- 12 cycles for 192 bit key.
- 14 cycles for 256 bit key.

Description of Algorithm:
Algorithm work in 4 steps:

1) Key Expansion

Round keys are derived from cipher keys and AES requires the 128 bit round key for each round.

2) Initial Round

1) Add Round key- Using bitwise operation each block of data is attached with one block of round key.

3) Rounds

a) Sub bytes - Each byte is replace with another byte.
b) Shift Rows- Cyclically last three rows are shifted.
c) Mix Columns- Combining four byte of each column.
d) Add Round Key

4) Final Rounds

a) Sub bytes
b) Shift Rows
c) **Add Round Key**

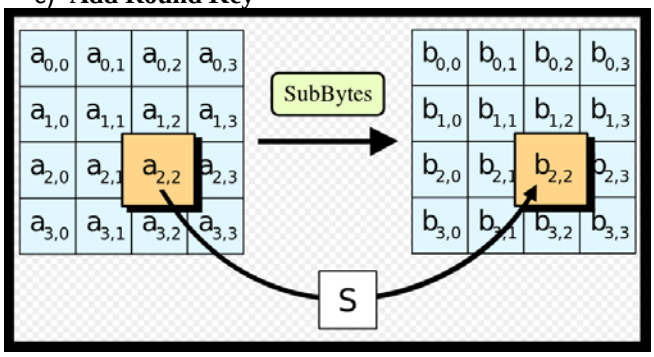

Figure 3: Sub Bytes

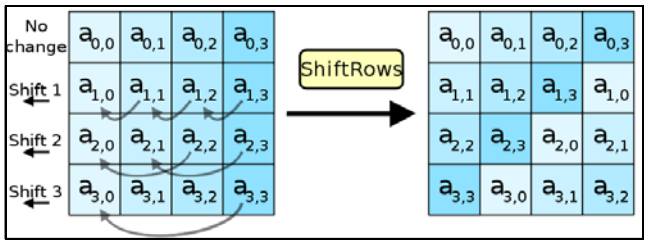

Figure 4: Shift Rows

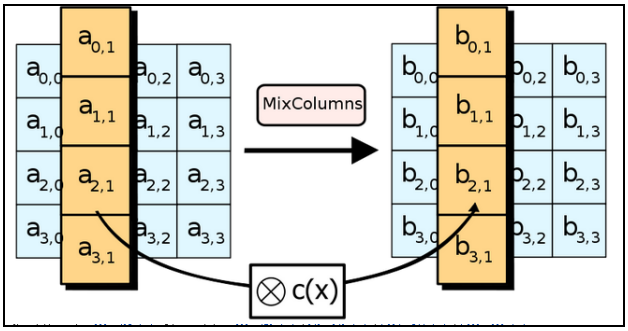

Figure 5: Mix Columns

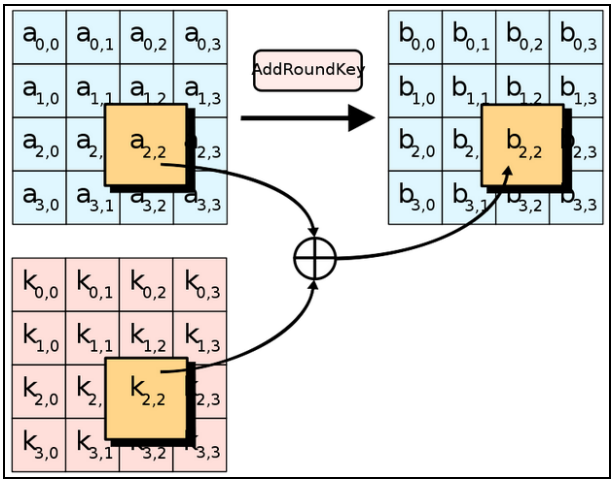

Figure 6: Add Round Key

MD5- (Message-Digest algorithm 5), a mostly known as cryptographic hash function with a 128-bit hash value, it processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks . the message is padded so that its length is divisible by 512.

This algorithm takes an input a message of undefined length but produces the 128 bit, which is generally less than the length of the input message. The MD5 algorithm is designed for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA ,DES, Triple DES, AES. This algorithm is mostly fast on 32 bit machines.

6. Conclusion

So now a day most of the organizations are using cloud servers or cloud databases for storing their databases. In this paper we are just trying to minimize the hackers attack from losing the private data from the server. There are many algorithms in the world out of that we are using AES and MD5 algorithms. AES having so many advantages so AES gives the better performance with MD5 algorithm.

References

[1] Mohammed A. AlZain, Eric Pardede, Ben Soh , James A. Thom “Cloud Computing Security: From Single to Multi-Clouds”,cloud computing , HICSS’12,Proc.45th Hawaii International Conference on System Sciences ,2012,pp 5490-5499
[2] Sravan Kumar R, Ashutosh Saxena, “Data Integrity Proof in Cloud Storage”, COMSNETS’11, Proc.Bangalore 3rd International Conference on Communications Systems and Networks,2011
[3] Tirthani, Neha, and R. Ganesan. "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography.", International Association for Cryptologic Research, 20140121/049
[4] Mohit Marwaha, Rajeev Bedi ,”Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing”, IJCSI,Vol.10,Jan.2013

[5] Mandeep Kaur,Manish Mahajan, "Using encryption Algorithms to enhance the Data Security in Cloud Computing", IJCCTS,Vol.01,Jan.2013
[6] K.S.Suresh, K.V.Prasad, "Security issues and Security algorithms in Cloud Computing",IJARCSSE,Vol.02,Oct.2012.
[7] Nesrine Kaaniche, Maryline Laurent, "A Secure Client side Dedplication Scheme in Cloud Storage Environment", New Technologies, Mobility and Security (NTMS), 2014 6th International Conference at Dubai ,2014,pp 1-7