain text back.

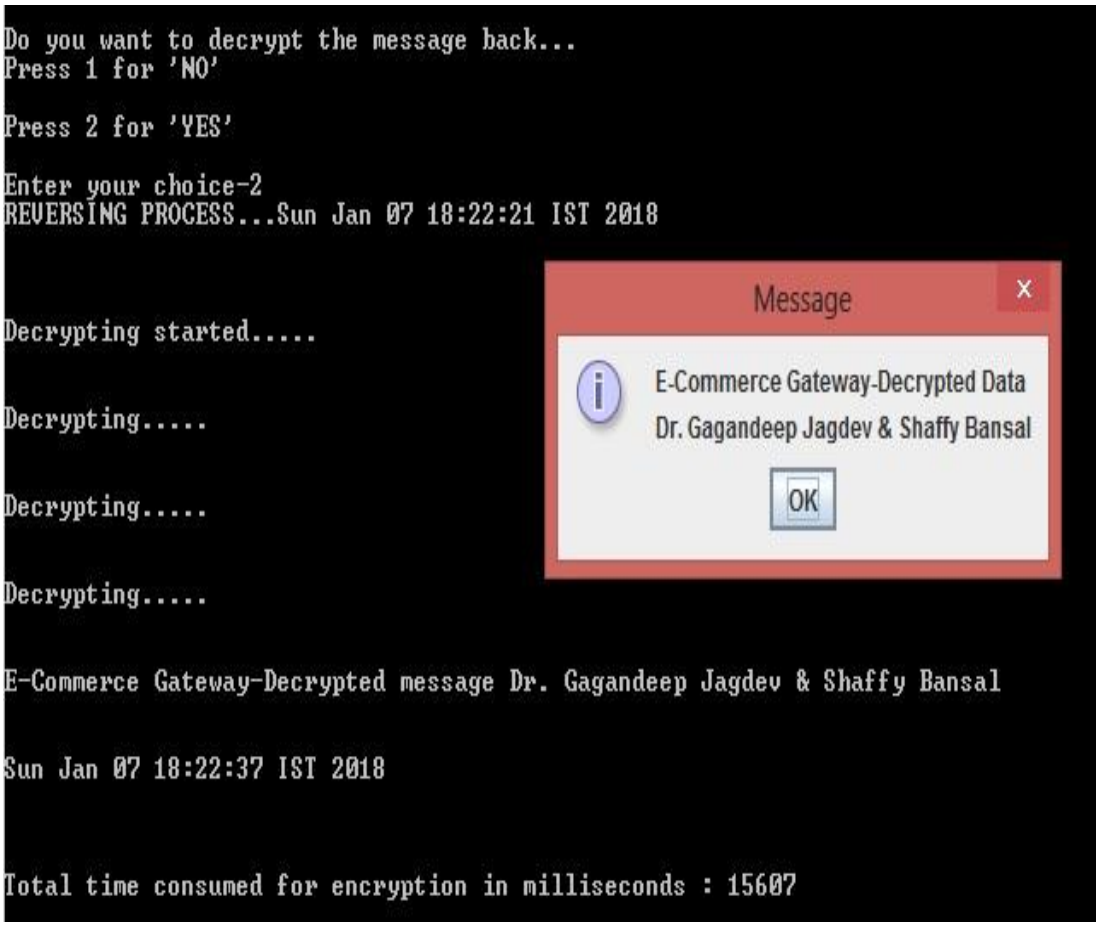

Fig7. *The figure shows the initiation of decryption and the decrypted message*

4. CONCLUSION

Cloud computing is a practice of offering set of resources or services to the users by the CSP (Cloud Service Providers) on their demand. The paper discussed the cryptographic algorithms which are responsible for keeping the messages secure by converting them into non-readable form. The implementation of AES algorithm using 256-bit key size further enhances the security level of the critical data been transferred via cloud.

REFERENCES

[1] Gagandeep Jagdev et al., "Implementation of DES and AES cryptographic algorithms in accordance with cloud computing", International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online),Volume 4, Issue 4, 2017, PP 1-14 DOI: http://dx.doi.org/10.20431/2349-4859.0404001.

[2] Akashdeep Bhardwaj, G.V.B. Subrahmanyam et al., "Security Algorithms for Cloud Computing", Elsevier, Procedia Computer Science, Volume 85, Pages 535-542.

[3] PriyadarshiniPatil et al., "A comprehensive Evaluation of Cryptographic Algorithms: DES,3DES, AES, RSA and Blowfish", 2015, Volume 78, 2016, Pages 617-624.

[4] AbidalrahmanMohd. et al.," AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation",7th International Conference on Information Assurance and Security, IAS 2011, Melacca, Malaysia, December 5-8, 2011.

[5] Gagandeep Jagdev et al., "Analyzing working of DES and AES algorithms in cloud security", International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)Volume 4, Issue 3, 2017, PP 1-9 DOI: http://dx.doi.org/ 10.20431 /2349-4859.0403001.

[6] Abhilasha CP et al., "Software Implementation of AES Encryption Algorithm", IJARCSSE, 2016.

[7] M.Meena et al., "A study and comparative analysis of cryptographic algorithms for various file formats.", IJSR, 2013, ISSN:2319-7064.

[8] Miss. Shakeeba et al., "Cloud Security using Multilevel Encryption Algorithms", IJARCCE, 2016, ISSN (online):2278-1021.

[9] Kumar Y., Munjal R. et al. "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures"**,** *IJAFRC*, Volume 1, Issue 6, June 2014.

[10] Pahal R., Kumar V., "Efficient Implementation of AES", IJARCSSE, Volume 3, Issue 7, July 2013.

[11] Aggarwal A., Singh G. et al., " Implementation of AES algorithm", *International Journal of Engineering Research & Science (IJOER),* Vol-2, Issue-4 April- 2016, pp. 112-116.

[12] Meena M.et al., "A study and comparative analysis of cryptographic algorithms for various file formats", *International Journal of Science and Research (IJSR)*, 2013, pp. 991 - 995.

[13] Shakeeba et al., "Cloud Security using Multilevel Encryption Algorithms", *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, Vol. 5, Issue 1, January 2016, pp. 70 – 75.

AUTHOR'S BIOGRAPHY

Dr. Gagandeep Jagdev, is a faculty member in Dept. of Computer Science, Punjabi University Guru Kashi College, Damdama Sahib (PB). His total teaching experience is above 11 years and has 122 international and national publications in reputed journals and conferences to his credit. He is also a member of editorial board of several international peer-reviewed journals and has been active Technical Program Committee member of several international and national conferences conducted by renowned universities and academic institutions. His field of expertise is Big Data, ANN, Biometrics, RFID, Cloud Computing, Cryptography, and VANETS.

Citation: *Shaffy Bansal & Dr. Gagandeep Jagdev (2018). Elaborating Security Algorithms in Cloud Environment, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 5(1), pp.1-8, DOI: http://dx.doi.org/10.20431/2349-4859.0501001*