**International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)**
*Volume 4, Issue 3, 2017, PP 1-9*
*ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)*
*DOI: http://dx.doi.org/10.20431/2349-4859.0403001*
*www.arcjournals.org*

# Analyzing Working of DES and AES Algorithms in Cloud Security

**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)*

**Abstract:** *Cloud computing security has been a fast-growing service which has many features similar to traditional IT security. It comprises of practices like protecting critical information from theft, data deletion, and data leakage. The biggest advantage of cloud services is that one can operate at scale and still remain secure. Cloud security provides new ways of delivering security solutions that address new areas of concern. It provides the users the comfort to perform security-related activities in more agile manner. The central theme of this research paper is to elaborate how secure is the one's data placed on cloud and what are the different security issues one should be concerned about when making use of the cloud. The paper also discusses the functioning and working of two symmetric algorithms, Data Encryption Standard (DES) and Advanced Encryption Standard (AES), responsible for providing cryptography in cloud security.*

**Keywords:** *AES, DES, cryptography, plain text, cipher text.*

**Abbreviations:** *AES, DES*

## 1. INTRODUCTION

Suppose two friends who share critical secret information have to split up. Now the problem that arises is that they have to communicate with each other from far of a distance. This distance invites eavesdropper to stop, intercept or interfere the communication between two friends in order to gain access to secret information. So, to avoid this, both the friends decided to lock their secret information in a box and the key to unlocking that box is known only to them. So, when first friend the locked box to the second, he/she unlocks it using the secure combination key. This is how cryptography works. Cryptography is a method of storing and disguising critical and secret information in a cryptic form so that only people intended to read it can have its access. The encryption is conducted by converting plain text into cipher text via using appropriate security algorithms and later on decryption is conducted which is reverting the cipher text back into plain text [7]. Cryptography provides with the features mentioned as under.

- *Data Integrity*: Data integrity means that information is valuable only if it is correct. It is concerned with maintaining and assuring the consistency of information.
- *Authentication*: Authentication refers to determining whether someone is in fact what he/she is declared to be.
- *Non-Repudiation*: It refers to the assurance that a party or an individual cannot deny the authenticity of his/her signature and send a message that they originated.
- *Confidentiality*: It relates to theft, unauthorized access and loss of privacy.

It is because of this cryptography that cloud is more secure as compared to traditional security systems. The difference between cloud computing security and traditional security system is mentioned in Table 1.

**Table1.** *Difference between Traditional security system and Cloud Security System*

| Traditional security system | Cloud security |
|---|---|
| In-house data centers | Third-party data centers |
| High upfront costs | Low upfront infrastructure investments |
| Slow scaling | Quickly scalable |
| Lower efficiency | Efficient resource utilization |
| Longer time to market | Reduced time to market |
| Higher cost | Usage-based cost |

## 2. SECURITY ISSUES IN CLOUD COMPUTING

The prominent security issues encountered in cloud computing are discussed as under [6, 12].

- **Data Breaches**

Cloud too faces the same threats as conventional networks used to face. But because of the huge amount of data stored in the cloud, the security concerns become an attractive subject and needs to deal very seriously. The impact of the damage depends upon the sensitivity of the data. Breaches related to health information, trade and intellectual property often prove to be more devastating. Whenever data breach takes place, companies have to incur heavy fines and even face lawsuits. Indirect impacts like loss of goodwill can have long-term impacts.

- **Compromised Credentials and Broken Authentication**

A data breach occurs because of weak passwords, poor certificate management and not enough strong keys. Organizations often allocate special permissions to their employees for performing tasks assigned to them. But these organizations often forget to change these passwords when employees leave the company. Authentication systems like OTP, phone-based authentication, and smartcards make it difficult for hackers to log in with stolen passwords. Many programmers often commit a mistake of writing credentials and cryptographic keys in the source code itself. Keys need to be well protected and it is advisable to change these security keys periodically. Also, centralizing identity into a single repository has its own risks.

- **Hacked Interfaces and Apis**

APIs are offered by every cloud service today. The security of cloud services depends upon the security of API. Weak APIs and interfaces expose organizations to security issues like integrity, availability, confidentiality, and accountability. APIs are most vulnerable because these are accessible from the open internet.

- **Account Hijacking**

Attackers can eavesdrop on activities, modify data and manipulate transactions via cloud services. Many attacks can be launched by using cloud application. Organizations should deny the sharing of account credentials between users and services.

- **Malicious Insiders**

The insiders refer to the current or former employees of an organization. Any corrupt employee in the cloud environment can destroy the whole infrastructure and manipulate data. Organizations should control the entire encryption process. Effective monitoring and auditing administrator activities need to be done essentially. Appropriate training is a critical factor for management to avoid mistakes.

- **Permanent Data Loss**

As the cloud computing has been in existence since many years now, it has matured to a very strong and robust technology. Today the reports of permanent data loss because of provider error is very rare. But still malicious hackers are in a continuous attempt to permanently delete data on the cloud to harm businesses and moreover, cloud data centers are as vulnerable to natural calamities as any other facility. To ensure the safety of critical data, cloud providers always recommends distribution of data and applications among multiple zones. Off-line storage and daily data backup are very important in cloud environments. Every time the burden of preventing data loss is not of cloud service provider. Suppose a customer encrypts his/her data before uploading it to the cloud, then it is the sole

responsibility of the customer to protect his/her encryption key. If a key is lost, so is the data. Cloud service providers also need to take care of compliance policies like how long organizations must retain audit records and other relevant documents.

## 3. Symmetric Algorithms Used For Cryptography in Cloud Computing

### A. Data Encryption Standard (Des)

The Data Encryption Standard (DES) is a symmetric-key block cipher proposed by National Institute of Standards and Technology (NIST). DES is constructed by implementing Feistel Cipher [11]. It makes use of 16 round Feistel structure and its block size is 64-bit. Although the key length of DES is 64-bit, 8 of the 4 bits are not used by the encryption algorithm and effective key length reduces to 56 bits [1, 4]. The general structure of DES is shown in Figure 1.

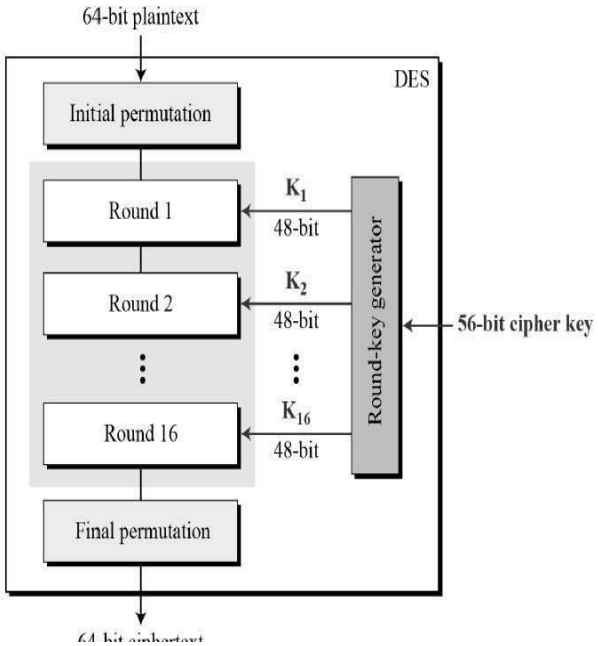


**Figure1.** *Working of DES*

***Initial and Final Permutation***

The initial and final permutations are straight permutation boxes (P=boxes) and are reverse of each other. Cryptography is not significant in DES. Figure 2 shows initial and final permutations as under.

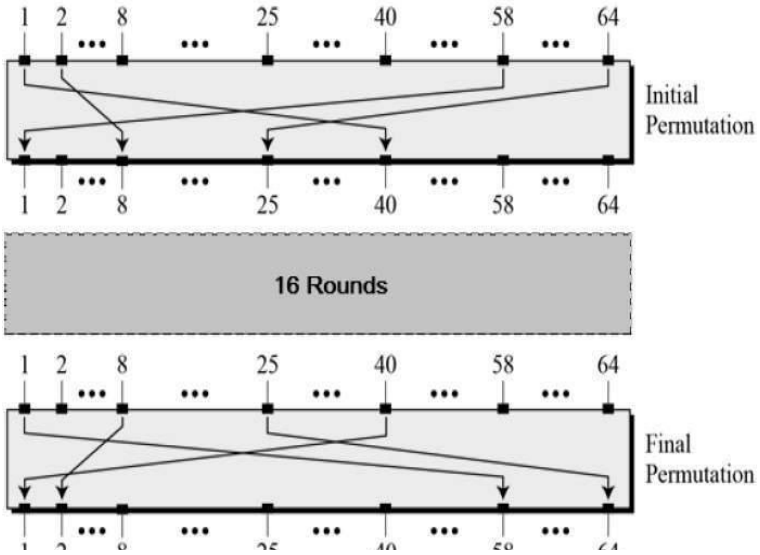


**Figure2.** *Initial and final permutations*

### *Round Function*

Here DES function (f) plays its role. The function applies 48-bit key to rightmost 32 bits to get an output of 32-bit as depicted in Figure 3.

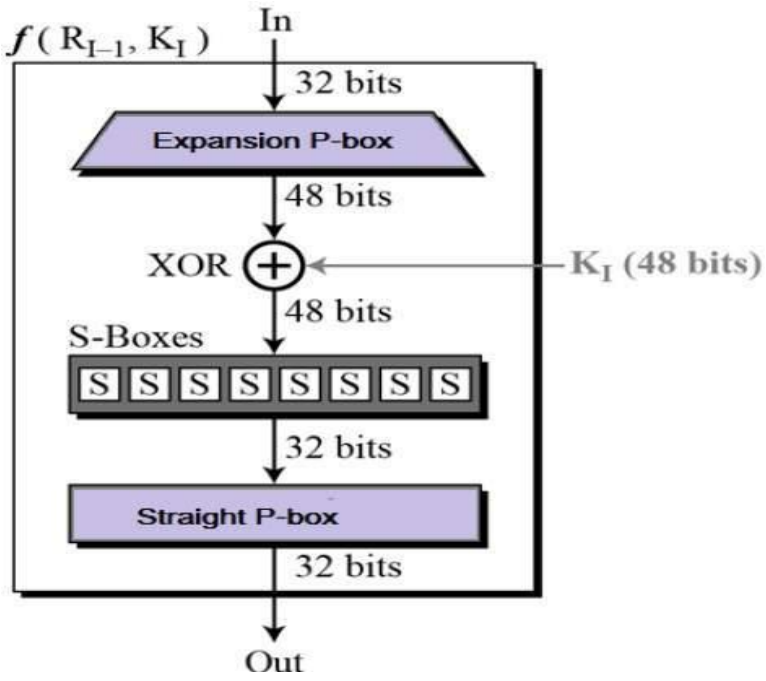


**Figure3.** *Working of Round Function*

### *Expansion Permutation Box*

Since the right input is 32-bit and the length of round key is 48-bit, there is need to expand right input to 48 bits as shown in Figure 4.

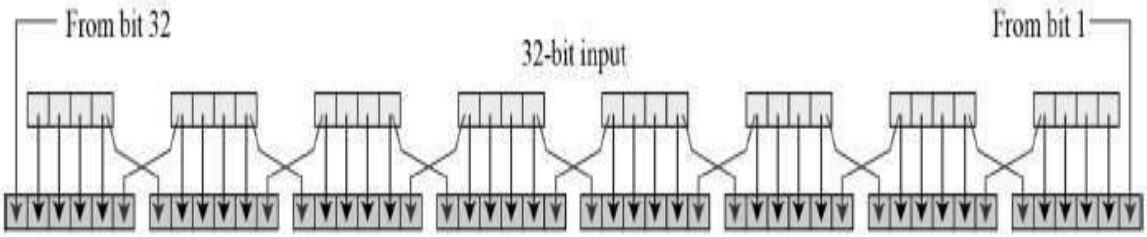


**Figure4.** *Expansion of right input of 32-bits to 48-bits*

The graphically depicted permutation logic is described as DES table as shown in Table 2.

**Table2.** *DES table*

| | | | | | |
|---|---|---|---|---|---|
| 32 | 01 | 02 | 03 | 04 | 05 |
| 04 | 05 | 06 | 07 | 08 | 09 |
| 08 | 09 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 31 | 31 | 32 | 01 |

### *XOR (Whitener)*

Followed by expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

### *Substitution Boxes*

The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output as shown in Figure 5.

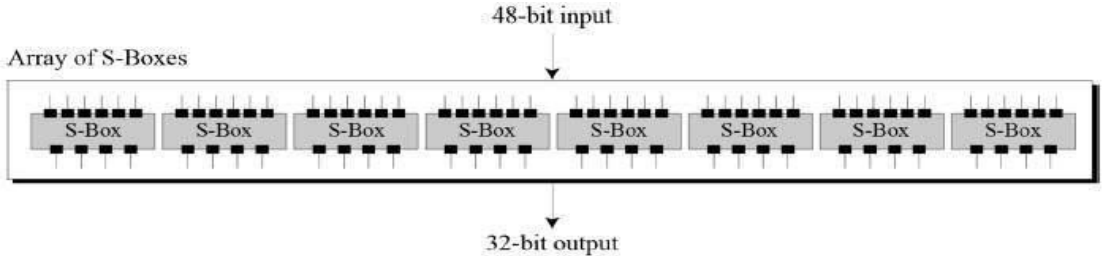


**Figure5.** *Substitution process*

The S-box rule is illustrated in Figure 6below.

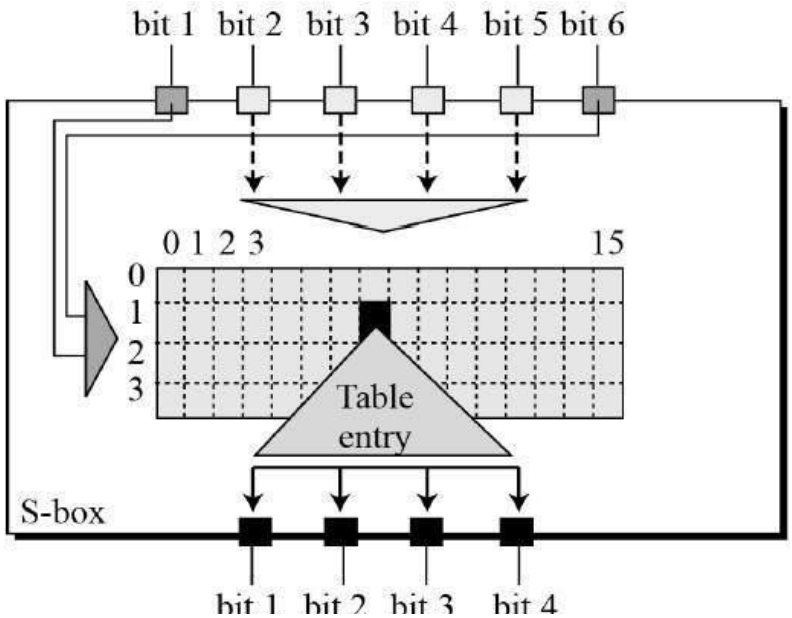


**Figure6.** *Working with S-box rule*

There is a total of eight S-box tables. The output of all eight s-boxes is then combined into the 32-bit section.

### *Straight Permutation*

The 32-bit output of S-boxes is then subjected to the straight permutation with the rule shown Table 3.

**Table3.** *Straight Permutation*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 07 | 20 | 21 | 29 | 12 | 28 | 17 |
| 01 | 15 | 23 | 26 | 05 | 18 | 31 | 10 |
| 02 | 08 | 24 | 14 | 32 | 27 | 03 | 09 |
| 19 | 13 | 30 | 06 | 22 | 11 | 04 | 25 |

The working of DES is summarized in the flowchart shown in Figure 7 below.

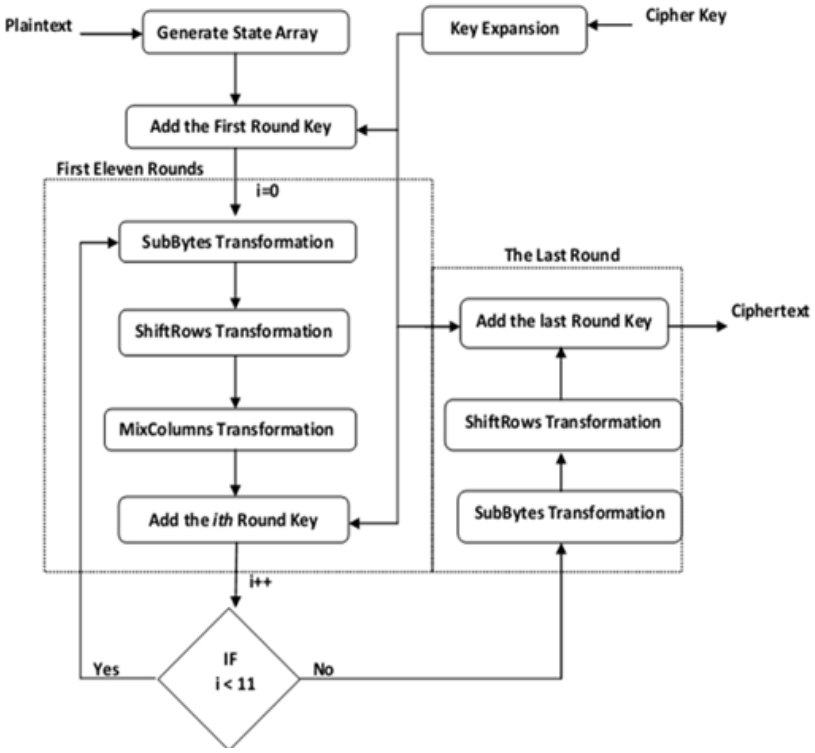


**Figure7.** *Flowchart depicting working of DES*

## B. Advanced Encryption Standard (Aes)

DES needs to be replaced because of its key size been too small. With day by day enhancing computing power, it was considered no longer secure against exhaustive key search attack. Moreover, the speed of DES is not too fast.

### *Working of AES*

AES involves replacing of inputs by specific outputs or shuffling of bits around [5, 8, 10]. AES is designed to perform all its operations on bytes rather than bits. It is because of this that plaintext block of 128 bits is treated as 16 bytes by AES. These 16 bytes are arranged in a matrix of 4*4 ( four rows and four columns). The number of rounds is not fixed in case of AES [9]. They depend on the length of the key. 128-bit keys require 10 rounds, 192-bit keys require 12 rounds and 256-bit keys require 14 rounds. Each round makes use of different 128-bit round key which is calculated from original AES key [2, 3]. The entire process is shown in Figure 8.

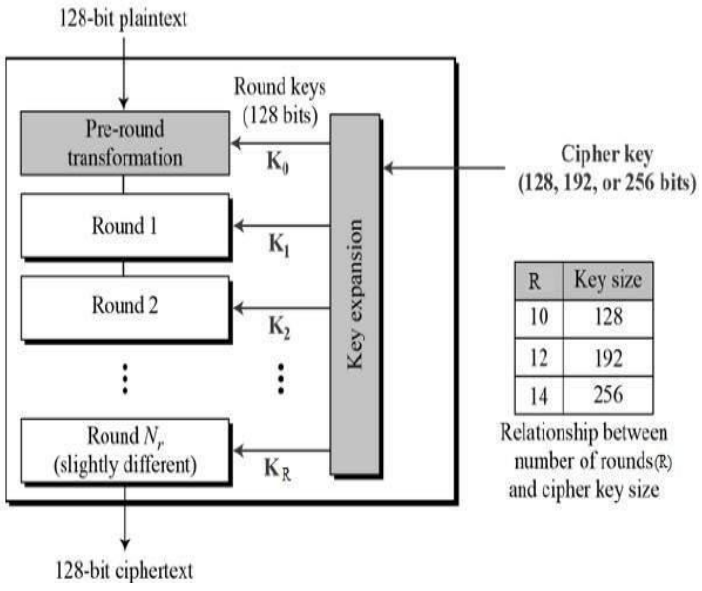


**Figure8.** *Working of AES*

***Encryption Process***

Each round comprises of four sub-processes which are shown in Figure 9.

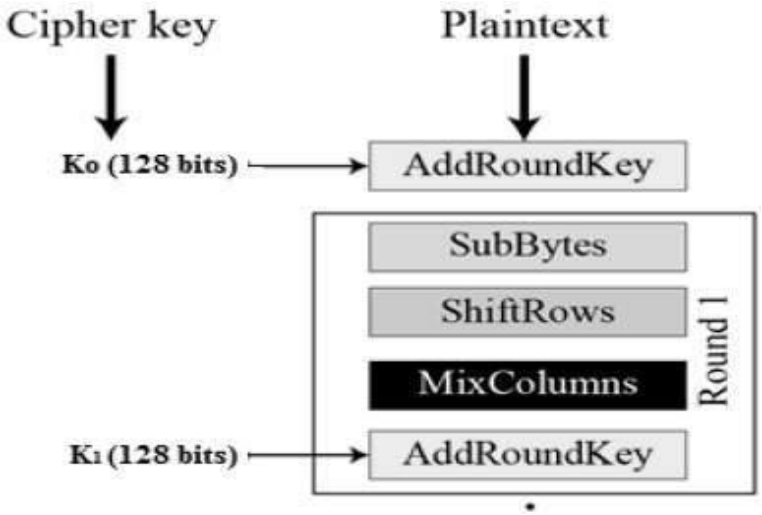


**Figure9.** *Steps involved in Encryption Process*

***Byte Substitution (Sub Bytes)***

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is a matrix of four rows and four columns.

***Shift rows***

Every row of the 4*4 matrix is shifted to the left. Entries which fall off are re-inserted on the right side of the row. The procedure followed to perform shift is mentioned as under.

- First row is not shifted.
- Second row undergoes one (byte) position shift to the left.
- Third row faces two positions shift to the left.
- Fourth row undergoes three positions shift to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

***Mix Columns***

Now a special mathematical function is used to transform each column of four bytes. The function takes four bytes of one column as input and outputs four completely new bytes which replace the original column. The result provides with a new matrix of 16 new bytes. This step is not performed in last round.

***Add Round Key***

The 16 bytes are now again considered as 128-bits and are XORed with 128 bits of the round key. The output is cipher text if currently running round is the last round. Else, the resultant 128-bits are again interpreted as 16 bytes and next round starts.

***Decryption Process***

The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round comprises four processes performed in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in a reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms need to be separately implemented, although they are very closely related.

The flowchart shown in Figure 10 summarizes the entire working of AES.

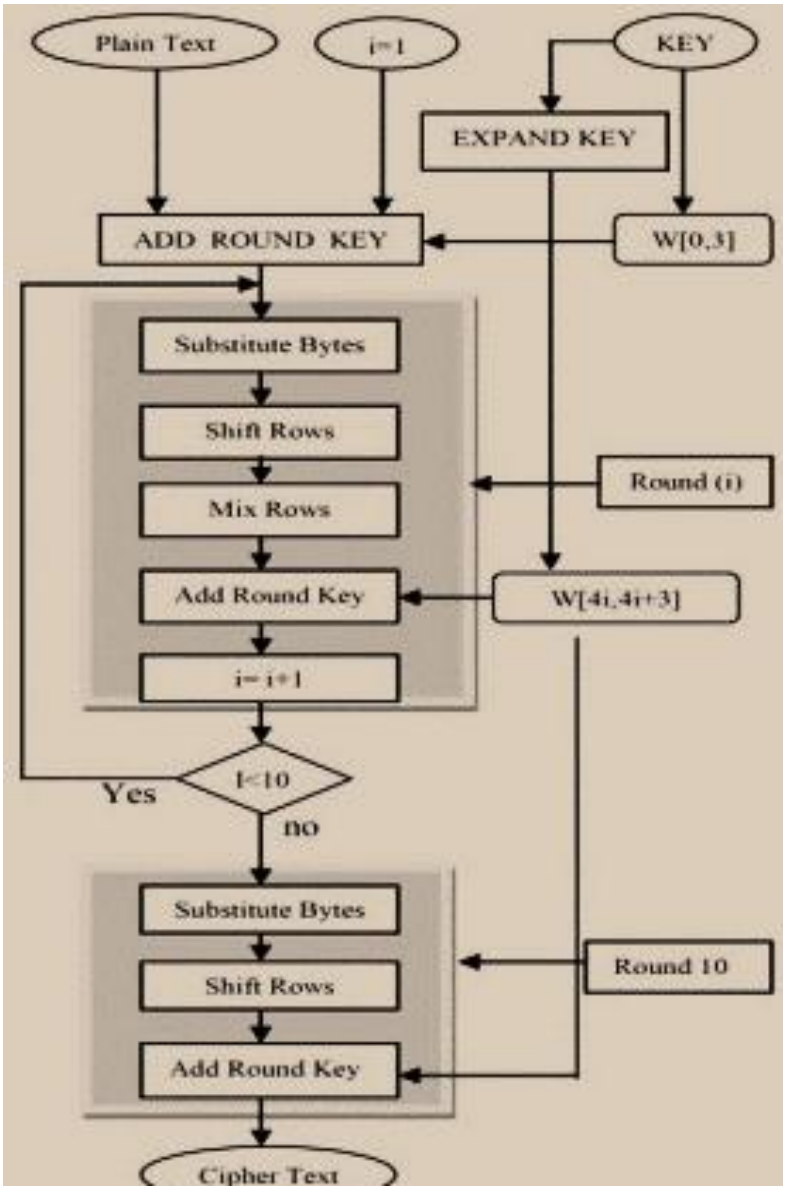


**Figure10.** *Flowchart showing working of AES*

## 4. CONCLUSION

The paper elaborates the importance of securityin cloud computing and how encryption can protect communications and stored information from unauthorized access.

The differences between DES and AES has been summarized in Table 4 below.

**Table4.** *Differences between DES and AES*

| | DES | AES |
|---|---|---|
| Developed | 1977 | 2000 |
| Key Length | 56 bits | 128, 192, 256 bits |
| Cipher Type | Symmetric block cipher | Symmetric block cipher |
| Block Size | 64 bits | 128 bits |
| Security | Proven inadequate | Considered Secure |

Currently, AES is most advanced and adopted algorithm for performing cryptography in both hardware and software. No successful cryptanalytic attacks against AES has been discovered to date. The feature of flexible key length allows a degree of future proofing against exhaustive key attacks.

## REFERENCES


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

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

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

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

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

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

[7] Preetha M., Nithya M., "A study and performance of RSA algorithm*", International Journal of Computer Science and Mobile Computing (IJCSMC)*, Vol. 2, Issue. 6, June 2013, pg.126 – 139.

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

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

[10] 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.

[11] 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.

[12] 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 10 years and has above 108 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 (2017). Analyzing Working of DES and AES Algorithms in Cloud Security, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 4(3), pp.1-9, DOI: http://dx.doi.org/10.20431/2349-4859.0403001*