International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.03, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Enrichment of Data Security by Amalgamation of Symmetric Encryption Algorithms

Varsha Gupta[1], Aman Thakur[2]

[1]*M.Tech Scholar, CSE, LR Institute of Engineering and technology Solan, (India)*
[2]*Assistant Professor, CSE, LR Institute of Engineering and technology Solan, (India)*

ABSTRACT

Nowadays cloud computing is on trend to make the data easily accessible remotely. Maximum of data are processed like document, email etc remotely so it needs to be more secure by implementing efficient algorithm. There are many algorithms which are implemented on cloud for data security but somewhere they could remove the security partially so our aim in this work is to design the efficient algorithm which makes the data secure with minimum processing time and memory usage. In this research we amalgamate AES+BLOWFISH to make the data secure with minimum processing time and memory usage and also compare our result with the existing work i.e. RSA+AES. The experimental result shows that hybridization of AES+BLOWFISH is much more efficient than existing work in terms of security, processing time and memory usage.

Keywords: AES, BLOWFISH, memory usage, processing time, RSA.

I. INTRODUCTION

The idea behind cloud computing is that storing or sharing the data over the internet so that it would make easier to access the information however there are certain things that one must be aware of when using the cloud to store data. The serious thing in cloud computing is data security. If the data is not handled properly a hacker can be able to access confidential information because all information is shared through internet. This can be prevented by taking certain security measures. So we use cryptosystem which is an implementation of cryptographic techniques to preserve the security in cloud. In cloud cryptography we use encryption techniques to keep the data secure [1]. Encryption techniques are used to encipher the sensitive information. Enciphering is to make the data in unreadable form by using encryption algorithm. There are two types of encryption algorithm 1) Symmetric Encryption 2) Asymmetric Encryption. In symmetric encryption same key is used for encryption and decryption. The sending party uses the secret key as a part of mathematical operation to encrypt plain text to cipher text. The receiving party uses the same key to decrypt the cipher text to plain text. DES, 3DES, AES and BLOWFISH are the common example of this type of technique. In DES input size of data is 64 bit blocks uses 56 bit key. Later it was proved as insecure because of shorter key length. Further 3 DES was implemented but it was vulnerable to few attacks. Then AES was developed which uses 128 bit block as input size and uses the key sizes of 128,192 and 256 bit mostly used in wireless communication, financial transaction, encrypted data

storage etc. Blowfish is considered to be more secure and fastest because of strong key size which enables it to be used in many application like bulk encryption, internet based security and packet encryption. In asymmetric encryption algorithm we use two keys for encryption and decryption. Private Key and public key, Public key is available to all including hackers. Private Key is a secret key which is only known to the user. When sender wants to send data to the receiver he used receiver public key to send the message. He encrypts the plaintext with public key and cipher text is obtained. When receiver wants to read the data he decrypts that message by using his private key and cipher text. The most common example of asymmetric encryption is RSA which can be used for both public key encryption and digital signatures. It is an authentication technique to protect computer passwords. The main disadvantage of asymmetric techniques is that they require more computational power and memory because of large mathematical operation [2].

II.RELATED WORK

To learn Blowfish Algorithm and AES, there are some other works from related field which shows the performance of both algorithms.

In [3] implement the four encryption algorithms DES, 3DES, AES and BLOWFISH and their performance is compared by encrypting input files of varying contents and sizes, on different Hardware platforms. The performance results have been summarized and a conclusion has been presented. From results, it has been concluded that the Blowfish is the best algorithm chosen for implementation. In [4] paper describes about the performance of different security algorithm AES, RSA, and MD5 for ensuring security framework. They compare these algorithms on the basis of encryption time, decryption time, and memory usage and speedup ratio. It has been found out that AES and MD5 algorithm uses the least time and low memory usage in comparison of RSA and AES has the highest speed as compare to other algorithms. In [5] paper presents an implementation of three encryption algorithms (DES, 3DES, BLOWFISH) and a comparison between them based on CPU execution time. The objective of this paper is to evaluate the performance of these three algorithms in terms of processing time required in the kernel and user space for generating the secret key, encryption and decryption operations. From the result we conclude that Blowfish algorithm is fastest, followed by DES algorithm then the T-DES algorithm. In [6] paper provides a comparative study that represents the differences between modern encryption algorithms in cloud computing. The study encompasses the key size, the performance and the size of the output encrypted file based two different categorizes of algorithms (symmetric and asymmetric). The results show that AES encryption algorithm enjoys certain advantages when compared to the others, especially with respect to the speedup of the encryption process. In [7] proposed hybridization of RSA and AES to ensure efficiency, consistency and trustworthiness in cloud servers. They also compared proposed schema with RSA on the basis of security, processing time, cost and memory size during encryption and decryption.

III. PROBLEM FORMULATION

Cloud computing is an emerging field of research. In cloud applications security of data and privacy are the major issues. Cloud service providers want to secure their data from the intruder. The users also want to assure that cloud service provider has taken proper security action to secure their data from intruder. Therefore security is needed on both the sides. In recent years, mass distributed storage became important to increase the data storage. Therefore, to access the sensitive data is one of the important issues of security in cloud computing. High level of performance is required to implement Mass Distributed Storage (MDS). In the previous method i.e. (RSA+AES) was implemented but due to factorization problem of prime no's it can be vulnerable to attacks and because of high computation algorithm became inefficient so it still needs improvement in security in which threats comes from any side. It is impossible to balance security and functional concern otherwise; cost will become a big factor. So in the proposed work, we are going to implement Blowfish algorithm with AES to enhance the security and efficiency of system.

IV. OBJECTIVES

- To implement existing techniques i.e. RSA+AES.
- To reduce the security problem by implementing AES+BLOWFISH algorithm.
- Minimize the processing time and memory usage to make the algorithm efficient.

V. DESIGN OF ALGORITHM

5.1 AES [8] Advanced encryption standard is the replacement of DES because of its shorter key length it was vulnerable to brute force attack. Then 3 des was to solve this problem but it was found slow. AES is usually known for using of less computing power and works with speed. AES takes input size of 128 bits support key length of 128, 192,256 bit. The no of round in AES depends upon the key size used. for 128 bit key length 10 round is iterate, for 192 bit key length 12 round is used for 256 bit 14 round is used. In encryption process every round needs a group of steps to change the state array. These steps involve four types of operation called:

- Substitution of bytes
- Shift rows
- Mix columns
- XOR round key.

i) Sub bytes: In this process every byte of the state array converts in to a different value.AES defines a substitution table of 256 values. Those 16 bytes of the state array use as an index in to 256 byte S table and replace the byte with the value from the substitution table. After indexing all the 16 bytes with stable it produces new result in the state array.

ii) Shift Rows: Shift rows apply on each row of the state array. Each row is rotated to the right by certain no of bytes.

iii) Mix Columns: Each column of the state array is processed separately to produce a new column. In this process each column is multiplied by fixed no of matrix to produce a new column.

iv) XOR round key: In this process value of the state array XOR with appropriate round key and replaces the state array with the result.

5.2 BLOWFISH [9] it was developed by Bruce Schneier in 1993. The aim of designing this algorithm to make the key strong so no one can crack the cipher key. This symmetric cipher splits messages in to blocks of 64 bits and encrypts them individually. It is one of the flexible encryption methods. Blowfish has a 64 bit block size and a key length of anywhere from 32 bit-448 bits. It is a 16-round feistel cipher and uses large key dependent boxes. Each line in S boxes represents 32 bits. The algorithm keeps two sub key arrays: the 18 entry P array and four 256 entry S boxes. The S boxes accept 8 bit input and produces 32-bit output. One entry of the p array is used every round and after the final round each half of the data block is XORED with one of two remaining unused p entries. Since blowfish is a feistel network it can be inverted simply by XORING P_{17} and P_{18} to cipher text block, then using the P entries in reverse order. The algorithm is divided in to two parts:

i) Key expansion: It will convert a key at most 448 bits in to several sub key arrays totaling 4168 bytes. The P array consists of 18, 32 bit sub keys. P_1, P_2,.....P_{18}. Four 32 bit S boxes consist of 256 entries each. The sub keys are calculated using the blowfish algorithm:

a) Initialize first the P-array and then the four S boxes in order with a fixed arrays string.

b) XOR P_1 with the first 32 bits of key, XOR P_2 with the second 32 bits of the key and so on for all bits of the key. Repeat cycle through the key bits until the entire P-array has been XORED with any bits.

c) Encrypt the all zero string with the blowfish algorithm using the sub key described in step1 and step2.

d) Replace P_1 and P_2 with the output of step 3.

e) Encrypt the output of step 3 using the blowfish algorithm with modified sub key.

f) Replace P_3 and P_4 with the output of step 5.

g) Continue the process replacing all entries of the P array and then all four S boxes in order with the output of continuously changing the algorithm. There are total 521 iterations are needed to produce all required sub keys.

ii) Data encryption part: It performs 16 round feistel network.

VI. HYBRID APPROACH OF AES AND BLOWFISH

The reason behind amalgamation of AES and BLOWFISH is to provide high throughput and high level of security to data in cloud computing as compare to existing algorithm i.e. RSA+AES. When we consider our approach we used 64 bit key size which means there are 2^{64} bit combinations for anyone to hack the key but in case of existing approach anyone who can find the p & q by factorized n can easily decrypt the message.

We can summarize the methodology as follows

i) Firstly a message of 64 bit is entered to be encoded.

ii) Then apply 64 bit key to that message using rand function.

iii) Pass the message in parity checking box to check padding is needed or not.

iv) Then split the message in to two parts using blowfish algorithm.

v) Then compute some constant data by looking in to substitution table.

vi) Apply permutation array to the output of substitution table which generate the random data.

vii) Then shift and mix the data in such a way that no one can decipher it.

viii) Apply same key to convert cipher form in to plain message.

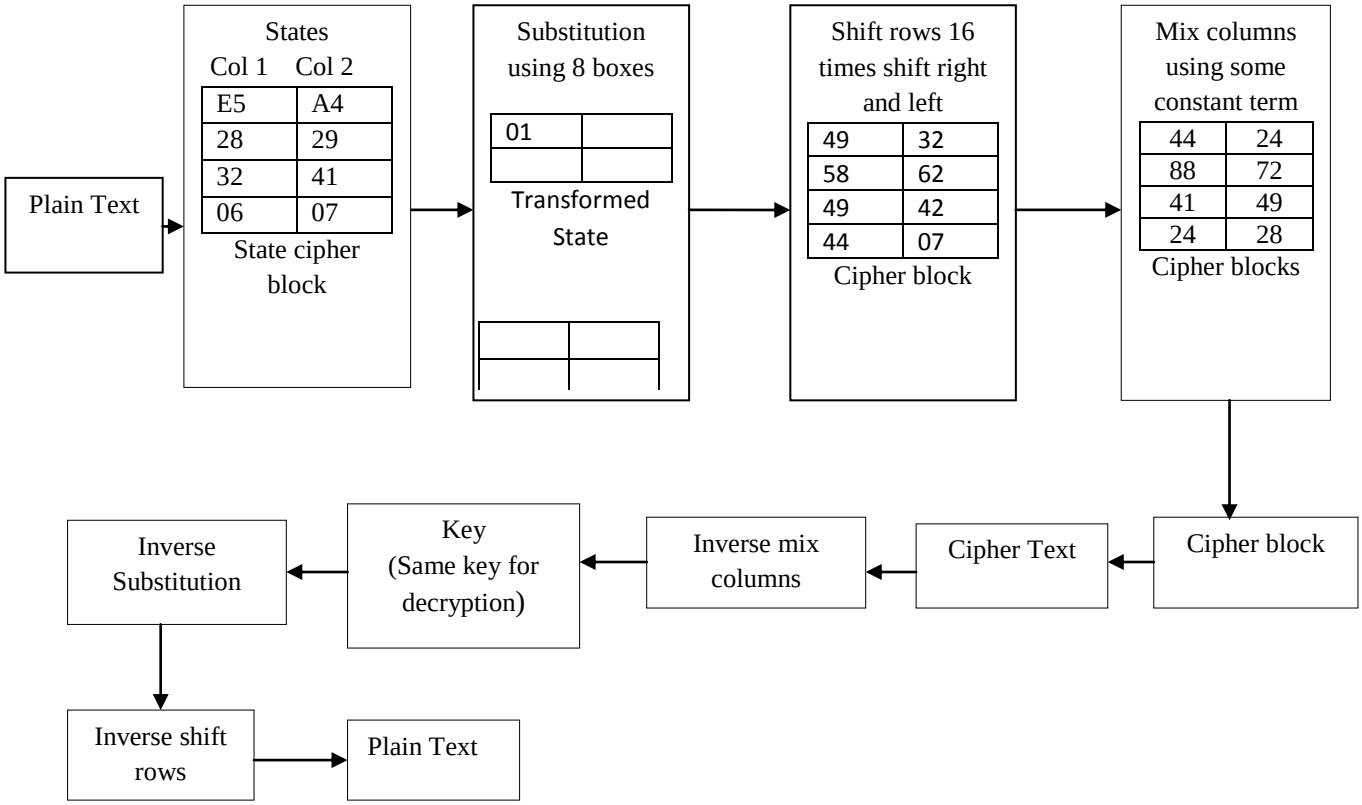

Fig: 1 Block Diagram of Hybrid Approach

6.1 Encoding the message using AES and Blowfish algorithm

a) AES algorithm

- **State Cipher Block**: Block contains fixed number of bits. Block cipher are used to implement encryption of bulk. Plain text is passed through state cipher block where each intersection of row and column represents some data and it would be transformed to another form when its value is looked in the substitution box.

- **Shifting**: Shifting is implemented using >> or << operator. Purpose of shifting is to enhance robustness. There are many operations where shifting is implemented so as to increase level of security.

b) Blowfish Algorithm

- Output of AES is passed through a shift. Some additional constant term are being added so as to increase the level of security.
- Convert the type of the result in double format and subtract some constant term from it. Comparison test is run and shifting is done.
- Convert the coded output to char format to encrypt the message and make it cipher. This is the final message which is in encrypted format.

6.2 Decoding the message

Again the same shifting is applied. Further comparison test is run applying the same condition as did during encryption side. Lastly same number is being subtracted and to show the original message the decoded message is converted to char form.

VII.COMPARISON BETWEEN TWO APPROACHES

i) Security Enhancement: When we consider our approach we used 64 bit key size which means there are 2^{64} bit combinations for anyone to hack the key but in case of existing approach anyone who can find the p & q by factorized n can easily decrypt the message. In simple words present hybrid approach is more secure in terms of hacking the key as combination are more required. Our present approach uses S box, mixing and shifting which further enhances the security and makes it reliable for encryption standard. Encryption using present approach increased randomness and makes more secure than existing approach.

ii) Processing Time and Memory Usage: Present approach is taking less encryption time than existing approach because in RSA+AES we are factoring the large prime numbers which makes computation very large and makes the processing time slow and consume large memory whereas in present approach we have used lookup tables which makes the processing time fast and consume less memory.

VIII. SIMULATION AND RESULT

The simulation was conducted on laptop with windows 64 bit processor i3 and CPU 2.00GHz with 4 GB of RAM. In this paper we compare the performance of existing work i.e. RSA+AES with proposed work i.e. AES+BLOWFISH. For performing the result we used MATLAB. Here we have taken various inputs of text files and compare the results of both the algorithm on the basis of CPU time and memory usage.

TABLE1 Total CPU time of RSA+AES and present work

S. No.	CPU time of RSA+AES	CPU time of present algorithm
1.	1.79561	0.608404
2.	2.76161	0.342567
3.	2.34161	0.748805
4.	1.84241	0.327602

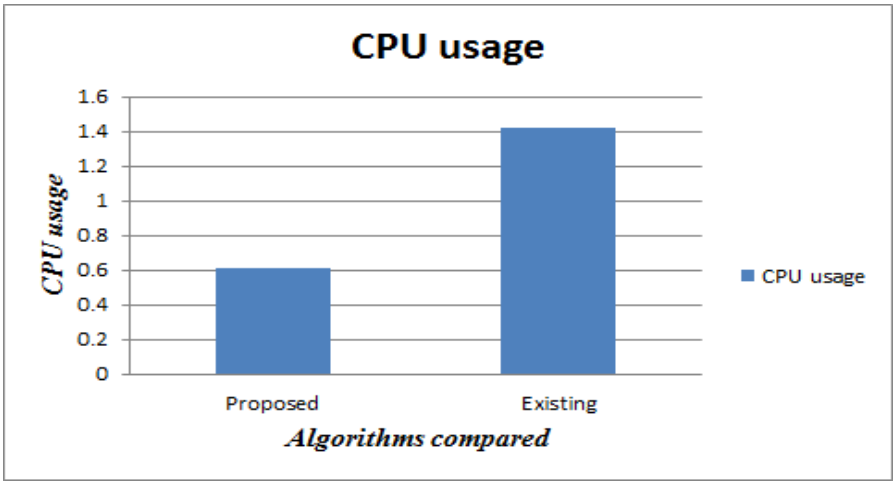

Fig: 2 Comparison results of AES+RSA and proposed work on the basis of processing power

TABLE 2 Memory usages of RSA+AES and present work

S. No.	Memory usage of RSA+AES	Memory usage of present algorithm
1.	1.9867e+09	1.8138e+09
2.	1.48587e+09	1.17902e+09
3.	1.48586e+09	1.17769e+09
4.	2.31299e+09	1.17834e+09

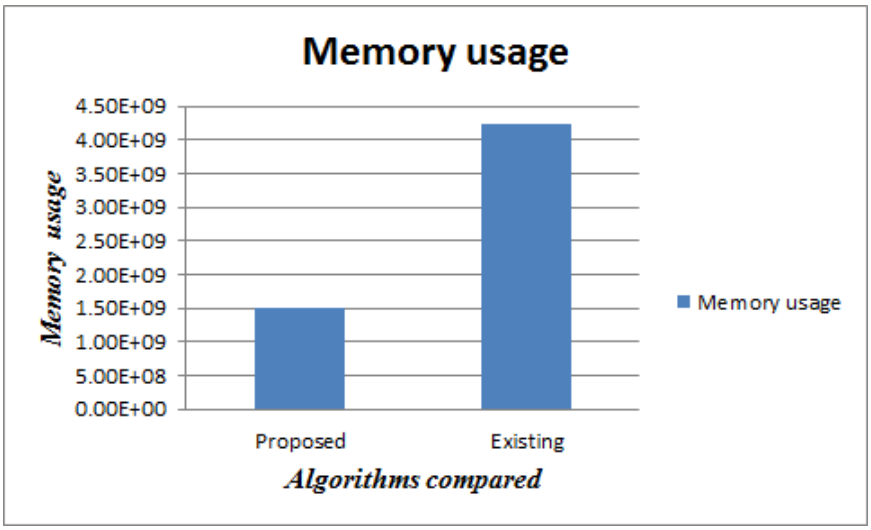

Fig: 3 Comparison results of AES+RSA and proposed work on the basis of memory usage

From the above results we found that hybridization of Blowfish and AES computes less memory and processing power as compare to existing work i.e. RSA+AES. As computation required in case of RSA +AES is a lot more as compared to hybrid symmetric AES+Blowfish. This makes them impractical for encrypting large chunks of data.

IX. CONCLUSIONS AND FUTURE SCOPE

Cloud computing have aim to use systems and services via internet so that it would be easy to access the information. As the data process and store on internet data may hack easily. The existing approach i.e. (AES+RSA) could not remove security partially with minimum processing time and memory usage because anyone who can find the p & q by factorized n can easily decrypt the message. To deal with such security issues we hybridized AES and Blowfish to make the data more secure with minimum processing time and memory usage. Considering Blowfish there is very less weak point and hence can be set as standard for encryption. Taking AES into account, it takes less processing power. In this approach we used 64 bit key size which means there are 2^{64} bit combinations to anyone hack the key. This approach used S box, mixing and shifting which further enhances the security and makes it reliable for encryption standard and use of lookup table makes the algorithm efficient. So BLOWFISH+AES algorithm is more efficient than RSA+AES in terms of security, processing time and memory usage. This research focuses on encryption of message using blocks and shuffling. In the future along with the encryption of content, alert generation system can also be developed compatible with the proposed technology. This enables users or desired person to know when the attack is made. Hence shift to machine learning can be implemented which will transform the proposed work into detection system. Further the proposed work can be further enhanced to survive dangerous attacks. One more aspect of the work can be implemented which can cover wireless networks.

REFERNCES

[1] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy "Cloud Computing: Security issues and Research Challenges" *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, 2011, Page 136-146.

[2] Dinesh Devkota, Prashant Ghimire, Dr. John Burris and Dr. Ihssan Alkadi "Comparison of Security Algorithms in Cloud Computing" IEEE Institute of Electrical and Electronics Engineers, 2015, Page 1-6.

[3] Aamer Nadeem, Dr M. Younus Javed "A Performance Comparison of Data Encryption Algorithms" IEEE Institute of Electrical and Electronics Engineers, 2005, Page 84-89.

[4] Vartika Kulshreshtha, Dr Seema Verma and Dr C. Rama K. Challa "A Comprehensive Evaluation of Cryptographic Algorithms in Cloud Computing" IEEE Institute of Electrical and Electronics Engineers, 2014.

[5] Najib A. Kofahi, Turki Al-Somani and Khalid Ai- Zamil "Performance Evaluation of Three Encryption/Decryption Algorithms" IEEE Institute of Electrical and Electronics Engineers, 2004, Page 790-793.

[6] Lo'ai Tawalbeh, Nour S. Darwazeh Raad S. Al-Qassas and Fahd AlDosari " A Secure Cloud Computing Model Based on Data Classification" *ELSEVIER First International Workshop on Mobile Cloud Computing Systems, Management and Security*, 2015 Page 1153-1158.

[7] Vishwanath S. Mahalle and Aniket K Shahade "Enhancing the Data Security in Cloud Computing by Implementing Hybrid (RSA&AES) Encryption Algorithm" IEEE Institute of Electrical and Electronics Engineers, 2014, Page 146-149.

[8] Nasrin Khanezaei and Zurina Mohd Hanapi "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" IEEE Conference on Systems, Process and Control, Page 2014, 58-62.

[9] Ashwak Alabaichi, Faudziah Ahmad and Ramlan Mahmod "Security Analysis of Blowfish Algorithm" IEEE Institute of Electrical and Electronics Engineers, 2013, Page 12-18.

[10] Tingyuan Nie "A study of DES and Blowfish Encryption Algorithm" IEEE Institute of Electrical and Electronics Engineers, 2009, Page 1-4.