COMAPARISON OF CRYPTOGRAPHIC ALGORITHMS FOR CLOUD COMPUTING

Deep Kumar Sharma[1], Amrita Kaur[2], Anjali Gangwar[3], Priyanka Pradhan[4]

[1,2,3,4] *Software Engineering, SRMSCET, Bareilly, (India)*

ABSTRACT

Cloud computing is a set of services in the IT, provided to a customer over a network and these services are delivered by third party. The use of cloud computing increasing day by day and the number of users also increases because of its attractive features and easy services. The increase in number of users increases the security issues. The security is very important factor in the cloud computing. The aim of this paper is to tell about the best security technique; here we discuss about the two encryption algorithms AES and DES. To compare these algorithms we show that which the best algorithm for cloud are computing.

Keywords: AES (Advanced Encryption Standard) Technique, Cloud Computing, DES (Data Encryption Standard) Technique.

I. INTRODUCTION

Cloud computing security is the set of control-based technologies and policies designed to hold to regulatory fulfillment rules and protect information, data applications, and infrastructure associated with cloud computing use.

There are four main type of cloud, proper security in these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider.

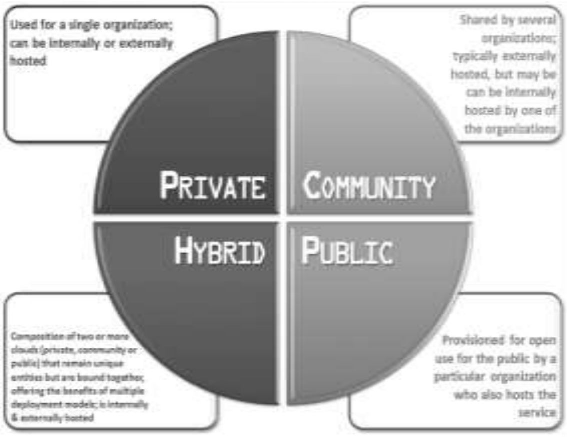

Used for a single organization; can be internally or externally hosted
Shared by several organizations; typically externally hosted, but may be can be internally hosted by one of the organizations
PRIVATE
COMMUNITY
HYBRID
PUBLIC
Composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models; is internally & externally hosted
Provisioned for open use for the public by a particular organization who also hosts the service

Fig. 1- Types of Cloud Computing

1.1 Types of Cloud

1) Public cloud**:** shared outside, anyone can use it and some payment may be needed.

2) Private cloud: It is opposite to public cloud, private cloud's resource is limited to a group of people, like a staff of a company.

3) Hybrid cloud: This is a mixture of previous two clouds, some cloud computing resource is shared outside but some don't.

4) Community cloud: This is a special type of cloud to share and reduce the cost of computing system. Data storage in cloud computing offers so many benefits to users:

a) It provides unlimited data storage space for storing user's data.

b) Users can access the data via internet, from everywhere in the world not on a single machine.

c) We do not buy any storage device for storing our data and have no responsibility for local machines to maintaining data [1].

II. SECURITY CHALLENGES

There are many security challenges in the cloud computing, so because of these challenges we need the, Security algorithms. In this session we discuss about these challenges

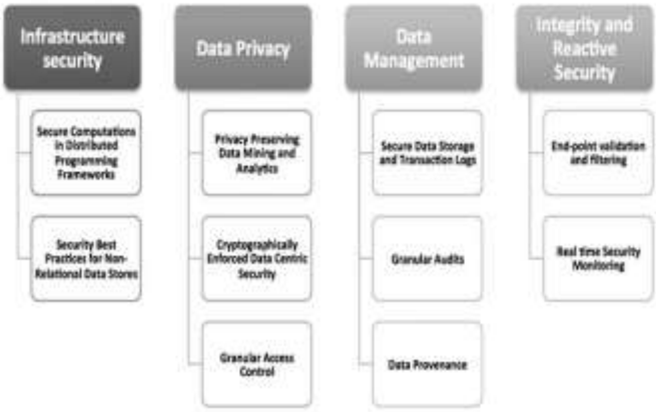

Infrastructure security
Secure Computations in Distributed Programming Frameworks
Security Best Practices for Non-Relational Data Stores
Data Privacy
Privacy Preserving Data Mining and Analytics
Cryptographically Enforced Data Centric Security
Granular Access Control
Data Management
Secure Data Storage and Transaction Logs
Granular Audits
Data Provenance
Integrity and Reactive Security
End-point validation and filtering
Real time Security Monitoring

Fig. 2- Security Challenges in Cloud Computing

Are:-

a) Infrastructure security.

b) Data Privacy.

c) Data management.

d) Integrity and reactive Security.

III. CRYPTOGRAPHY

Cryptography is basically the process of hiding information. Our ATM cards, computer passwords and transferring data from one place to another are done with cryptography. The main goal of cryptography is keeping data secure from unauthorized attackers. The reverse of data encryption is decryption [2].

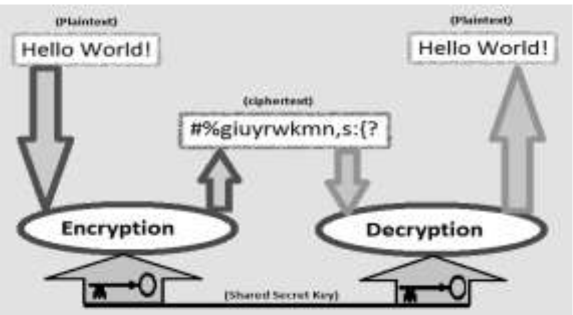


Figure 3-Working of Cryptography

There are many security algorithms in the cryptography, but here we discuss only about the two basic algorithms:-

1) DES.

2) AES.

1) DES (Data Encryption Standard)

DES was developed as a standard for communications and data protection by IBM research team. DES is a broadly-used method of data encryption using a secret key. DES originated at IBM in 1977 and was adopted by the U.S. Department of Defence. It is precise in the ANSI X3.92 and X3.106 standards and in the Federal FIPS 46 and 81 standards. There are 72 quadrillion or other promising encryption keys that can be used. For each given message, the key is selected at random from among this huge number of keys. Both the sender and the receiver must know and use the same private key. DES applies a 56-bit key to each 64-bit block of data. The method can run in several modes and involves 16 rounds or operations [4].

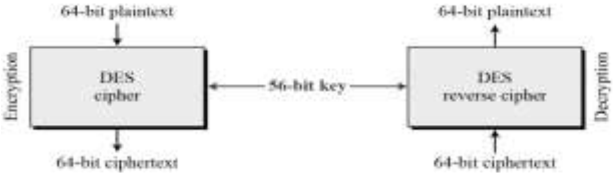


Figure 4 - Encryption and decryption with DES

The encryption process is made of two permutations (P-boxes), which we call initial and final permutations, and sixteen Feistel rounds.

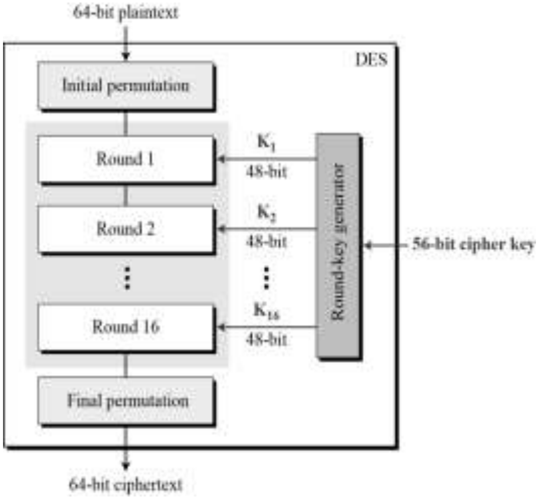


Fig. 5 - Working of DES Algorithm

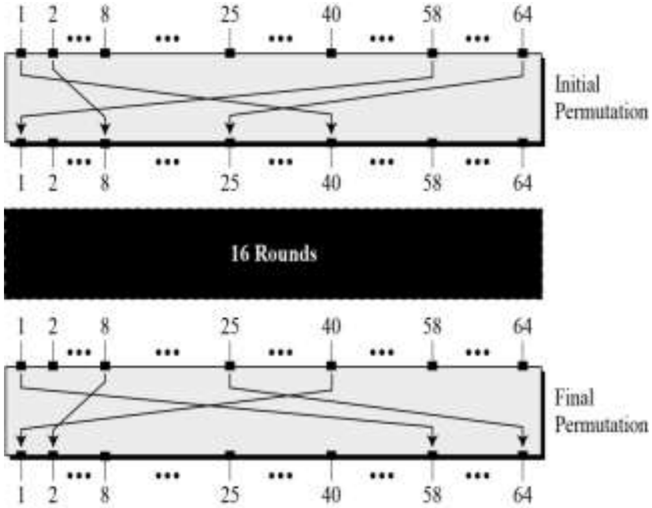
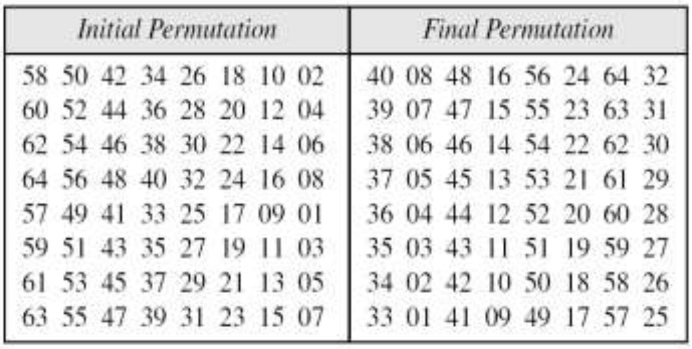


Fig. 6 - Initial and Final Permutation Steps in DES



Initial Permutation	Final Permutation
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

Fig. 7 - Initial and Final Permutation Table

The 58th bit of input x will be the first bit of output IP(x), the 50th bit of x is the second bit of IP(x), etc.

Steps of DES:-

- Get the Plaintext.
- Get the Password.
- Convert the Characters into binary form.
- Derive the Leaders (L1 to L16) from the Password.
- Apply the Formula to get the encrypted and decrypted message.

2) AES (Advanced Encryption Standard)

The AES is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001. for the encryption of electronic data. AES is a latest cryptographic algorithm that can be used to defend electronic data. Exclusively, AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). Unlike public-key ciphers, which use a pair of keys, symmetric-key ciphers use the same key to encrypt and decrypt data. Encrypted data returned by block ciphers have the same number of bits that the input data had. Iterative ciphers use a loop structure that repeatedly performs permutations and substitutions of the input data [5].

AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds. AES has defined three versions, with 10, 12, and 14 rounds. Each version uses a different cipher key size (128, 192, or 256), but the round keys are always 128 bits.

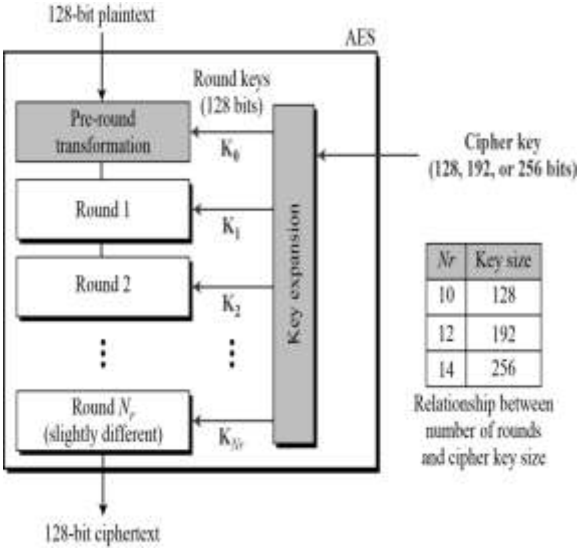


Fig. 8 - General design of AES encryption cipher

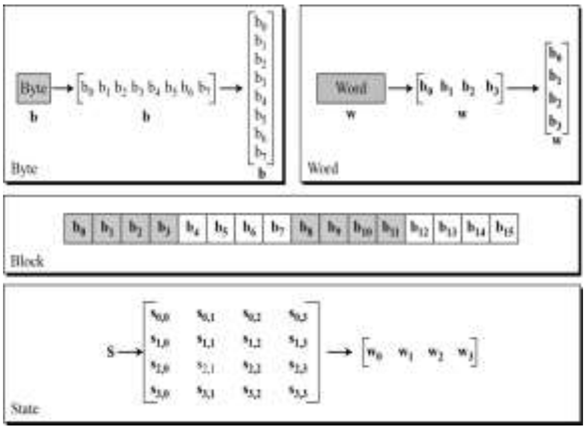

Byte
b
b_0 b_1 b_2 b_3 b_4 b_5 b_6 b_7
Byte
Word
w
b_0 b_1 b_2 b_3
Word
b_0 b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8 b_9 b_{10} b_{11} b_{12} b_{13} b_{14} b_{15}
Block
S
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
w_0 w_1 w_2 w_3
State

Fig. 9 - Data units used in AES

To provide security, AES uses four types of transformations:

- The sub bytes step
- The Shift Rows step
- mixing
- key-adding

1) The Sub Bytes step

In the Sub Bytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, *S*; b_{ij} = *S*(a_{ij}).While performing the decryption, Inverse Sub Bytes step is used, which requires first taking the affine transformation and then finding the multiplicative inverse (just reversing the steps used in Sub Bytes step).

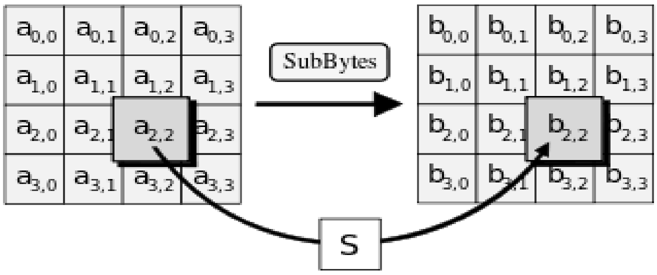

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

Fig.10 – Working of Sub Bytes Steps

2) The Shift Rows step

In the Shift Rows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n is shifted left circular by n-1 bytes. In this way, each column of the output state of the Shift Rows step is composed of bytes from each column of the input state. For a 256-bit block, the first row is unchanged and the shifting for the second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks. The importance of this step is to avoid the columns being linearly independent, in which case, AES degenerates into four independent block ciphers.

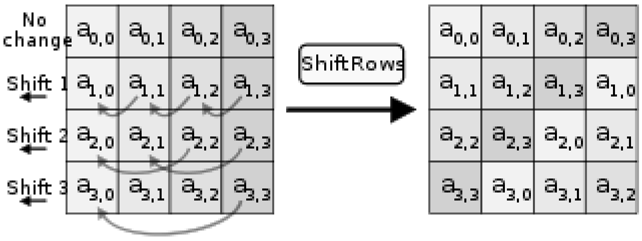

No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Fig. 11 – Shift Rows Steps

3) The Mix Columns step

In the Mix Columns step, each column of the state is multiplied with a fixed polynomial *c(x)*.

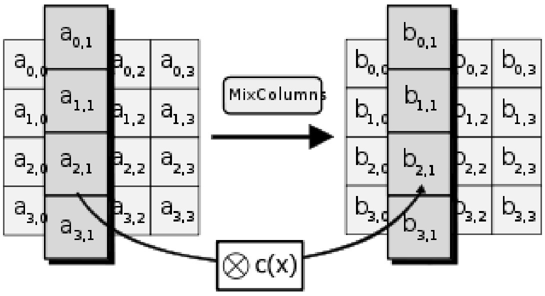

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$\otimes c(x)$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig. 12 - Mix Columns Steps

4) The Add Round Key step

In the Add Round Key step, each byte of the state is combined with a byte of the round sub key using the XOR operation (⊕).

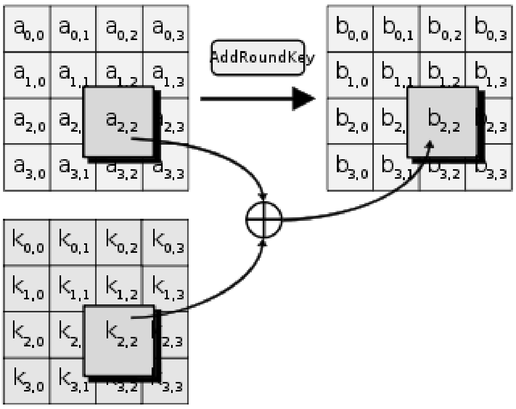
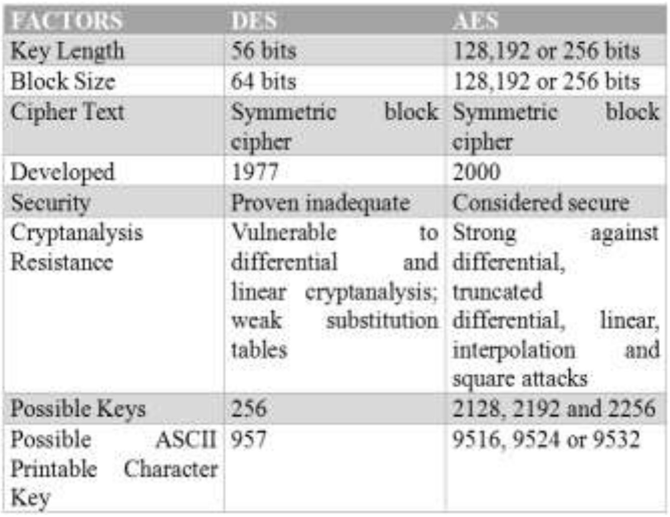

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$\oplus$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

Fig. 13 - The Add Round Key steps

IV. COMPARISON BETWEEN AES AND DES

Here we compare Data Encryption Standard (DES) and Advance Encryption Standard on the following factors that are based on different parameters and a comparative study between DES and AES is done by the nine factors, Which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time required to check all possible key.



FACTORS	DES	AES
Key Length	56 bits	128,192 or 256 bits
Block Size	64 bits	128,192 or 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Cryptanalysis Resistance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and square attacks
Possible Keys	256	2128, 2192 and 2256
Possible ASCII Printable Character Key	957	9516, 9524 or 9532

Table .1 Comparison between AES and DES

V. CONCLUSION

In this paper, there is a proportional study between DES and AES were done. Here the theoretical analysis is done for DES and AES algorithms. On the basis of that comparison it was concluded that AES algorithm consumes least encryption and decryption time as compared to DES algorithm.

REFERENCES

[1] Neha jain, Gurpreet kaur, “Implementing DES algorithm in cloud for data security”, in VSRD-IJCSIT, VOL-2(4), 2012, 316-321.

[2] Shraddha soni, Himani agrwal, Dr.(Mrs.) Monisha sharma, “Analysis and Comparison between AES and DES cryptographic algorithm,” in IJEIT-2012.

[3] Shraddha soni, Himani agrwal, Dr.(Mrs.) Monisha sharma, “Analysis and Comparison between AES and DES cryptographic algorithm,” in IJEIT-2012.

[4] Mrs.Aruna A, Ms.Suganya N, Ms.KeerthanaAnandhi N, Ms.Priyanka A, “Assured Data Transfer under Auditing in Distributed Circumstances,” IJSRP, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153

[5] Mrs.Aruna A, Ms.Suganya N, Ms.KeerthanaAnandhi N, Ms.Priyanka A, “Assured Data Transfer under Auditing in Distributed Circumstances,” IJSRP, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153