Performance Analysis of Encryption Algorithms with Pat-Fish for Cloud Storage Security

M. Usha and A. Prabhu

Abstract In the era of the Cloud, a remote user connected from anywhere, anytime is provided with any form of access to the storage services. Internet of things is growing rapidly in all aspects and Cloud storage has become an essential aspect in the day to day life. Data Science and Big data analytics, and other technologies use the smart devices like personal Laptop, tablet and smartphone and enterprises are interested to store data and the transactions in Cloud data centres. However, cloud storage needs a secured transaction and authentication system. Cloud service providers need to provide high security at their storage level. Our approach combines Blowfish algorithm and Pattern matching to secure the data in cloud data storage. Pattern matching algorithm is the best algorithm in terms of time complexity and space complexity. Blowfish algorithm is a 16-round Fiestal algorithm, which is used to encrypt and decrypt the input files. This paper evaluates the hybrid Pat-Fish algorithm with DES, RSA, and Blowfish methods on text files. The standard evaluation parameters namely encryption time and decryption time are taken for performance comparison. This Pat-Fish approach yields less time for encryption and decryption compared to DES, RSA and Blowfish algorithms. This method is suitable for cloud storage to store the client data with security.

Keywords Encryption · Decryption · DES · Blowfish · RSA
Pat-Fish · Pattern matching algorithm

M. Usha (✉)
Sona College of Technology, Salem, Tamil Nadu, India
e-mail: usha@sonatech.ac.in

A. Prabhu
PSG Institute of Technology and Applied Research, Coimbatore
Tamil Nadu, India
e-mail: prabhuak@gmail.com

K. J. Kim and H. Kim (eds.), *Mobile and Wireless Technology 2018*, Lecture Notes in Electrical Engineering 513, https://doi.org/10.1007/978-981-13-1059-1_11

1 Introduction

Every day new technologies are mushrooming as per the industry needs and spreading into all the places, to reduce the human effort and to improve seamless services. Industries like to have much more technology [1] in their business world and have a large number of data to be stored. Recent days "Cloud computing" is a trendsetter which supplements all the existing techniques by storing huge volumes of data in a secure way [2].

1.1 Cloud Computing

Traditional applications are so complicated for the user and industry, and a partial amount is to be invested in the hardware and software to run a business. Cloud computing overcome all barriers for storage of the traditional methods. Cloud-based applications can run through the browser with the help of the internet. It has various benefits like self- serving provisioning, elasticity, pay per use, workload resilience, and migration flexibility.

Types of Cloud Computing Services: The cloud offers three types of services. *Infrastructure as a service.* Example: networks, storage and operating systems.

Platform as a service. Example: Web services, application development beds and search engines.

Software as a service. Example: Internet web browser and applications.

Cloud Computing services are available across the globe. Based on the usage and location, it's divided into many types such as Private, Public Cloud and Hybrid Cloud.

1.2 String Matching Algorithms

The World is full of textual information. To get the information using textual queries or image mapping from websites, books and newspapers are needed. In the view of computer science, search engines use many string algorithms. Matching a similar text is called string matching. There are various types of string matching algorithms available [3].

- Naïve string search algorithm
- Rabin–Karp string search algorithm
- Boyer–Moore string search algorithm
- Knuth–Morris–Pratt algorithm
- Bitmap algorithm

Every algorithm has unique features and capabilities. Mathematical implementations calculate the exact patterns in the millions of the texts. Many attempts have been made to exploit the different pattern matching algorithms in cloud and communication networks [4–7].

1.3 Cryptography Algorithms

Cloud computing faces a lot of security issues in the storage and network platforms. Cryptography algorithm is the process to protect data that are sent through communication networks [8]. It is an art of hiding information by encrypting the message. The readable message is converted into an unreadable format is called cipher-text (Fig. 1).

The fundamental set of cryptography algorithms can be divided into three groups:

- Symmetric encryption algorithm
- Asymmetric encryption algorithm
- Hash functions

2 History of Existing Techniques

Symmetric encryption (Private Key): It's a unique key to encrypt and decrypt the data. Asymmetric encryption (Public Key): It is also called as a public key encryption algorithm. The algorithm uses a pair of keys that help to do encryption and decryption.

2.1 Popular Encryption Algorithms

Many symmetric and asymmetric cryptography algorithms have been proposed (Fig. 2) in literature. *Blowfish Encryption Algorithm*. Blowfish [9] was designed in 1993. It is a symmetric key block cipher. It has a key length from 32 to 448 bits and block size of 64 bits. It's a Feistel network. It was designed by Bruce Schneier to replace the DES or IDEA algorithms. Blowfish is a license-free algorithm.

Data Encryption Algorithm (DES). DES [10] is a symmetric key block cipher algorithm and it was discovered in 1972 by IBM. This method was accepted by the United States of America. The key length is 64 bits (56 + 8 parity bits) and block size is 64-bit length. DES handles different mode operations such as CBC, ECB, CFB and OFB. It has some failures when a weak key is used.

Rivest-Shamir-Adleman (RSA) Algorithm. RSA is founded by Rivest, Shamir and Adelman in 1977 [11]. It's an asymmetric cryptographic algorithm and generates two keys: Public Key and Private key. The public key and private key is used to encrypt and decrypt the message respectively.

Fig. 1 Encryption process

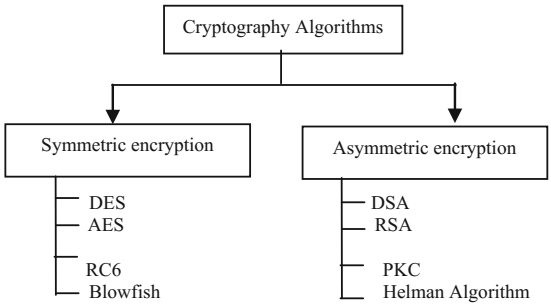

Fig. 2 Types of cryptography algorithms

RSA algorithm consists of three steps:

- Key generation is used to encrypt and decrypt data.
- Data encryption is converting the plaintext to ciphertext.
- The third step is converting the chipper text to plain text.

Key size is 1024 to 4096 bits. RSA is one of the first algorithms and is broadly used for secure data transmission.

Advanced Encryption Standard (AES) algorithm. AES is a symmetric key block cipher algorithm submitted by Joan Daemen and Vincent Rijmen in 1998. AES algorithm supports multiple combinations of key with the length of 128, 192, and 256 bits. 128-bit data are split into basic operational blocks and it's are considered as an array of bytes formed as a 4×4 matrix which is also called as states. For encryption, 10, 12, 14 iterations are used with the key length of 128,192 and 256-bits. Every round of AES uses the order and substitution methods in the network, it is suitable for both hardware and software implementation. Since AES requires more processing power [12] it is not taken for comparison in this work.

3 Evaluation Metrics

The following evaluation metrics are used and compared with the existing techniques which are normally adopted by researchers [13].

i. Encryption Time
ii. Decryption Time
iii. Throughput

3.1 Encryption Time

The number of cycles executed to convert from plain text into cipher text is called encryption time. Encryption time is based on key length and input file size. In our

experimental setup, encryption time is measured in milliseconds and based on the performance of the system.

3.2 Decryption Time

The time taken to convert plain text from cipher text is called decryption time. The decryption time is normally very less than the encryption time. Decryption time is used to measure the performance of the system and it's quite faster than encryption algorithm. Decryption time is measured in milliseconds.

3.3 Throughput

Throughput is calculated based on the file size and execution time. The number of resources (MB/milliseconds) executed at a particular time (MB/milliseconds) is called throughput using the following formula:

$$\text{Throughput} = \text{File size}/\text{Execution time}$$

4 Proposed Method

To enhance the Cloud storage security, a combined approach, Pat-Fish is proposed which is a combination of Blowfish with Pattern Matching. The block diagram of the proposed method is shown in Fig. 3. The Pat-Fish method has two phases:

i. Authentication Phase
ii. Cloud Data encryption Phase

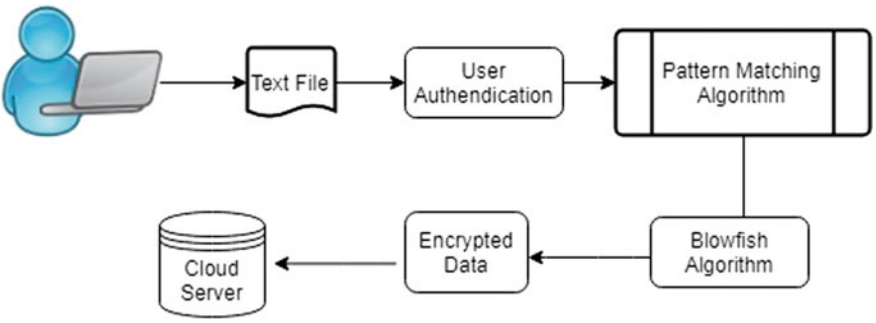

Fig. 3 The block diagram of proposed method

4.1 Authentication Phase

Authentication is an important process to allow the authorized users to access the application. In this process, data sets are compared with the database of authorized users' information within an authentication server.

If the user credentials are matched with the existing data set, then the user is permitted to access the application. During authentication, the user or computer has to get the authorization from the server or client.

4.2 Cloud Data Encryption Phase

In this phase, two existing algorithms, namely the Pattern Matching algorithm and Blowfish algorithm are combined together for fast encryption. The input data is subdivided column-wise using pattern matching technique, the pattern matching takes into account a data 'D' of length 'n' and a pattern of length 'm' with sub-dividing the entire data into the columns. The portioned data is then encrypted with the help of the Blowfish algorithm.

Blowfish Encryption Algorithm. Blowfish is a 64-bit block cipher encryption algorithm. There are two ways to implement the blowfish algorithm through via software and hardware (Fig. 4).

This structure is known as a Fiestal network. Blowfish has 16- Fiestal rounds. The block size is divided into two parts such as left-hand side 32-bits and right-hand side 32-bits. The input divides a 32-bit into four 8 bytes. The output results are added, XORed and swapped in this function. Blowfish algorithm has a set of procedure used to decrypt as well as encrypt the input text. It has the following two functions.

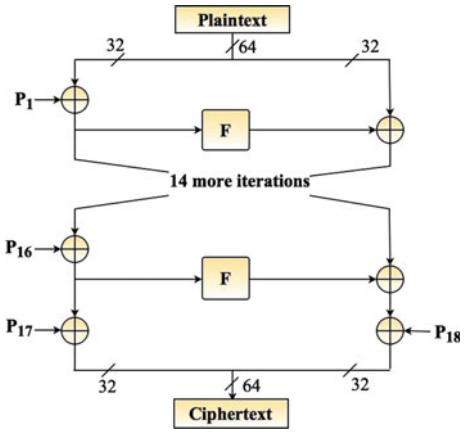

Fig. 4 Graphical representation of blowfish Algorithm

- Key Expansion
- Data Encryption

Key-expansion. The 448 bit key is separated into 4168 bytes. The P-array consists of 18, 32 bits (P1, P2… P18). The following steps are used to calculate the subkeys:

1. P-array and four S-boxes are initialized. The string contains the hexadecimal values obtained from Pi. P1, P2, P3, P4 array values are generated by Key Generator.
2. Right-hand side 32-bits are XORed with P1 of the key, left-hand side 32-bits are XORed with P2 of the key. Encrypt the all-zero string with the Blowfish algorithm.
3. Exchange P1 and P2 (2).
4. Encrypt the exchanged values (3) using the algorithmic procedure with the subkeys.
5. Exchange P3 and P4 (4).
6. Continue the process and concatenate x = mL and mR values.

Data Encryption. The 64-bit input data is divided into two 32-bit halves, which are labeled as the left halves (LH) and right halves (RH). The Blowfish algorithm executes the first 32-bit left half and the P-array performs the XOR function. The outcomes are furnished to the function (FmL). Subsequently, the XOR function is executed for both left halves and the next 32-bit right halves elegantly. This is followed by the swapping of both outcomes. The rest of the round continues until it reaches 16th round.

Four 32-bit S-Boxes consist of 256 entries each:

S1 1, S1, 2 … S1, 256
S2 1, S2, 2 … S2, 256
S3 1, S3, 2 … S3, 256
S4 1, S4, 2 … S4, 256

Process of F_{ml} function. The F_{ml} function executes 32-bit S-boxes, with each one encompassing 256 entries. In this Blowfish technique, the first 32-bit left half is subdivided into four 8-bit blocks such as m, n, o and p. The Eq. (1) gives F(mL) function in detail [9].

$$F(mL_H) = ((S_{b1,m} + S_{b2,n} \bmod 2^{32}) \oplus S_{b3,o}) + S_{b4,p} \bmod 2^{32} \quad (1)$$

Data Encryption algorithm:

Step 1: Get the input file ‘m’
Step 2: ‘m’ is divided into two 32-bit, named as mL, mR
Step 3: For i = 1 to 32, and do the XOR operation with the Key (Pi)

$$mL = mL \text{ XOR } Pi$$

$$mR = F(mL) \text{XOR } mR$$

Step 4: Swap mL and mR

5 Results and Discussion

The experiments were run in NetBeans with CloudSim. The performance of the algorithm compared for encryption time and decryption time with the DES, RSA and Blowfish algorithms. The Pat-Fish approach encryption runtime is compared in Fig. 5.

The bar charts in Fig. 5 show the encryption times for the various file sizes. It is shown that whenever the file size increases the encryption time also increases linearly (Fig. 6).

The decryption time is always low compared with the execution of encryption time. This approach proves the decryption time is lower than the encryption time.

The throughput and average run time of Pat-Fish algorithm are calculated using the encryption time with various files sizes as given in Table 1.

The Tables 2 and 3 show the performance comparison of Pat-Fish's encryption and decryption time using 1, 2, 5 and 10 MB text files. Based on these values Pat-Fish algorithm is far better than DES, RSA, and Blowfish algorithms. Normal encryption method encrypts the text only, but encryption algorithm separates the text file using a pattern matching algorithm. The fragmented file encrypted by Blowfish algorithm and cipher-text file stored in the Cloud server. The authors have

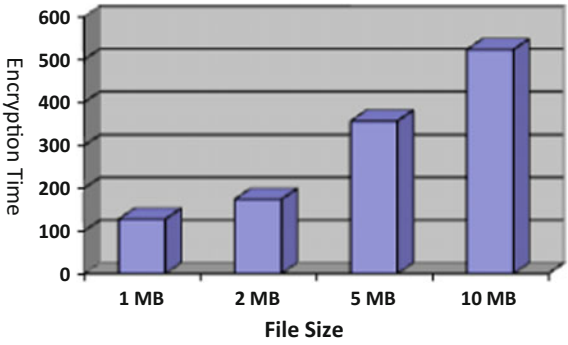

Fig. 5 Pat-Fish algorithm encryption time graph

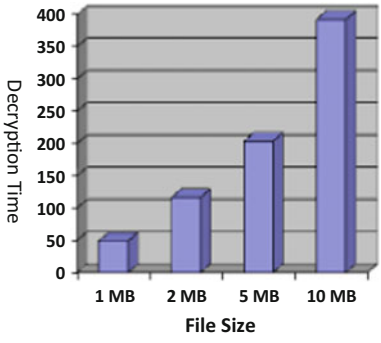

Fig. 6 Pat-Fish algorithm decryption time graph

Tabel 1 Execution time for Pat-Fish

File size	Pat-Fish algorithm (in ms)
1 MB	127.5
2 MB	173.9
5 MB	391.70
10 MB	523.42
Average run time	295.30
Throughput (MB/s)	14.79

Table 2 Performance comparison of encryption time

File size	DES (in ms)	RSA (in ms)	Blowfish (in ms)	Pat-Fish (in ms)
1 MB	136.2	425.6	133.2	127.5
2 MB	269.6	710.9	192.6	173.9
5 MB	665.4	1710.9	373.6	356.4
10 MB	1325.2	2352.24	752.80	523.42
Average run time	599.10	1299.91	363.05	295.30
MB/s	7.51	3.46	12.39	14.79

Table 3 Performance comparison of decryption time

File size	DES (in ms)	RSA (in ms)	Blowfish (in ms)	Pat-Fish (in ms)
1 MB	144.6	375.80	50.2	48.1
2 MB	269.6	541.68	126.3	107.8
5 MB	690.9	995.70	210.7	187.3
10 MB	1874.35	1897.35	521.47	392.18
Average run time	744.86	952.63	227.16	203.84
MB/s	6.04	4.72	19.80	24.47

proposed the time complexity reduction using finite automata [14] in cloud virtualization in their previous work. Combined with the security aspect proposed in this paper, a framework is now established for cloud data centres.

6 Conclusion

In this research paper, DES, RSA and Blowfish algorithms are compared with Pat-Fish. The results show that the Pat-Fish approach's performance is better than other encryption algorithms. 1 MB, 2 MB, 5 MB and 10 MB files are evaluated for the encryption and decryption times. The proposed Pat-Fish method improves the performance by 11% compared to Blowfish technique.

In future, this algorithm will be tuned to improve the efficiency by combining the data center selection [15] too. Space complexity analysis of Pat-Fish and a separate hardware implementation are to be taken up in future.

References

1. Mohammad A (2014) Cloud of things: integrating internet of things with cloud computing and the issues involved. In: Proceedings of 11th IEEE international Bhurban conference on applied sciences and technology IBCAST, pp 14–18
2. Christos S (2016) Secure integration of IoT and cloud computing. Future Generation Comput Syst 78:964–975
3. Priyadarshini P (2016) A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. In: International conference on information security & privacy—Elsevier Procedia computer science, vol 78, pp 617–624
4. Kavitha P (2016) Anomaly based intrusion detection in WLAN using discrimination algorithm combined with naïve Bayesian classifier. J Theor App Info Technol 62(1, 3):646–653
5. Usha M (2017) Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier. Wireless Netw 23(8):2431–2446
6. Abdel-Karim Al Tamimi (2008) Performance analysis of data encryption algorithms, available at https://www.cse.wustl.edu/∼jain/cse567-06/ftp/encryption_perf/
7. Prabhu A (2018) A Survey on the pattern matching algorithms in cloud computing. In: National conference on emerging trends in signal and image processing, communication, VLSI design and nano technology (NCSICVN-18), pp 38–43
8. Hussain I (2013) Improved approach for exact pattern matching (Bidirectional exact pattern matching). IJCSI Int J Comput Sci Iss 10(3):59–65
9. Schneier B (1993) Description of a new variable-length key, 64-Bit block cipher (Blowfish). In: Fast software encryption, cambridge security workshop proceedings, Springer, pp 191–204
10. Data Encryption Standard (1999) Federal Information Processing Standards Publication No. 46, National Bureau of Standards
11. Rivest RL (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
12. Sanchez-Avila C (2001) The Rijndael block cipher (AES proposal): a comparison with DES, Security Technology, In: 2001 IEEE 35th international carnahan conference on. IEEE, pp 229–234
13. Bijoy K (2013) Designing and performance analysis of a proposed symmetric cryptography algorithm. In: International conference on communication systems and network technologies-ieee computer society, pp 453–446
14. Prabhu A (2015) Nondeterministic finite automata to reduce the time complexity in cloud virtualization. Int J Appl Eng Res 10(37):28021–28025
15. Prabhu, A A Secured best data centre selection in cloud computing using encryption techniques. Int J Business Intell Data Mining (Accepted for publication). https://doi.org/10.1504/ijbidm.2018.10007299