International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 5, Issue 1, 2018, PP 17-25
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
DOI: http://dx.doi.org/10.20431/2349-4859.0501003
www.arcjournals.org

Comparative Analysis and Implementation of Cryptographic Algorithms in Cloud Computing

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: *Cloud computing is the outsourcing of communications relevant to IT sector via the use of the internet and maintaining own software and hardware environment. It is an on-demand service facilitated by CSP (Cloud Service Provider). It is available whenever one need it, as much he/she need, and one pays for what he/she use. Security factor is a primary concern of cloud environment. In this research paper along with discussing the basics of cloud computing and the threats involved in a cloud environment, the two main algorithms of cryptography, DES (Data Encryption Standard) and AES (Advanced Encryption Standard) has been elaborated with their individual practical implementation detailing the conversion of plain text to cipher text and vice versa.*

Keywords: *AES, attacks, cipher text, cryptography, cloud computing, DES, plain text*

Abbreviations: *AES, BFA, COA, CSP, CPA, DES, KPA, MIM, SCA*

1. INTRODUCTION

The practice of delivering computing services over the internet is referred as cloud computing. Cloud enables users to make use of such software's and hardware's that are managed by third parties at faraway location. It includes accessing social networking sites, online business applications, online file storage, and webmail services. Cloud environment provides shared pool of resources, comprising of networks, computer processing power, user applications, specialized corporate, data storage space and much more [1, 2, 13]. Cloud computing is an on-demand network access that can be quickly provisioned and could be conveniently released with insignificant management effort or interaction with service providers. It is because of all these provisions that every organization is willing to move their data to the cloud. Fig. 1 shows the setup of cloud environment.

Fig1. *The figure depicts the setup for cloud computing*

The effective use of cloud computing brings up the need to protect the data against any kind of unauthorized access, denial of service, or modification. Securing the cloud means to secure the

calculations and databases which are hosted by individual CSP's (Cloud Service Providers). The three objectives of the security goals are to ensure availability, integrity, and confidentiality of the cloud data. The confidentiality factor is handled by cryptography [3, 12].

The art and science of constructing a cryptosystem that ensures the security of information is known as cryptography. It actually deals with securing the digital data as shown in Fig. 2. Today cryptography is based on multiple concepts of mathematics like probability theory, computational-complexity theory, and number theory. It works on binary bit sequences. It trusts on publicly known mathematical algorithms for coding the information. A secret key is used to obtain the secrecy which acts as a seed for the algorithms. Because of the computational difficulty of the used algorithm and presence of a secret key, it becomes difficult for an unauthorized person to gain original information despite him/her knowing the used algorithm [4, 5].

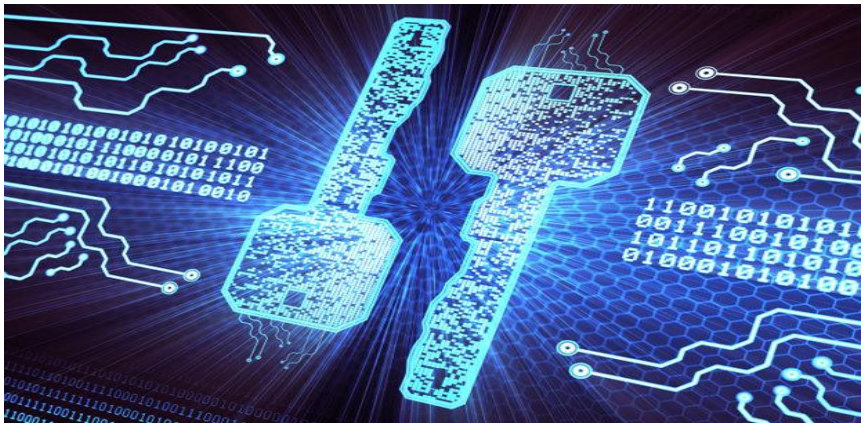

Fig2. *The figure depicts the use of cryptography (public and private keys) in digital world*

2. ATTACKS INVOLVED IN CRYPTOSYSTEMS

Today every aspect of human life is driven by information. It has turned out to be domineering to protect useful information from unauthorized attacks [1, 6]. These attacks can be broadly classified into two categories: Passive attacks and Active attacks.

Passive Attacks

Passive attacks are concerned with gaining unauthorized access to the information. For instance, eavesdropping and intercepting are kind of passive attacks. Passive attacks are silent attacks which neither interrupt the communication channel nor affect information. It is basically about stealing the information. The difference between stealing goods and information is that in case of information the owner still possesses the stolen data. These kinds of thefts often goes unnoticed.

Active Attacks

Active attacks change the information by steering some kind of unauthorized process on the information. It may be unauthorized deletion of data, unapproved modification of information, alteration of authenticated data, and denial of access to authorized users.

Different attacks on cryptosystems are mentioned as under [5, 11].

Cipher Only Attacks (COA) – In this attack the hacker is in possession of cipher text but has no access to plaintext. This is said to be successful only when matching plaintext can be extracted from the cipher text. Infrequently, the encryption key can be obtained via this attack. However, modern cryptography guards against such attack.

Known Plaintext Attack (KPA) – In this attack, the hacker has knowledge of plain text for some parts of the cipher text. The objective is to decrypt the rest of the cipher text. For instance, linear cryptanalysis against block cipher.

Chosen Plaintext Attack (CPA) – In this attack, the hacker is in access of cipher text-plaintext pair of his choice. Hence the job of determining the encryption key is simplified. For instance, differential cryptanalysis against block cipher.

Dictionary Attack – In this attack, the hacker cashes on his/her experience to build a dictionary of plaintexts and corresponding cipher texts which he/she has gained over a period of time. The hacker refers to this dictionary whenever he/she needs to obtain plain text from a cipher text.

Brute Force Attack (BFA) – In this attack, the hacker attempts to find out the key by attempting all possible keys. If the key under consideration is 8 bits long, then the total number of possible keys is 256. The hacker is already in possession of cipher text and knows the applied algorithm, so he/she attempts all 256 keys for decryption. The longer is the key, more is the time required to complete the process.

Man in Middle Attack(MIM) – In this attack, the key exchange takes place before the actual communication begins. The communication is initiated between node A and node B, so in accordance with this node A requests public key of node B. But on the way over insecure channels, the hacker intercepts the request and sends his/her public key instead. Because of this, the hacker is able to read whatever node A sends to node B. In order to avoid the breakage in communication, the hacker re-encrypts the data after reading his/her public key and sends it to node B. The node B takes this key as if it is the original key send from node A, which actually is not.

Side Channel Attack (SCA) – This attack exploits the weakness in the physical execution of the cryptosystem.

Timing Attacks–These attacks make use of the detail that different computations take different times to calculate on processor. This gives an idea about a particular computation the processor is carrying out. For instance, if encryption is taking more time, it directs that the secret key is long.

Power Analysis Attacks – This attack is very similar to the timing attacks except that the power consumed is utilized to attain information regarding the nature of the computations under consideration.

3. CONTRIBUTION AND IMPLEMENTATION

The DES (Data Encryption Standard) is based on the Feistel structure in which the plaintext is divided into two halves. The DES receives 64-bit plain text as input and key of 56-bit to output cipher text of 64-bit. Firstly the 64-bit plaintext experiences initial permutation and rearranges the bits to get 64-bit permuted input. This 64-bit permuted input is divided into two halves, 32-bit as left portion and 32-bit as right portion. These two portions undergo sixteen rounds each where each round follows the same functions. As the sixteen rounds are completed and the final permutation is completed, the 64-bit cipher text is obtainedas shown in Fig. 3 [1, 7, 9].

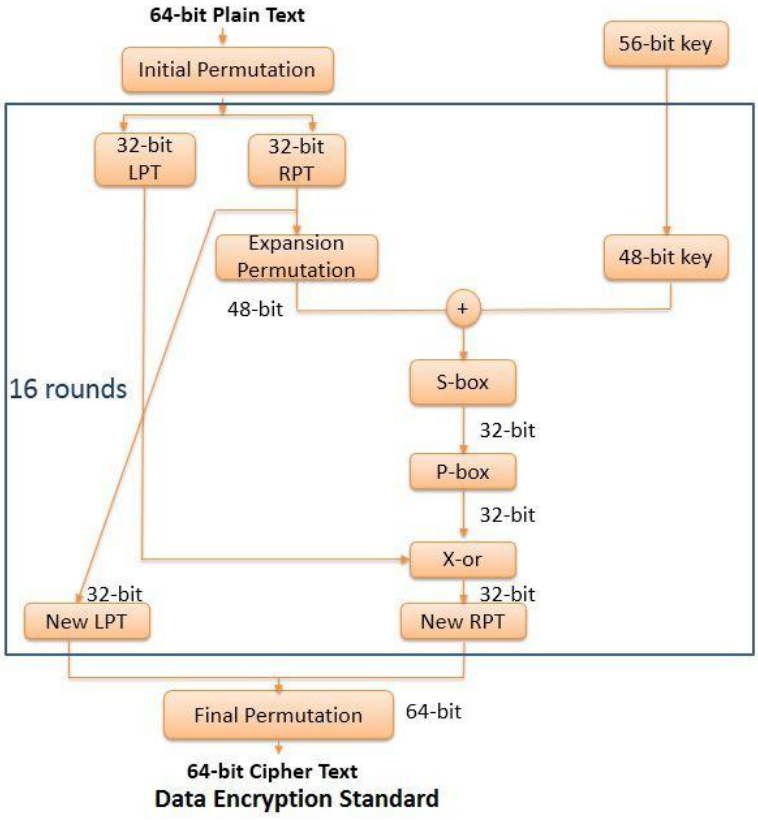

Fig3. *The figure shows the detailed set up of DES algorithm*

Each round comprises of the functions mentioned as under.

- The first step is of *expansion permutation* in which 32-bit right portion is lengthened to 48-bit right portion.
- Next, the 48-bit right portion is *XORed* with 48-bit subkey attained from the 56-bit key and results in 48-bit output.
- The next step is of *S-box* where the obtained 48-bit is reduced to 32-bit again.
- Finally the *P-box* operation is initiated where the 32-bit result derived from S-box is permuted and gives 32-bit permuted output.

AES (Advanced Encryption Standard) algorithm takes 128-bit plaintext along with 128-bit secret key as input, which together forms a 128-bit block depicted as 4 * 4 square matrix. This matrix undergoes initial transformation followed by ten rounds among which nine rounds involve below mentioned stages [1, 5, 8] and in Fig. 4.

- The sub bytes make use of S-box in which byte by byte substitution of entire matrix is performed.
- Shift rows shift the rows of the matrix.
- Thereafter the columns of the matrix are shuffled from right to left.
- Next the XOR of the current block and the expanded key is performed.
- And the last 10th round involves Subbytes, Shift Rows, and Add round key stages only and provides 16 bytes (128-bit) ciphertext.

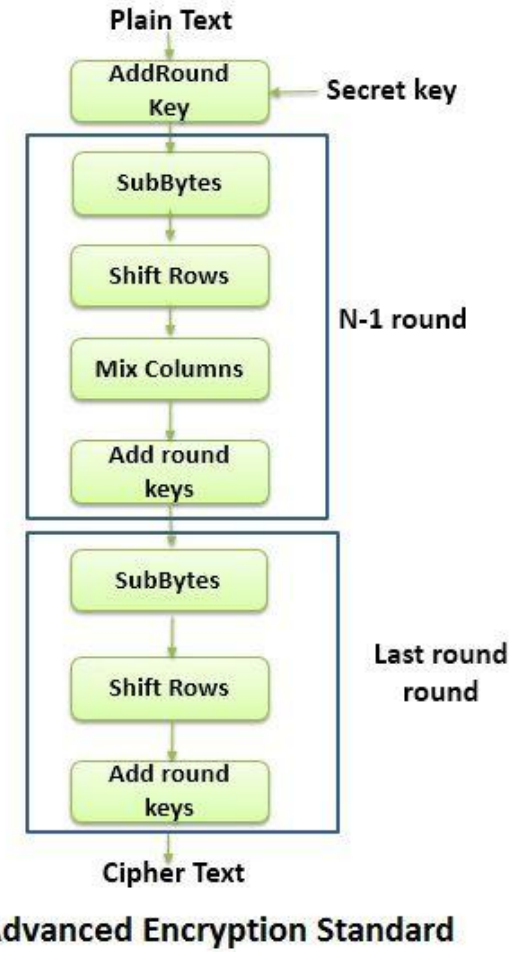

Fig4. *The figure shows the detailed set up of the AES algorithm*

The research work shows the practical implementation of the two prominent cryptography algorithms DES (Data Encryption Standard) and AES (Advanced Encryption Standard). The Fig. 5to Fig. 8shows the coded framework built for conducting the encryption/decryption as per DES algorithm [9].

Fig. 5 depicts the 8-bits entered keyword in the textbox titled “KeyWord”.

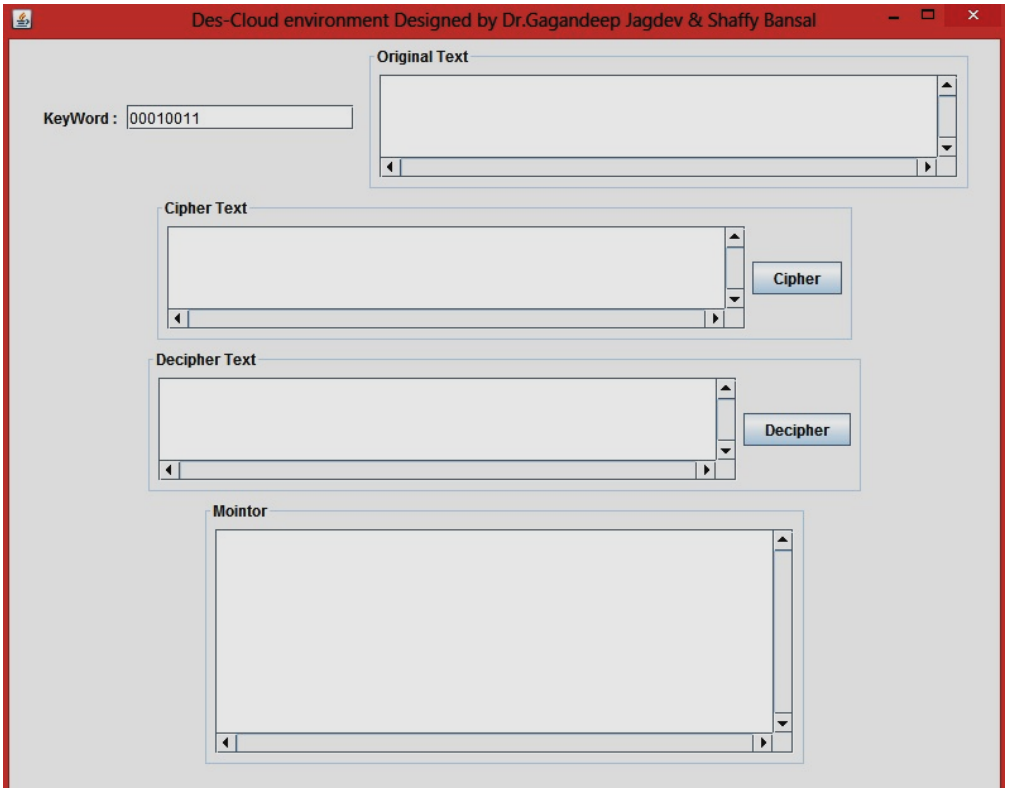

Fig5. *The figure shows the 8-bits keyword entered in the “Key Word” textbox.*

The Fig. 6 shows the plain text to be encrypted been entered in the “Original Text” textbox.

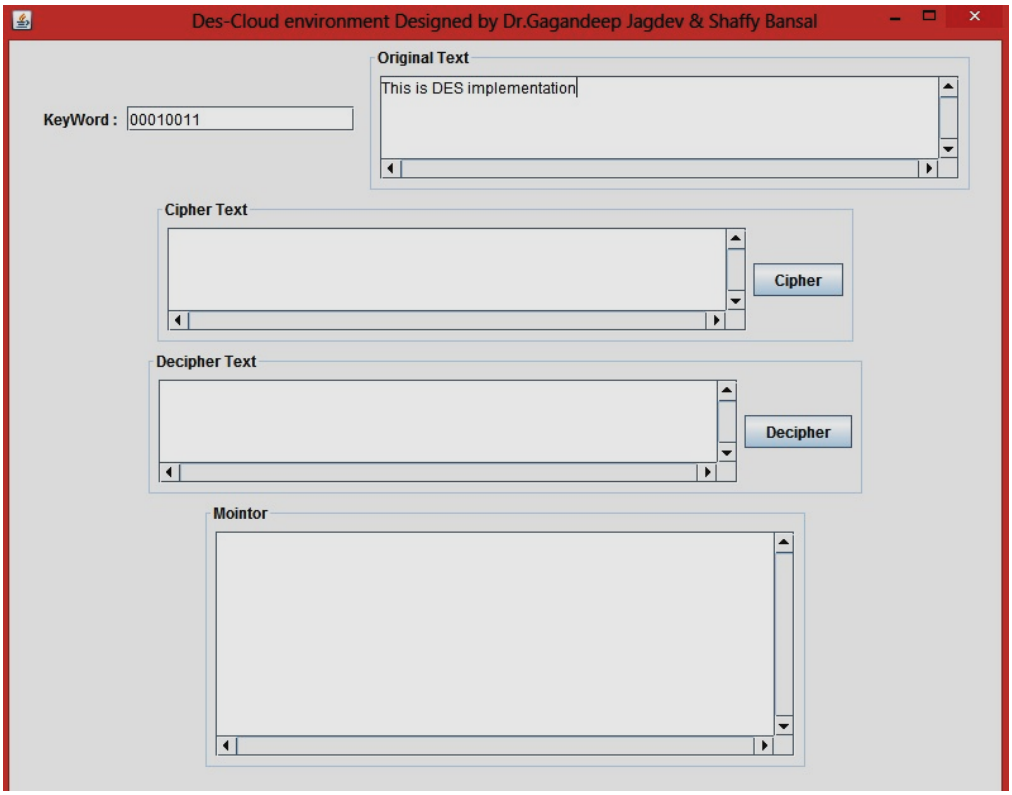

Fig6. *The figure shows the entered plain text in the “Original Text” section*

On pressing the “Cipher” button, the encryption process starts and the entered plain text changes to cipher text as per DES algorithm. This conversion is shown in Fig. 7. The “Monitor” section depicts the entire process which is carried out to convert plain text into cipher text according to DES algorithm.

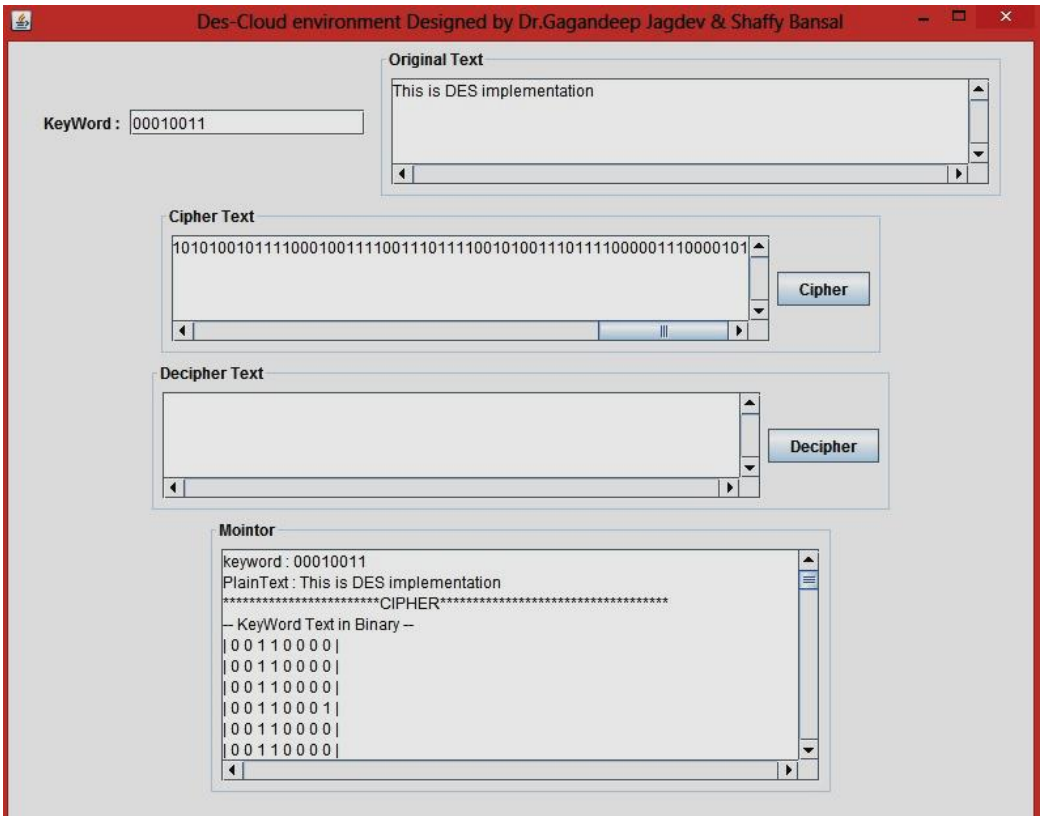

Fig7. *The figure shows the converted plain text into cipher text and also depicts the operation carried out in the "Monitor" section*

On pressing the "Decipher" button the entire process is reversed and the cipher text changes back to plain text as shown in Fig. 8.

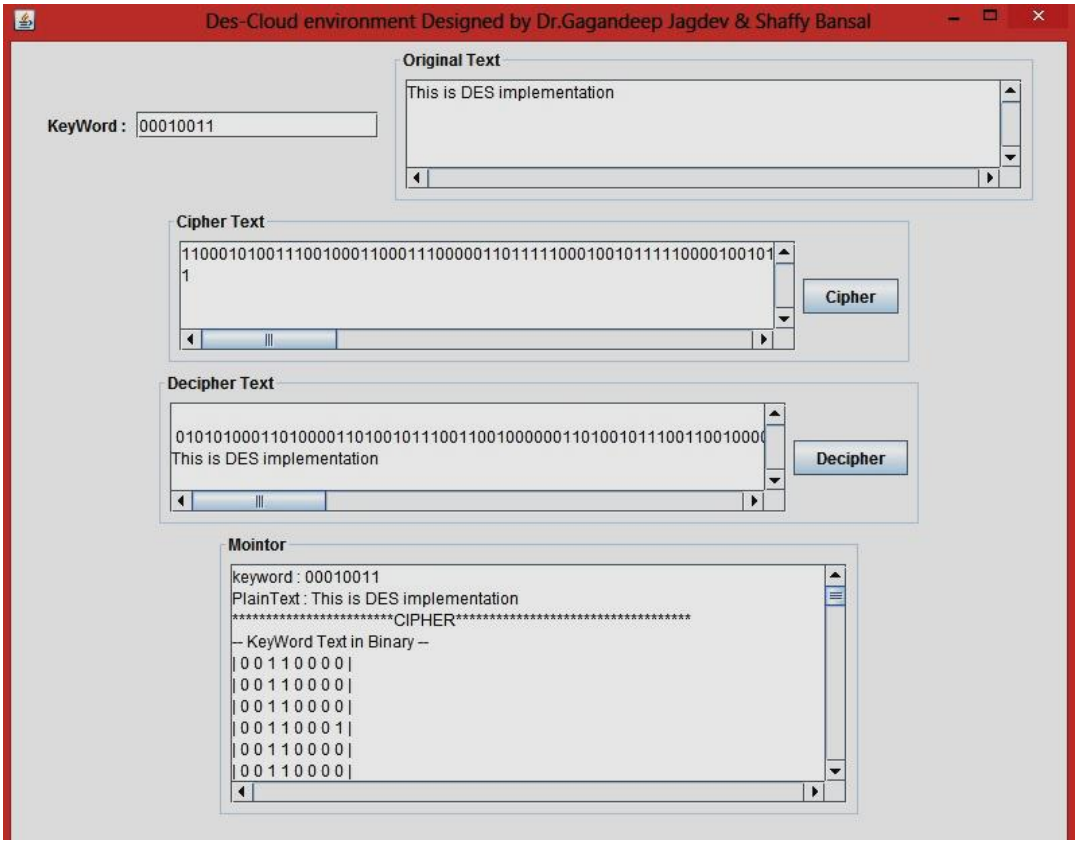

Fig8. *The figure shows the reverse operation converting back cipher text to plain text*

The Fig. 9 shows the 16-bit keyword entered in the "Key Word" section of the AES implementation.

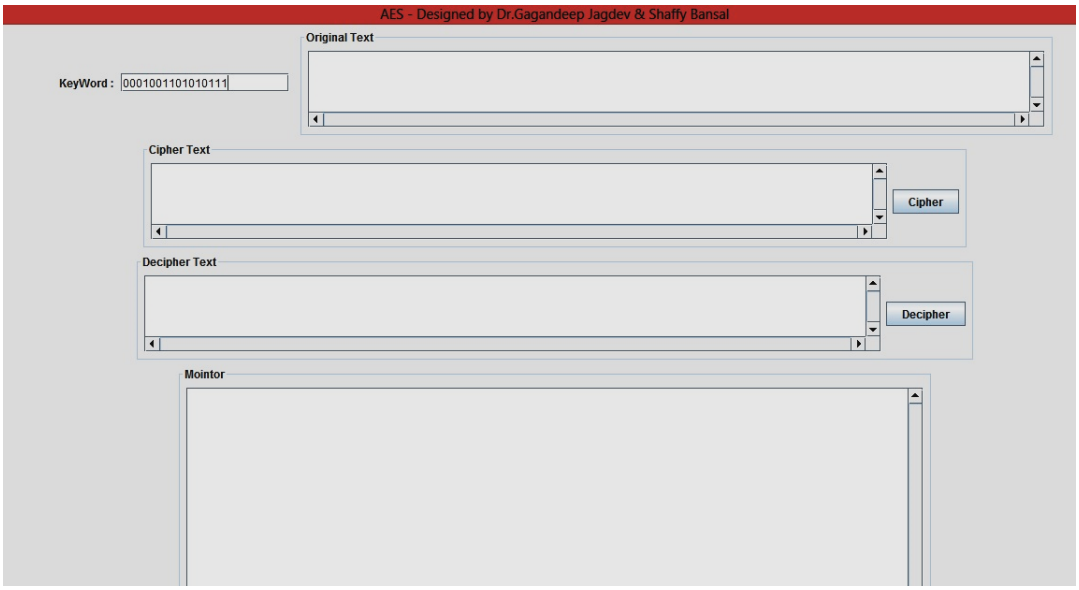

Fig9. *The figure shows the 16-bit key entered in the "Keyword" section*

Fig. 10 shows the plain text entered in the "Original Text" section of the coded set up.

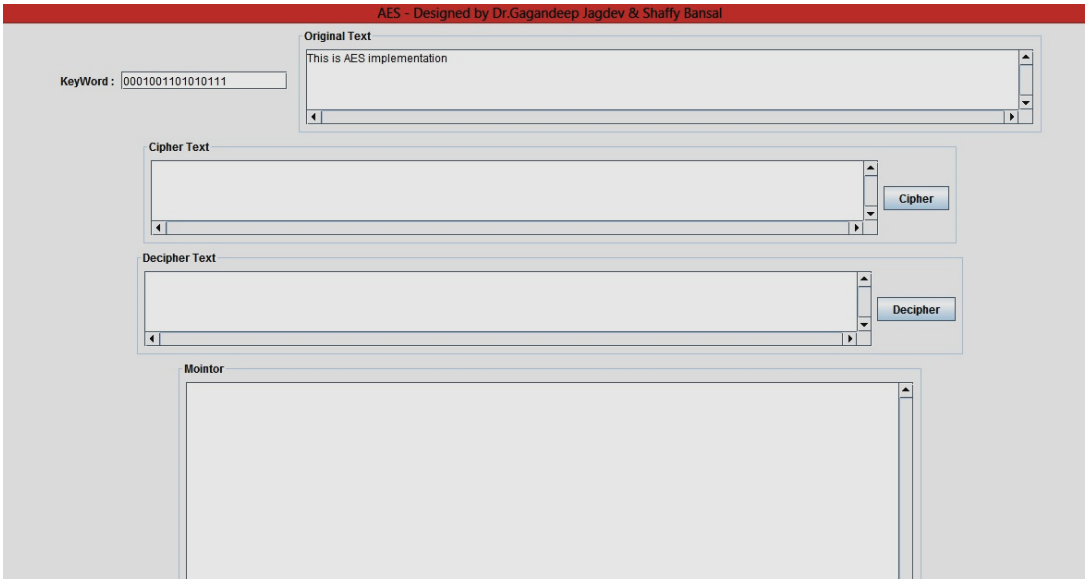

Fig10. *The figure shows the entered text in the "Original Text" section of the AES set up*

On pressing the "Cipher" button the plain text gets converted into the cipher text as displayed in "Cipher Text" section of Fig. 11.

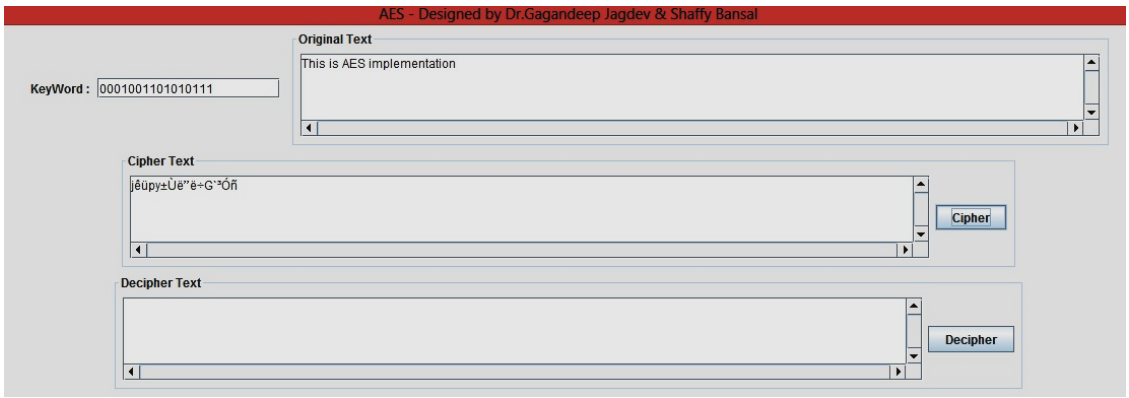

Fig11. *The figure shows the converted plain text into cipher text displayed in "Cipher Text" section*

Fig. 12 shows the operations being carried out during conversion from plain text to cipher text in the "Monitor" section.

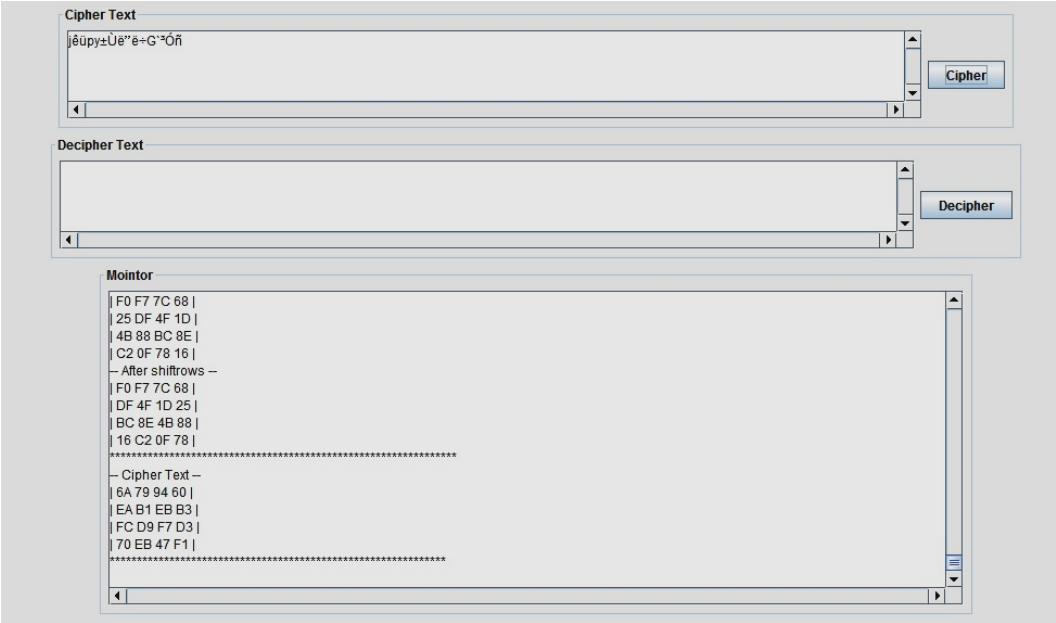

Fig12. *The figure displays the operation carried out in converting plain text to cipher text in "Monitor" section*

On pressing the "Decipher" button, the entire process is reversed and the cipher text is converted back into plain text as shown in Fig. 13.

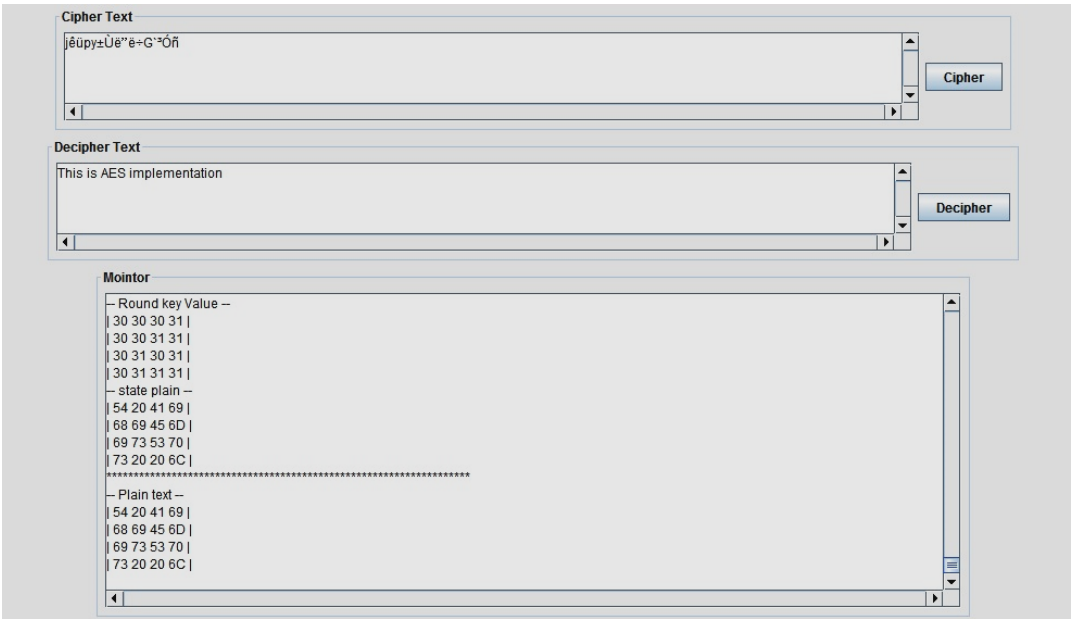

Fig13. *The figure shows the deciphered text displayed in "Decipher Text" obtained from plain text*

4. CONCLUSION

The research paper elaborated the working of two main cryptographic algorithms involved in data security when it travels on insecure channels. The implementation of DES and AES has been shown in the research paper via developing a set up coded in Java. The major differences between DES and AES is illustrated in Table 1 below [1, 10].

Table1. *The Table displays the difference between DES and AES algorithms*

COMPARISON FACTOR	DES (DATA ENCRYPTION STANDARD)	AES (ADVANCED ENCRYPTION STANDARD)
Basic	In DES the data block is divided into two halves.	In AES the entire data block is processed as a single matrix.
Principle	DES work on Feistel Cipher structure.	AES works on Substitution and Permutation Principle.
Plaintext	Plaintext is of 64 bits	Plaintext can be of 128,192, or 256 bits
Key size	DES in comparison to AES has smaller key size.	AES has larger key size as compared to DES.

Rounds	16 rounds	10 rounds for 128-bit algo 12 rounds for 192-bit algo 14 rounds for 256-bit algo
Rounds Names	Expansion Permutation, Xor, S-box, P-box, Xor and Swap.	Subbytes, Shiftrows, Mix columns, Addroundkeys.
Security	DES has a smaller key which is less secure.	AES has large secret key comparatively hence, more secure.
Speed	DES is comparatively slower.	AES is faster.

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). Comparative Analysis and Implementation of Cryptographic Algorithms in Cloud Computing, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 5(1), pp.17-25, DOI: http://dx.doi.org/10.20431/2349-4859.0501003*