IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

IMPLEMENTATION OF CRYPTOGRAPHY TECHNIQUES IN CLOUD COMPUTING

Shaffy Bansal[1*], Vijay Bhardwaj[2]

[1,2]Dept. Of Computer Applications, Guru Kashi University, Talwandi Sabo (PB), India

Available online at: www.ijcseonline.org

Accepted: 19/Oct/2018, Published: 31/Oct/2018

Abstract— Cloud computing is the set of IT services that are provided by cloud service provider to the users over the Internet. It is Pay-per-use for On-demand service. The main concern of the cloud computing is Security. In this paper, studies the basics of cloud computing and two main encryption/decryption algorithms that are AES (Advanced Encryption Standard) and DES (Data Encryption Standard). The paper shows the implementation of AES and DES algorithms for the conversion of Plaintext to Cipher text.

Keywords— AES, DES, cloud computing, issues, cryptography, plaintext, cipher text

I. INTRODUCTION

Cloud computing is the buzzword that means different things to different people. For some, it's just another way of describing IT (information technology) "outsourcing"; others use it to mean any computing service provided over the Internet or a similar network; and some define it as any bought-in computer service we use that sits outside your firewall. Cloud computing refers to the entire collection of software and hardware one uses which is placed at remote location. Such service provider's companies are referred as Cloud Service Providers (CSP) and often-huge giant companies provide these services. The Cloud computing is a transforming technology. The information and the processes are migrating to the cloud.

Cloud computing handles all the challenges faced by conventional computing including handling and installation of software. It is an on demand service and facilitates user to utilize services as and when required. The cloud computing is a pay as per use. User pays as per his/her requirements [2, 3, 4].

Fig1. Shows the cloud computing Environment

Suppose two friends who share crucial secret data ought to break up. Currently the matter that arises is that they need to speak with one another from way of a distance. This distance invitions hearer to prevent, intercept or interfere the communication between two friends so as to realize access to secret data. So, to avoid this, each the chums determined to lock their secret data in a box and also the key to unlocking that box is thought solely to them. So, once the first friend the latched box to the second, he/she unlocks it exploitation the secure combination key. This can be however cryptography works. Cryptography [1,2].

Cloud be a technique of storing and disguising crucial and secret data in a very cryptic kind in order that solely folks meant to browse it will have its access. The cryptography is conducted by changing plain text into cipher text via exploitation applicable security algorithms and afterward decipherment is conducted that is reverting the cipher text back to plain text.

Fig2. Shows the encryption/decryption process

A. ***Data Encryption Standard (DES)*** an early encoding normal supported by the U.S. National Bureau of Science. It is based on Feistel structure in which plaintext is divide in to two halves DES receives 64-bit plaintext and key of 56-bit to output. In DES, input is divided into halves, 32-bit as left portion and 32-bit as right portion.

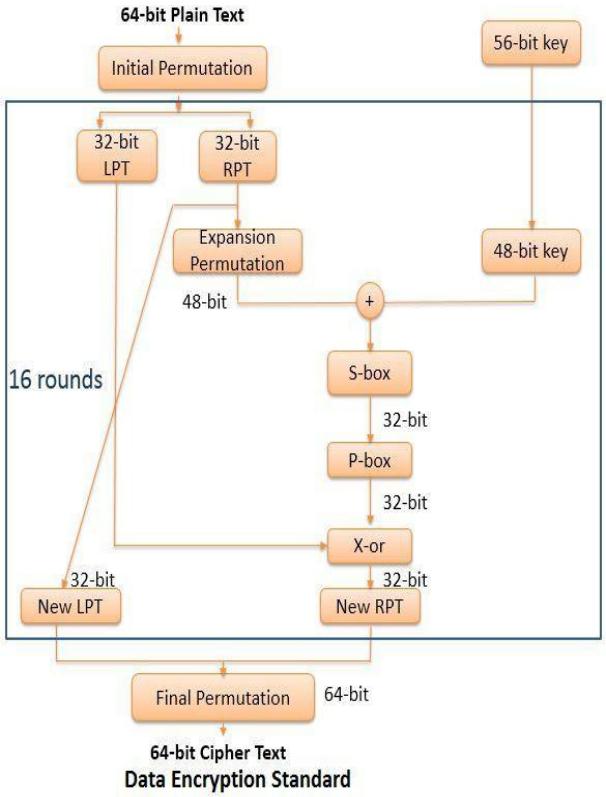

Fig3. Shows the DES algorithm

Each round contains the capacities said as under.

- The initial step is of expansion permutation in which 32-bit right part is extended to 48-bit right part.
- Next, the 48-bit right part is XORed with 48-bit sub key attained from the 56-bit key and results in 48-bit yield.
- The subsequent stage is of S-box where the got 48-bit is lessened to 32-bit once more.
- At long last the P-box activity is started where the 32-bit result got from S-box is permuted what's more, gives 32-bit permuted yield.

B. Advanced Encryption Standard is the Advanced encoding normal was revealed by the National Institute of Standards and technology in 2001. AES is that the algorithm program trustworthy because the normal by the U.S. Government and diverse organizations. Though it's extraordinarily economical in 128-bit type, AES conjointly uses keys of 192 and 256 bits cipher. Still, security specialists believe that AES can eventually be hailed the de facto normal for encrypting information within the personal sector. This algorithm program is spoken as AES-128, AES-192, and AES-256 depending on its key length. The cipher consists of N rounds wherever the amount of rounds depends on the key length: 10 rounds for a 16 computer memory unit key, 12 rounds for a 24 computer memory unit key and 14 rounds for a 32 computer memory unit key. AES permits a 128-bit information length, which will be split into four basic operational blocks.

- The sub bytes make utilization of S-confine which byte-by-byte substitution of whole matrix is performed.
- Shift rows shift the rows of the matrix.
- The columns of the matrix are shuffled from right to left.
- Next he XOR of the current block and the expanded key is performed.
- And the last 10^{th} round involves Sybbytes, Shift Rows, and Add round key only and provides 128-bit cipher text.

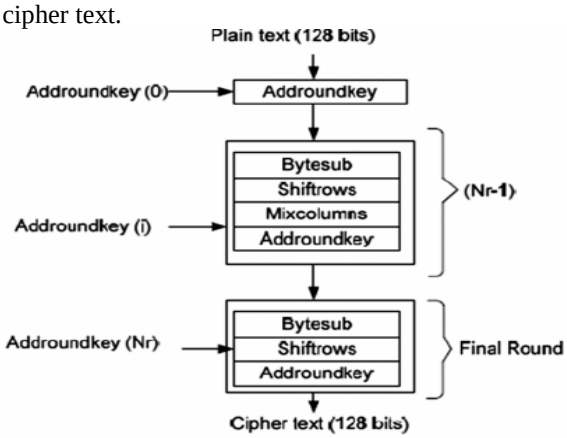

Fig4. Shows setup of AES algorithm

II. METHODOLOGY

A. ***Implementation of DES***

The implementation of DES algorithm is done in Java using Eclipse Java Oxygen 3.A. The snapshots below illustrate the implementation process step-by-step.

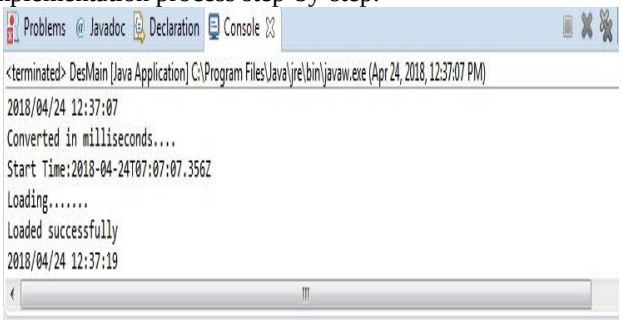

Fig5. Shows the start time of DES algorithm

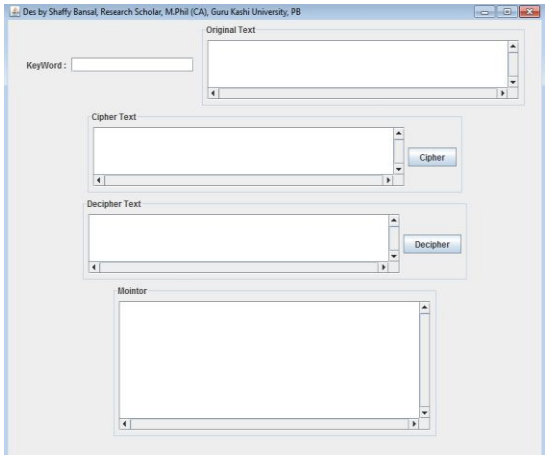

Fig6. shows the interface created for carrying out encryption/decryption as per DES algorithm

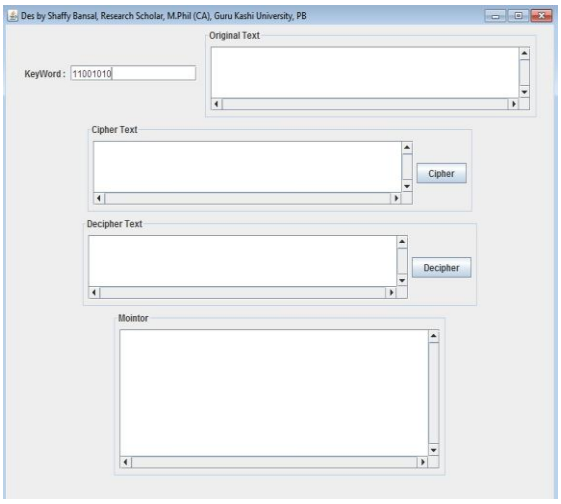

Fig7. Shows the interface having 8-bit keyword entered in the Keyword sub-section of the interface

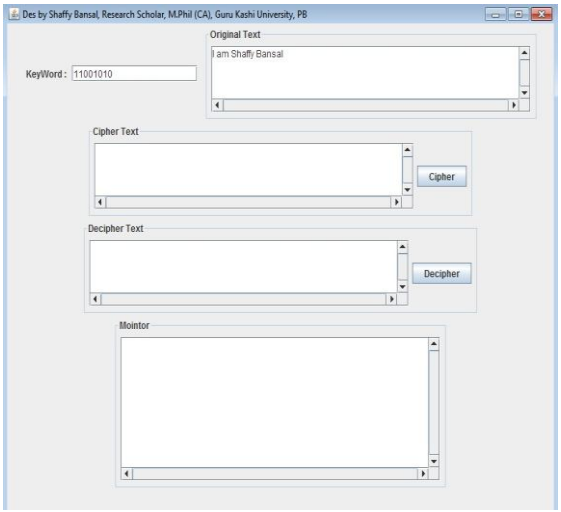

Fig8. Shows the text to be encrypted (plain text) been entered in the "Original Text" section of the interface

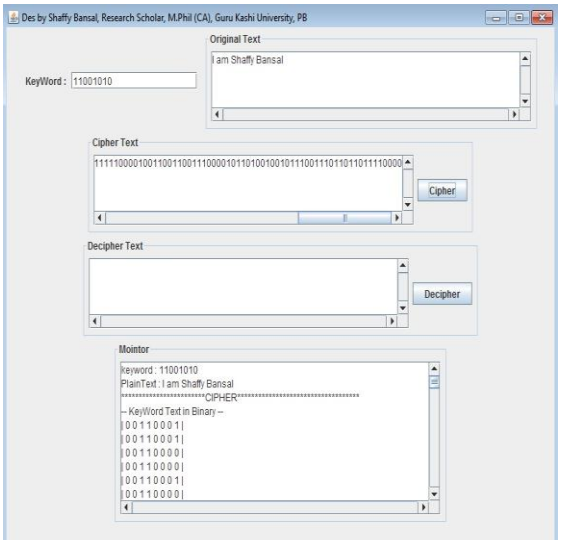

Fig.9 Shows the cipher text displayed under "Cipher Text" section of the interface

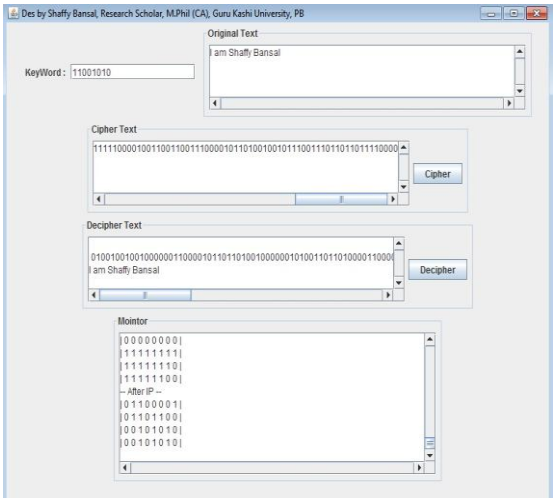

Fig10. Shows the obtained plain text back from cipher text under "Decipher Text" section, which is generated on pressing the "Decipher" button

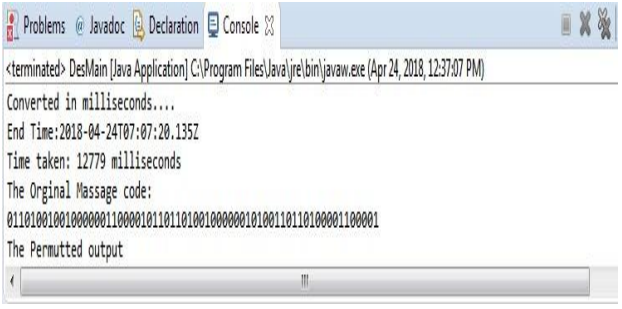

Fig11. Shows the total time elapsed in conducting encryption/decryption using DES Table

Table1. The table represents different cases run on DES

Sr. No.	Plain Text	No. of Bytes	No. of bits in cipher text	Time duration (Seconds)
1	Hello	5	64	12.809
2	ABCDEFGH	8	64	12.822
3	ABCDEFGHIJKL	12	128	13.310
4	SHAFFY BANSAL GK	16	128	13.878

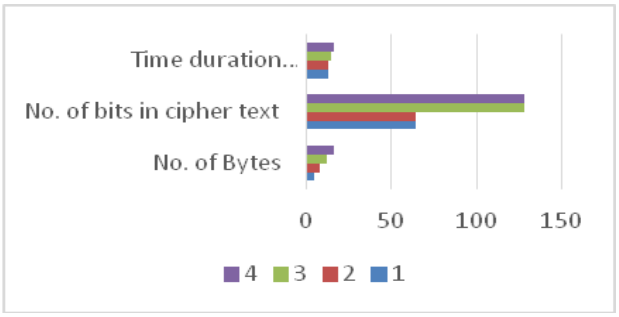

Fig12. Shows the graphical representation of data present in Table1

B. ***Implementation of AES***

The implementation of AES algorithm is done in Java using Eclipse Java Oxygen 3.A. The snapshots below illustrate the implementation process step-by-step.

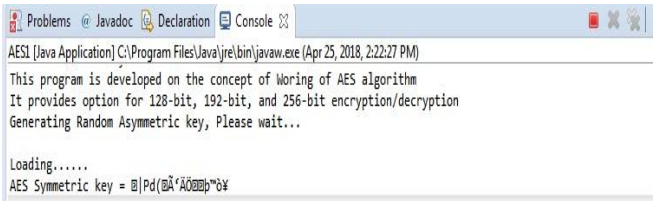

Fig13. Shows the date, time, and randomly generated AES symmetric key

Fig14. Shows the message displayed illustrating the amount of bytes in relevance with three different key encryptions

Fig15. displays the number of rounds the encryption/decryption process will undergo in each category

Fig16. Shows the message box meant for entering the plain text

Fig17. Shows the cipher text obtained from plain text

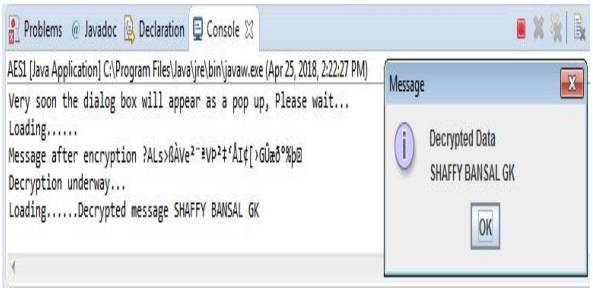

Fig18. Shows the decrypted message obtained from cipher text

III. RESULTS AND DISCUSSION

Table2. illustrates six different scenarios to be examined using AES encryption/decryption

Sr. No.	Plain Text Message	No. of Bytes	No. of Rounds	Time duration (seconds)
1	Shaffy	16	10	89.914

	Bansal GK			
2	Shaffy Ban	10	10	84.607
3	Shaffy Bansal GKU Talwan	24	12	123.388
4	Shaffy Bansal Mphil.	20	12	109.135
5	I am a student of Guru Kashi Uni	32	14	131.612
6	Guru Kashi University T Sabo PB	30	14	127.185

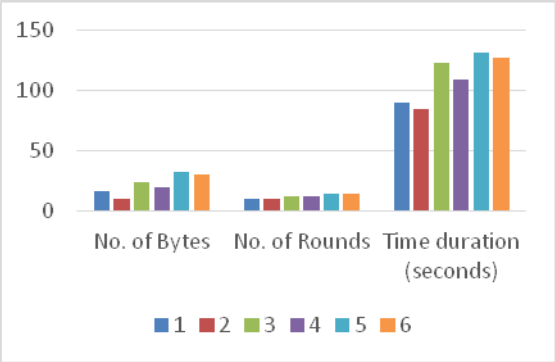

Fig19. Displays the graphical results obtained from data in

IV. CONCLUSION

The research work analyzed Symmetric algorithms for different encryption and encoding techniques. The research work discussed the cryptographic algorithms, which are responsible for keeping the messages secure by converting them into non-readable form. The implementation of AES algorithm increases the security level of the crucial data been transferred through the cloud using 256-bit key size. The research work found AES to be a good candidate for key encryption.

V. FUTURE WORK

In future, the stress should be laid on implementation and development of dynamic and flexible alternatives that can be used by enterprises with full confidence and trust and preferably such software's should be available at low cost.

REFERENCES

[1]. Kevin Hamlen et al.; (April-June 2010) International Journal of Information Security and Privacy, 4 (2), 39-51, April-June 2010 39,"Security issues for Cloud Computing".

[2]. Rabi Prasad Padhy et al. (December 2011) IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, "Cloud Computing: Security issues and Challenges".

[3]. Manpreet Kaur et al. (June 2015), International Journal of Advances in Engineering & Technology, June 2015, © IJAET ISSN: 22311963," A Review of Cloud Computing Security Issues".

[4]. Leena Khanna, Anant Jaiswal, "Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them", IJARCSSE 2013.

.

