Journal of Mathematical Control Science and Applications
Vol. 7 No. 2 (July-December, 2021)

Submitted: 25th August 2021 *Revised: 30th September 2021* *Accepted: 20th November 2021*

CRYPTOGRAPHIC ALGORITHM FOR CLOUD SECURITY

[1]K. RAMAKRISHNA REDDY, [2]O. SRI NAGESH, [3]NAGAMANI.C,
[4]M.VENU GOPALACHARI , [5]Y.AYYAPPA.

4

Abstract. Information is now exchanged over global networks in the form of digital bits and bytes. Personal computers are used to store, separate, and transmit sensitive information. Due to the crucial function that information plays, hackers are using personal computers to access communication programs in order to either steal sensitive data or even disrupt a major info system. The information security is decreased because there is unquestionably no difference between client-side and cloud-based encryption. The goals of the security system can be achieved by encryption algorithms with strong security in place and a respectable promptness restriction. As a result, the performance analysis is crucial for the basic encryption methods. The merging and alteration of the MD5 and Blowfish encryption algorithms in this paper's proposed innovative hybrid cryptographic algorithm for cloud security can increase security.

Keywords: DCT-Divide and Conquer Tables, SED2-Secure Efficient Data Distributions, ED Con-Efficient Data Conflation, AD2-Alternative Data Distribution, SA-EDS -Security Aware Efficient Distributed Storage, BPMN -Business Process Modelling Notations

1. Introduction

Today's new growing sector for services that are dynamically offered through the internet using hardware and software virtualization on demand is cloud computing, also known as distributed computing [3]. The greatest benefit of cloud computing, according to user needs, is the adaptability of resource release and leasing. Additionally, the cloud service providers provide two reservation plan types: short-term and long-term. Insightful cloud computing organization includes features like security, transparency, scalability, and monitoring. Cloud computing is a new trend where storage capabilities are independently transferred to service providers. Users are reluctant to accept cloud services since direct control over outside data is lost. For the purpose of developing a cloud computing system that is more secure, platforms for services and degrees of application software are taken into account. Information security in cloud computing can be accomplished through the encryption of the data. Users encrypt the data by storing or processing it in cloud-based cryptography to prevent unauthorized access. The system-level design and execution of information encryption, which is characterized as cloud computing with encrypted data [4,5,6], have traditionally received the majority of attention. Data transmission and storage are made possible by the cloud system built on encryption. Certification and categorization, which are assigned using the public-key and private-key or the private-key alone, are essential steps in the information transmission process. Client and cloud establish a relationship in this They use their own understanding of logical relationships as the foundation for the description of data identification and the cloud Client independent way.

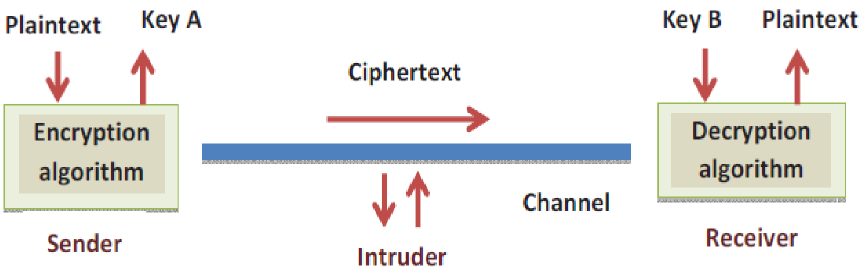


Figure: 1 encryption and decryption process

Spammers and hackers that want to alter, amend, or remove material being transferred abound in the online world. Other times, an external component, such as electromagnetic fields around a wire, may have an impact on some bits. There is no guarantee that the message will be received exactly as intended by the recipient. This article describes the hashing methods MD5 and SHA1. It is a technique to guarantee confidentiality and make sure the right data is received on the other end. In order to comprehend its importance in the field of forensic analysis and truth-seeking, it delves deeper into this subject. For additional information, continue reading.

HASHING

It involves giving the source text a mathematical function of any length. Create a message digest, also known as a hash value, which can be used to obtain data from storage more rapidly or for security checks.

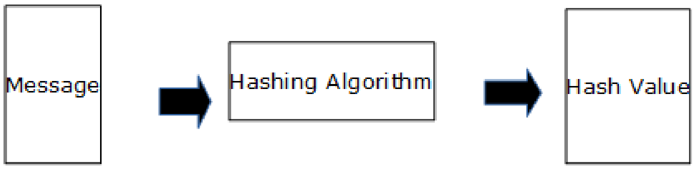


Figure 2. Hashing

2. Definition of Hash Function

These mathematical procedures, h(), take input X and result in output h. (x). It obtains a name digest while also compressing the data into a smaller representation. A hash sum is typically produced using two fixed-size blocks of data with a size between 128 and 512 bits.

2.1 Working of a Hash Function

Each byte of the message is separated into blocks. These become the input for a binary operation with two possible values. The original text is the other; the first is a preset string. It outputs a string that is a fixed length. Depending on the algorithm, every data block is different.

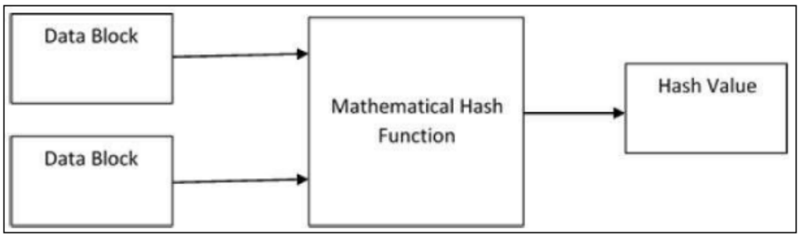


Figure 3. Hashing Prototype

In order to increase security, this study suggests a brand-new hybrid cryptographic method that combines and modifies the MD5 and Blowfish encryption algorithms. A hybrid MD5-Blowfish cryptographic calculation is created in order to get over the limitations of symmetric block cryptography and hash function approaches.

3. Related Work

A well-organized Remote Data Auditing (RDA) procedure is presented for the storage in cloud systems in [1].It is based on the algebraic signature property and has low processing and communication expenses. A brand-new data format called DCT successfully enables dynamic data structures including insertion, add, removal, and modification. Comparing their approach to other state-of-the-art RDA methodologies demonstrates how the security and efficiency improvement approach is at reducing auditor and server computing and communication costs. [2] highlights how some cloud applications are constrained due to important difficulties with data confidentiality and safekeeping, one of which is that sensitive information is accessible to cloud service providers. They suggested a clever cryptographic strategy that would prevent cloud operators from directly accessing incomplete data. The method employed and supported by the algorithm given, which consists of SED2, ED Con, and AD2 algorithms, is known as the SA-EDS model. This proposed approach stores the data on dispersed cloud servers after partitioning the data file. The overall evaluation of the cloud and data security literature is done in [3]. Examples of the security designs of two cloud service providers are provided, and the use of BPMN is described as a service offering security design and data security. In any situation of a security breach, BPMN can be used to pinpoint the attacks on the security service area. [4] suggests a secure and efficient privacy-preserving technique that outsources data from mobile devices with limited resources to the cloud and encrypts the data using a probabilistic public-key cryptographic algorithm using ranking keyword search, the file is still retrieved from the cloud despite data encryption. This approach seeks to develop an adequate data encryption system without compromising data privacy. A method for maintaining the security and integrity of data is described in [5]. The RSA Partial Homomorphic and MD5 hashing techniques are combined in this method. In this example, the data is encrypted with RSA Partial before being uploaded to a cloud provider. The MD5 hashing algorithm determines the file's hash value after uploading it. The next stage is where all of these viewpoints go through encryption and decryption, uploading data to the cloud, encoding, and validation examines the issue of sub-tree scaling privacy protection on the cloud over large amounts of data in [6], and a hybrid strategy is suggested that combines Top-Down Specialization (TDS) and Bottom-Up Generalization (BUG) (TDS). The hybrid method, which compares k-anonymity user-specified parameter values with the workload balancing point, automatically selects two of the components. Designing Map Reduce jobs in series allows for both BUG and TDS to be accomplished in a highly scalable manner. [7] suggests decryption and encryption methods such as taking into account RC4 and

RSA for more information, which is utilized in cloud computing for storage security of data. The service providers are in charge of installing email and cloud-based server administration software. Data security is a big risk or concern that still affects how easily people may access work and business. Customers have high expectations, and cloud computing only has one security architecture layer. Their computer system is well-organized, with data storage, processing, and bandwidth all being centralized.

4. System Model:

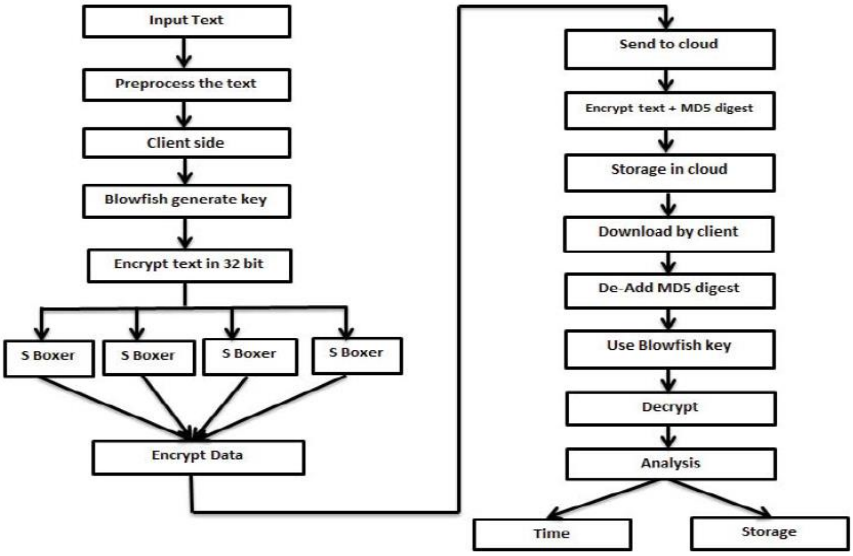


Figure 4. System prototype

1. Steps for a system model:
2. First, enter the text to be processed.
3. Client-side Blowfish technique key creation in step two (as shown in the key generation).
4. To encrypt the text, the 64-bit string is split into two 32-bit halves (as shown in the encryption algorithm).
5. The fourth phase in data encryption involves calculating the P-arrays and four S-boxes.
6. The data is uploaded to the cloud in step five.
7. The output of the MD5 algorithm's message digest generation is saved in the cloud.
8. The message digest is once more appended on the client-side after the encrypted data has been retrieved from the cloud.
9. Using a Blowfish key to decrypt the data.
10. Based on two primary parameters, the method is evaluated: storage

5. Algorithm

In order to improve security, this study suggests a new parallel cryptographic method that combines and replaces the MD5 and Blowfish encryption algorithms. To resolve the drawbacks of symmetric key cryptographic techniques and hash techniques, a hybrid Blowfish MD5 cryptographic algorithm is developed.

Blowfish consumes a key span extending from 32 bits to 448 bits and a chunk size of 64 bits. There are two sections to the algorithm. A key-expansion component is one, and a data-encryption component is another. Several subkey arrays totaling 4168 bytes can be created from a key of no more than 448 bits. In the 16-round Feistel cypher, big, key-dependent S-boxes are used. A key-dependent permutation and a key-dependent replacement are both included in each cycle. It also has a structure in common with CAST-128, which similarly uses fixed S-boxes. As user key associations and sub-key complexity increase, so does the level of security.

Algorithm 1: Blowfish

Encryption:

```
1: First, type the character (64-bit), X.
2: The text is split into the 32-bit XL and XR portions.
3: From 1 to 16 for I:
        XL =XL xor PI
        F (XL) xor XR XR = F
        Exchanged are XL and XR.
        Then I again switched XL and XR
        P17 = XR = XR xor
        XL = P18 or XL
        Mix XL and XR.
4: Determine Function f: There are four eight-bit quarters in XL: A, B, C, and D are the variables in f(XL) = ((S1, A + S2, B mod 232) XOR S3, C) + S4, D mod 232
```

Decryption:

With the exception of using P1, P2,...P18 in reverse sequence, the decryption process is same.

Key Generation:

S boxes and P arrays are initialized in step 1.

In step 2, key bits are XO Red with P arrays (P1 XORs 32 bit keys first, P2 XORs 32 bit keys next, etc.).

3: Using the manner described above, all zero strings are encrypted.

4: This new output comes from P1 and P2.

5: Using sub-keys, the new P1 and P2 are encrypted (modified).

6: P3 and P4 are the newly generated outputs.

7: After repeating step 6 521 times, calculate a new P-array and 4 S-boxes.

B. *MD5 Hashing Algorithm*

The information message in the MD5 (Message-Digest algorithm) is divided into 512-bit blocks (each with sixteen 32-bit sub-blocks). Following a series of processes, MD5 generates a 128-bit message process with four connected 32-bit document integrity barriers.

Algorithm 2: MD5

Step 1: The input bit count is verified.

Step 2: Increasing the message input's (MI) bit count so that the resulting data length equals 512 times (additional bits are 0 1 0..........0).

Step 3: Add 64-bit MI to the result from Step 2 to obtain the output, which is represented as m.

Step 4: Blocks from m to b are separated (512 bit each).

Step 5: Each block has 32 bits and goes from b(blocks) through x(16 blocks).

Step 6: The algorithm consists of 4 rounds, each of which has 16 steps (64 steps in total).

Step 7: Four shift registers with 32 bits and hex. Values are displayed as:
reg a= [7 6 5 4 3 2 1 0] 32- bits [a]=[d]
Regulated as [f e d c 8 a 9 7] 32- bits [b]=[c]
[8 9 a b c d e f]
32- bits [c]=[d]
reg d= [0 1 2 3 4 5 6 7]
32-bits [d]=[a]

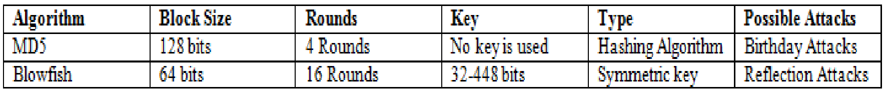
Step 8: Temporarily storing the values of a, b, c, and d in the corresponding spaces aa, bb, cc, and dd.

Step 9: The processing of the algorithm includes 4 rounds with different f, g, h, and I functions. The following single-step function operation:
A is equal to B plus ((a + f(b, c, and d) + xi[k] + t[i] S, where xi[k] is the 32-bit kth word of the left circular shift of S bits. Add output to first round input at the end of each of the four rounds.

10. Obtaining 128 bits of output.

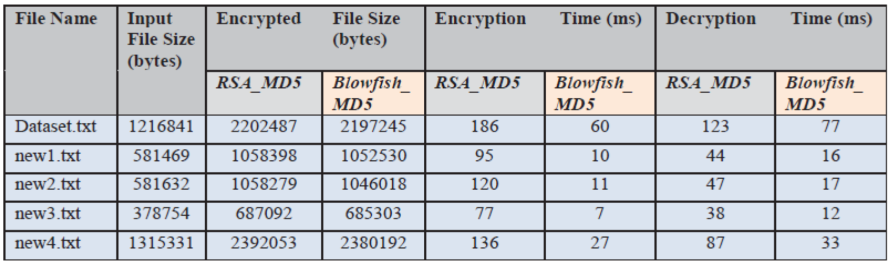
6. Result and Discussion

Comparative examination of the hybrid encryption algorithm is provided in the tables below. A table of experiment results shows a comparison of the encryption file sizes for Blowfish-MD5 and RSA-MD5 (Rivest, Shamir, and Adleman encryption algorithm with message digest hashing technique). The effective performance for the cloud environment is examined through the comparison of these two hybrid algorithms. Table1 Shows the comparison of MD5 and Blowfish algorithm based on block size, key and number of rounds [8].



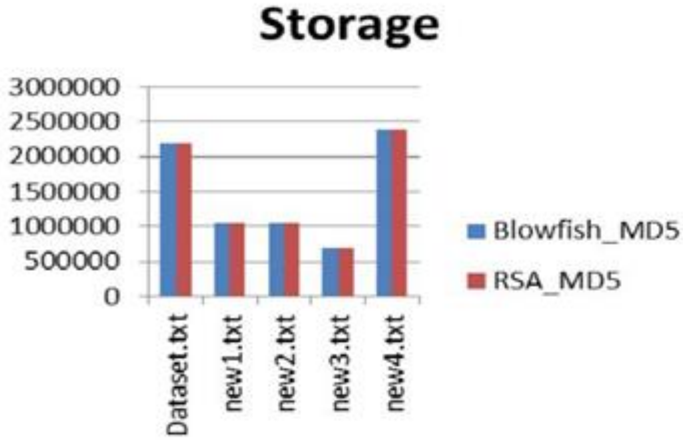
Algorithm	Block Size	Rounds	Key	Type	Possible Attacks
MD5	128 bits	4 Rounds	No key is used	Hashing Algorithm	Birthday Attacks
Blowfish	64 bits	16 Rounds	32-448 bits	Symmetric key	Reflection Attacks

Table 2. Table of RSA_MD5 and Blowfish_MD5 comparision



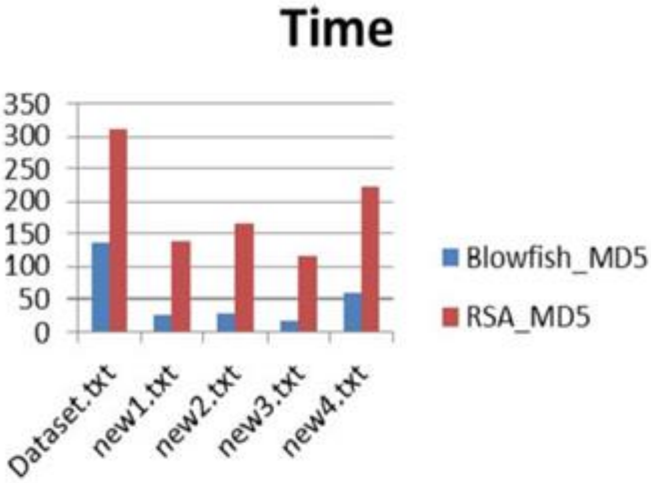
File Name	Input File Size (bytes)	Encrypted	File Size (bytes)	Encryption	Time (ms)	Decryption	Time (ms)
		RSA_MD5	*Blowfish_ MD5*	*RSA_MD5*	*Blowfish_ MD5*	*RSA_MD5*	*Blowfish_ MD5*
Dataset.txt	1216841	2202487	2197245	186	60	123	77
new1.txt	581469	1058398	1052530	95	10	44	16
new2.txt	581632	1058279	1046018	120	11	47	17
new3.txt	378754	687092	685303	77	7	38	12
new4.txt	1315331	2392053	2380192	136	27	87	33

The outcomes achieved in the framework of the storage size constraint are improved in cases where the projected approach is used, as can be seen from the tabular results above. As the data is encrypted using the Blowfish MD5 algorithm's construction of S-boxes, pipeline-based parallel processing quickens the execution process, cutting down on execution time.



Graph 1: RSA MD5 and Blowfish MD5 encrypted file sizes are contrasted.

The graph above displays a comparison of the two-hybrid encryption methods. The hybrid Blowfish-MD5 algorithm takes less time to encrypt data than the RSA-MD5 approach, as demonstrated in the graph above.



Comparison of the encrypted times for RSA MD5 and Blowfish MD5 is shown in graph two.

The assessment of the two-hybrid encoding techniques is revealed in the graph above. According to the diagram above, the hybrid Blowfish-MD5 technique takes less time to encrypt and decode data than the RSA-MD5 approach.

8. Conclusion:

This work proposes a novel parallel cryptographic technique that combines and alters the MD5 and Blowfish encryption algorithms to improve security. The constraints of symmetric block cryptography and hash function methods are overcome via a hybrid MD5-Blowfish cryptographic calculation. The performance of the suggested technique is compared to the hybrid RSA and MD5 algorithms using two criteria: storage and time. Faster than the hybrid RSA-MD5 system is the hybrid Blowfish-MD5 algorithm. So far, blowfish-MD5 has shown to be more effective than the first suggested approach.

References:

[1] Sookhak, Mehdi, et al. "Dynamic remote data auditing for securing big data storage in cloud computing." Information Sciences 380 (2017): 101-116.

[2] Li, Yibin, et al. "Intelligent cryptography approach for secure distributed big data storage in cloud computing." Information Sciences (2016).

[3] Ramachandran, Muthu, and Victor Chang. "Towards performance evaluation of cloud service providers for cloud data security." International Journal of Information Management 36.4 (2016): 618-625.

[4] Pasupuleti, Syam Kumar, Subramanian Ramalingam, and Rajkumar Buyya. "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing." Journal of Network and Computer Applications 64 (2016): 12-22.

[5] Priyanka Ora and Dr.P.R.Pal, "Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography" IEEE International Conference on Computer 2015.

[6] Zhang, Xuyun, et al. "A hybrid approach for scalable sub-tree anonymization over big data using MapReduce on a cloud." Journal of Computer and System Sciences 80.5 (2014): 1008-1020.

[7] Prof Swarnalata Bollavarapu, Bharat Gupta, 'Data Security in Cloud Computing, Volume 4, Issue 3, March 2014

[8] L. Kranthi Kiran, J.E.N. Abhilash, P. Suresh Kumar, "FPGA Implementation of blowfish Cryptosystem Using VHDL", International Journal of Engineering Research & Technology, pp. 1-5, 2013.

K. RAMA KRISHNA REDDY: Professor, Department of CSE (AI & ML), Vignan Institute of Technology and Science, Deshmukhi (V), Pochampally (M), Yadadri-Bhuvangiri (Dist)-508284, TS, India.
Email: ramakrishnareddy524@gmail.com

O.SRI NAGESH: Professor, Department of CSE , Vignan Institute of Technology and Science, Deshmukhi (V), Pochampally (M), Yadadri-Bhuvangiri (Dist)-508284, TS, India.
Email: nagesh.osri@gmail.com

Nagamani.C: Associate Professor, Department of CSE, Malla Reddy College for Women (A), Hyderabad, TS, India.

M.Venu Gopalachari: Associate Professor, Department of IT, Chaitanya Bharathi Institute of Technology, Hyderabad, TS, India.

Y.Ayyappa: Department of CSE, Koneru Lakshmiah Education Foundation, Guntur, Andhra Pradesh, India.