Volume 4, Issue 9, September 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Analysis of Symmetric Block Cipher Algorithm and Security Issue on Cloud Encrypted Data

Dr. V. Venkatesa Kumar*
Department of CSE ,
Anna Univeristy Regional Centre-Coimbatore, India

A. Murugavel
Department of CSE
Anna Univeristy Regional Centre-Coimbatore, India

Dr. M. Newlin Rajkumar
Department of CSE
Anna Univeristy Regional Centre-Coimbatore, India

Abstract— In cloud, data can be stored and get into anytime and anywhere. The cloud is a memory system where any consumer can access the files which are already laid in. Meanwhile, any consumer can access the cloud storage; security on the stored files reduces. Hence it gets necessary to shield the files in the cloud. In order to protect the files from the intruder, we are applying an encryption technique. On our proposal block cipher algorithm from symmetric encryption technique is used to shield the files. The Block cipher method includes AES, Blowfish, IDEA and RC5 algorithm.

Keywords— Block cipher, Blowfish, AES, IDEA, RC5.

I. INTRODUCTION

Cloud computing refers to the legal transfer of computing resource over the net. The cloud server allows individual and business to use software and hardware that are managed by third parties in a remote position [8]. Example of cloud services includes online file storage, social networking website, webmail, online business application. The cloud computing model allows accessing the data and computer resource from anywhere, where the net connection is usable. At the present time files stored in the cloud service are not always secured. For many people security is one the major concern, when it comes to posting their files into the cloud. They cared about their files being viewed or even comprised of other people because they don't recognize the transparency of the process in background. For the customer to conviction the cloud service such that files are securely laid in, they necessitate to run short for substitute elucidation. One such elucidation is encryption technique.

Encryption is the process by which one user data is bundled with an encryption key without which the data cannot be reproduced to original form. The goals of encryption in ensuring that the data in cloud protected against unauthorized access. There are various ways in encryption to secure the files in service. In this proposal one of the encryption technique named block cipher from symmetric technique. The Block cipher model includes AES, Blowfish, IDEA and RC5 algorithm.

II. SECURITY CHALLENGES IN CLOUD COMPUTING

The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, thereby infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. There are five types of issues [2] raise while discussing security of a cloud.

1. Data Issue

Information stored in the cloud can be accessed by anyone from anyplace at whatever time. The information accessed by consumer may be common files, private or sensitive files. These cases of files accessed by cloud consumers leads to modification of actual data and also in the data security like an organization detail or personal detail of cloud consumers may be misused by the other cloud consumers. To secure the information from the above issue data integrity method [3] is the best alternative.

2. Privacy Issue

In the cloud service, consumer personal information may be secured by a service provider from other service providers and consumers. The cloud service provider should have knowledge of who is accessing and maintaining the server to protect consumer personal information. Authentication [4] is the best solution for the privacy issue.

3. Infected Application

There may be a probability of uploading an infected application in cloud with or without intention of cloud provider or consumer. To prevent [5] the cloud server from such infecting application, service provider should receive terminated access to the server to all rights for monitoring and maintenance of the server.

4. Security Issue

Cloud computing security must be done at provider level and on the consumer level. The consumer should be aware that loss or stealing or tampering of data from other consumer using the same cloud. Security on cloud server must be properly kept [7] by the service provider from all external threats. A quality and security of cloud storage depend on proper service shielded by service provider.

5. Trust Issue

The cloud does not build the trust between consumer and provider which necessary aspect in business. Then the supplier must make use of a marvelous application to create confidence.

III. SYMMETRIC BLOCK CIPHER ENCRYPTION ALGORITHM

Symmetric cipher uses the same encryption key for both encryption and decryption of a message. Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of information. Symmetric cipher can operate in either block mode (or) stream mode. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption.

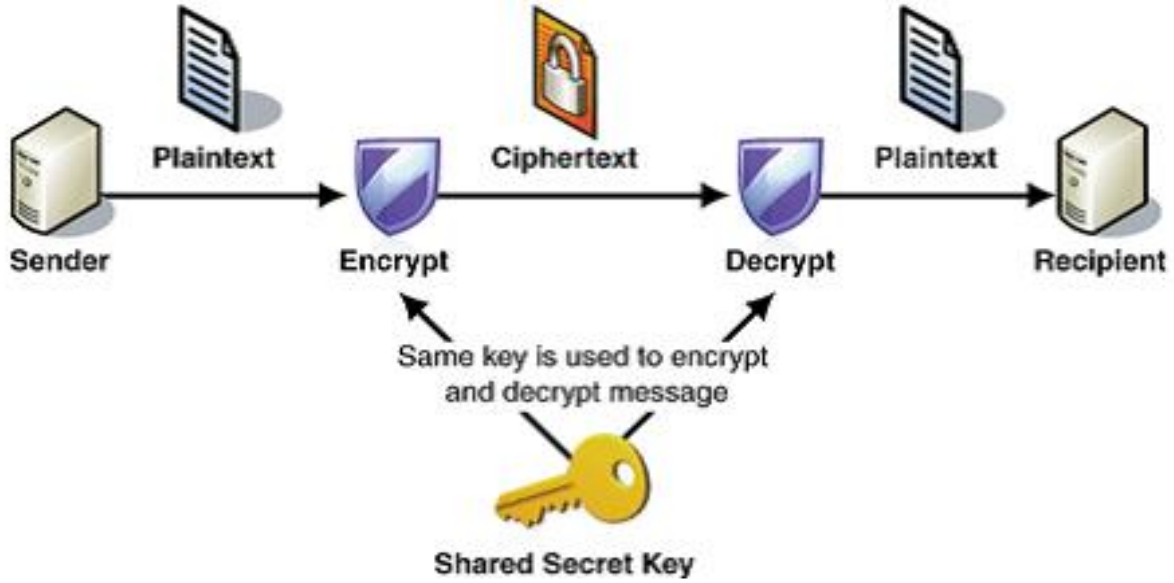

Fig 1. Symmetric encryption technique

In **block mode,** cryptographic algorithm splits the input message into an array or small fixed-sized and then encrypt or decrypt the block one by one. In **stream mode**, every digit (usually one bit) of the input messages encrypted separately. Several block cipher encryption algorithms are available and are used in information security. Out of the different encryption algorithms, few algorithms are described in this section.

1. Blowfish Algorithm

Blowfish is a symmetric block cipher [1] was designed in 1993 by Bruce Scheier, which can be effectively used for encrypting and safeguarding of information. It encrypts block information of 64 bits at a time. It will follow the feistel network and this algorithm is split into two sections.

1) Key Expansion:

It will convert a key of at the most 448 bits into many subkey arrays totaling 4168 bytes Blowfish uses a large number of subkeys. These keys generate earlier to any encryption or decryption. The p-array consists of eighteen, 32-bit subkeys: P1, P2… P18.

2) Data Encryption:

Data encryption occurs via a 16-round Feistel network. Each flip consists of a key dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions in 32-bit words. The sole extra operations are four indexed array information lookups per round.

```
Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16:
        xL = xL XOR Pi
        xR = F(xL) XOR xR
        Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.
Then, xR = xR XOR P17 and xL = xL XOR P18.
Finally, recombine xL and xR to get the ciphertext.
```

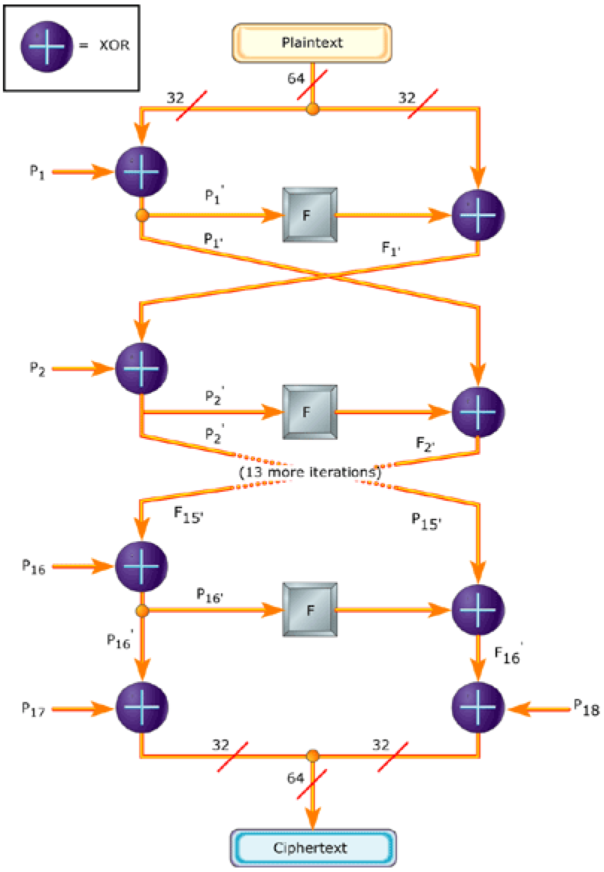

Fig 2. Encryption with Blowfish

1) *Advanced Encryption Standard (AES)*

Advanced Encryption Standard is a symmetric- key block cipher [6] published as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). AES is a non-Feistel cipher. AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits as shown in figure 3. AES operates on a 4×4 column-major order matrix of bytes, known as the state.

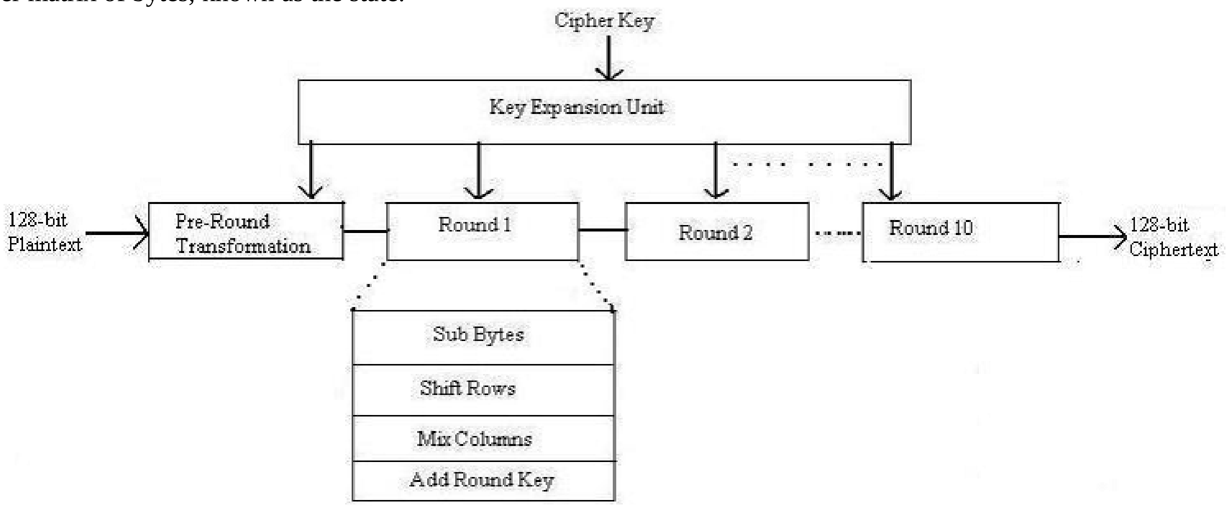

Fig 3. Encryption with AES

2) *International Data Encryption Algorithm (IDEA)*

International Data Encryption algorithm (IDEA) is a symmetric key block cipher [9] published in 1991 by James Massey and Xuejia Lai. It operates on 64-bit block using 128-bit key. On the basis of addition and multiplication. It consist eight identical transformations.

1) *Data Encryption*

In the IDEA algorithm, we assume the input text of size 64-bits at a time and divide it in evenly; i.e., 64-bit plain text is divided into 4 sub-blocks, each of 16-bits in size. .Operations needed in the first 8 rounds Multiplication modulo 2^{16} +1, Addition modulo 2^{16}, Bitwise XOR and Output transformation phase Multiplication module 2^{16} +1, Addition modulo 2^{16}.

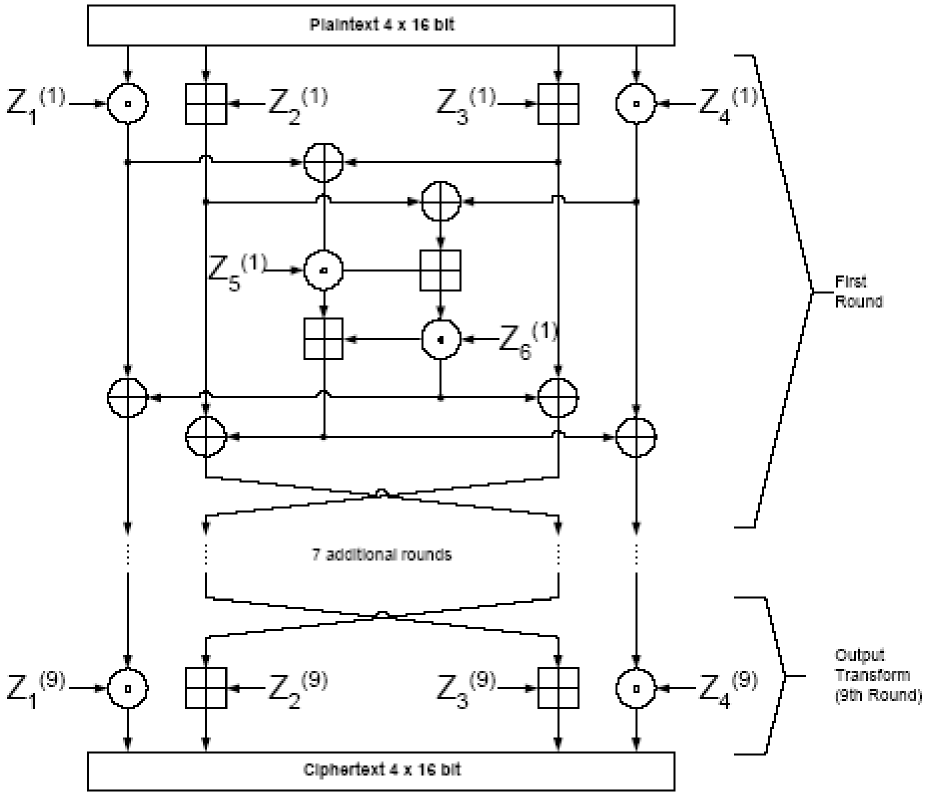

Fig 4. Encryption with IDEA

3) *RC5*

RC5 is a symmetric key block cipher [10] designed by Ron Rivest [RIVE94, RIVE95]. It encrypts the information with block size of 32, 64 or 128 bits employing a key length range from 0 to 2040 bits. A particular version of RC5 is selected as RC5-w/r/b.

TABLE. 1

PARAMETER	DEFINITION	ALLOWABLE VALUES
w	The word size in bits. RC5 encrypts 2-word block	16,32,64
r	Number of rounds.	0,1,…,255
b	Number of 8-bit in the secret key K.	0,1,…255

1) *Data Encryption*

The plaintext is assumed to initially reside in the two *w*-bit register A and B .We apply the variables LE_i and RE_i to refer to the left and right half of the data after round *i* has completed. The encryption algorithm can be specified by the following pseudocode:

```
$LE_0 = A + S[0];$
$RE_0 = B + S[1];$
for $i = 1$ to $r$ do
$LE_i = ((LE_{i-1}$ XOR $RE_{i-1}) <<< RE_{i-1}) + S[2 * i];$
        $RE_i = ((RE_{i-1}$ XOR $LE_i) <<< LE_i) + S[2 * i + 1];$
```

The resulting ciphertext is contained in two variable LE_r and RE_r. Each of the *r* rounds consists of substitution using both words of data, a permutation using both words of data and a substitution that depends on key.

IV. CONCLUSION

In the study nature of symmetric block cipher algorithms that are Blowfish, AES, IDEA, and RC5 are investigated, examined and evaluated by taking specialized in cloud computing atmosphere. The main goal of those algorithms is to secure the encrypted files that are kept on cloud server and also measure the performance analysis.

REFERNCES

[1] B. Schneier, *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption,* Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[2] C.N. Höfer and G. Karagiannis, *Cloud computing services: taxonomy and comparison*, Internet Serv Appl (2011).

[3] Priyanka Arora, Arun Singh and Himanshu Tyagi, *Evaluation and Comparison of Security Issues on Cloud Computing Environment*, (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, p.p (179-183), 2012.

[4] Jagpal Singh, Krishnan Lal and Dr. Anil Kumar Shrotiya, *Journal of Computer Science and Applications*., ISSN 2231- 1270 Volume 4, Number 1 (2012), pp. 1-7. http://www.irphouse.com

[5] Kevin Hamlen, Murat kantarcioglu, Latifur Khan and Bhavani Thurasingham, *International Journal of Information Security and Privacy*, 4 (2), p.p (39-51), April-June 2010.

[6] Rashmi Nigoti, Manoj Jhuria Dr. Shailendra Singh *A Survey of Cryptographic Algorithms for Cloud Computing* in IJETCAS 13-123; p.p (141-146) (2013).

[7] Security analysis of cloud computing :(http://cloudcomputing.sys-con.com/node/1330353).

[8] Introduction to cloud computing (http://www.priv.gc.ac/resource/fs-fi).

[9] How-Shen Chang International *Data Encryption Algorithm* CS-627-1 Fall 2004.

[10] Ronald L. Rivest *the RC5 encryption algorithm* mass 02139, 1997.