International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

Enhancing the Integrity of Cloud Computing by Comparison between Blowfish and RSA Cryptography Algorithms

Randa Mohamed Abdel Haleem
Department of Computer Science
King Khalid University
Abha, Saudi Arabia

Eltyeb Elsamani Abd Elgabar
Department of Computer Science
Al Neelain University
Khartoum, Sudan

***Abstract*— Cloud computing is a new architecture that has released users from hardware requirements and complexity but the rapid transition toward clouds has many concerns related to security.The algorithms that exist now whether they are symmetric or asymmetric still have some loopholes that expose them to violations and attacks. Thus, to address this issue we propose in this paper a new encryption algorithm by hybrid some features of (RSA)and (Blowfish) algorithms that are applied to data for more security and integrity, we discuss their features and weaknesses, and compare with RSA and Blowfish, this new hybrid algorithm increasing the security and reliability of cloud computing and improves thereby creating a secure platform for business applications and IT infrastructure information to become more reliable and thus increases the adoption of companies migrating steadily to cloud computing and transfer their data and applications to the cloud full safely.**

Keywords-Cloud computing; Security; Privacy; Data ;Algorithm ; Cryptography, RSA, Blowfish .

I. INTRODUCTION

The cloud computer is vulnerable to attack so the study of encryption algorithms and the methods used in computer fasteners is considered one of the most challenges concerning the key issues that must be addressed consistently with the stunning development of the technology overall online accreditation in all aspects of practical life and institutions[1].

Cloud computer security:

When writing about security in cloud computing, the following elements must be addressed:

A. *Identity management:*
Where there must be a special department to identify the data requester and verify its identity.

B. *Data protection:*
The responsibility for preserving the data lies with both the service provider and the customer, as it is his responsibility not to disclose his confidential data, which makes it easy to access and attack his data.

C. *Privacy Policy:*
It must clearly contain the privacy policies that fully preserve the rights of the customer and the rights of the service provider alike. It is considered one of the strongest criteria that measures the strength of cloud service providers.

D. *Application security:*
Where the service provider must provide applications that enjoy a high degree of security and inability to penetrate.
Privacy issues are a very big concern for cloud computing users, as some sensitive information whose leakage to unauthorized users is considered one of the biggest problems that may stop the spread of cloud computing use, identity management solutions(IDM)by maintaining user data, where it tracks sensitive information , manages how it is used, and verifies that the service provider applies all required policies for the privacy of sensitive data[2].

II. ENCRYPTION AND DECRYPTION ALGORITHM

This

Encryption, in general, is the process of maintaining the confidentiality of information using the programs that have the ability to encrypt the information into symbols, if the encryption file is accessed by persons not authorized cannot understand anything, the strength of encryption and effectiveness of algorithm depends on two basic factors, the types of algorithms, and the length of the key which is increased the proportion of safety and the difficulty of decoding the code[3].

Cloud encryption is one of the most important topics that are researched in the field of cloud computing, where encryption is defined as the science that combines mathematical sciences and data technology and focuses on three aspect[4] :

- Data integrity.
- Reliability Authenticity
- Security Confidentiality

There are two encryption systems:

A. *Symmetric systems:*
It is considered one of the very old and traditional methods of encryption between two sides, and it was used to encrypt messages in the past and even before the advent of the computer.
Types of symmetric encryption are DES, AES, Triple DES, and Blowfish algorithms[5].

B. *Asymmetric coding systems:*
Asymmetric algorithms were invented in the last quarter of the twentieth century after the one-way mathematical relationship reported by Davy and Hillman was discovered. It is more complex than the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

symmetric algorithm and differs from symmetric algorithms in their speed of operation, the robustness of safety, and also in their suitability for some applications. In the asymmetric encryption process, data is encrypted and decrypted by two different keys, one used for encryption and the other used for decryption:

Public key: The public key is recognized by anyone and enables the person to encrypt the data.

Private key: The private key is recognized only by the designated person receiving the message and is used to decrypt and verify the authenticity of signatures.

One of the early and widely used algorithms that implement this principle is the RSA algorithm[6].

III. PREVIOUS STUDIES

This paper [7]proposed a modified blowfish algorithm that uses a 128-bit block size and a 128-bit key, maintaining the original structure of blowfish for a smooth migration with a reduced number of s-boxes to provide less memory consumption.

Study [8]authors design secure cloud storage for healthcare data by using a Hybrid cryptographic technique. Within this, the data are encrypted through the asymmetric algorithm, and keys are encrypted using an asymmetric algorithm. The performance evaluation, as well as the security of the proposed method, was measured and compared to an existing technique.

Study [9]designs and studies distributed RSA encryption algorithm based on the distributed file system and programming model. It is proved that the distributed encryption algorithm can optimize the operation speed and can be applied to the processing of massive data.

Study [10]proposed algorithm reduces the time of encryption and decryption processes by dividing the file into blocks and enhances the strength of the algorithm by increasing the key size. This strength paves the way to store data in the cloud by the users without any inconvenience.

IV. BLOWFISH AND RSA ALGORITHM

The blowfish algorithm is one of the types of symmetric encryption algorithms developed by Bruce Schneier. This algorithm can be used instead of the Data Encryption Standard (DES) because of its advantages. This algorithm takes different lengths for its key (from 32 bits to 448 bits), where the length key ranges between these two mentioned numbers. This makes it ideal and has a high speed compared to the Des algorithm. At the time of the development of this algorithm, most cryptographic algorithms were of limited use or rather protected by patents, government secrecy, or the intellectual property of the developing company, as no one could use it. However, Bruce Schneier published the blowfish algorithm as a public domain where anyone has the right to use it for free and licensed[11].

The prime factors for Blowfish include a table search, as well as the presence of the XOR function. The table includes four Xbox boxes and a description of P[12].

The Blowfish algorithm is a cryptographic code based on Feistel rounds, and the design of the F function used is equal to A so that it simplifies the principles used in DES to provide the same security quickly and more efficiently in the software.

Blowfish is a 64-bit block encoder and is suggested as an alternative to DES. Blowfish's algorithm is fast and data can be encrypted on a 32-bit microprocessor.

Among the most important of these advantages[11]:

1) Controls information in large parts
2) It consists of a block size of 64 bits.
3) It has an adaptive key, from 32 bits to no less than 448 bits.
4) Uses exceptionally straightforward operations such as XOR expansion and expansion.
5) Uses an easily accessible layout. This encourages examination and broadens confidence in the account.
6) It's fast because the algorithm rate on a 32-bit chip is 26 clock cycles per byte.
7) It is minimized so that it can be executed with less than 5 KB of memory.

Disadvantage of the Blowfish:

The disadvantage of the Blowfish algorithm is that it must get the person's key out of range specifically and not through the unsecured transmission channel. Each user pair needs a unique feature, so as the number of users increases, key management becomes complex. Blowfish's algorithm is not able to provide authentication to anyone who has the same key. It also has weaknesses in the decoding process over other algorithms in terms of time-consuming and stringency in throughput[11].

RSA Algorithm :

It is a type of asymmetric encryption algorithm that appeared in 1978. The algorithm is a public key cipher algorithm that is widely accepted and implemented by the public and is a public key cryptographic algorithm developed by Ron Rivest, Adi Shamir, and Len Adleman in 1977 (At MIT). It can be used to encrypt/decrypt messages and digital signatures and distribute the secret key of symmetric systems. It is one of the main asymmetric cipher algorithms which use prime numbers to generate the public and private key based on mathematical functions and multiply large numbers together, and use standard exponential[13].

RSA algorithm advantages and disadvantages:

The primary advantage of public-key encryption with the RSA algorithm is increased security and convenience: the private keys do not need to be transferred or disclosed to anyone. In a secret key system, unlike other algorithms where secret keys must be sent (either manually or over a communication channel) and then the same key is used for encryption and decryption[14].

Another key advantage of public-key systems is that they can provide indisputable digital signatures. Authentication via secret key systems requires the sharing of some confidential information and sometimes requires the trust of a third party as well. As a result, a sender can disavow a previously authenticated message by claiming that the shared key has been compromised in one way or another by one of the parties sharing the mufti. For example, the Kerberos secret key authentication system includes a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

central database that keeps copies of the secret keys for all users; An attack on the database would allow for widespread fraud[15].

V. CO M PA R IS O N AND ANA L YSES O F RSA , BLOWFISH AND PROPOSED SYSTEM

The proposed system is the hybridization of RSA and Blowfish. one issue in the Blowfish algorithm is the slow time in encryption and decryption in this new proposed algorithm show in table (1) which takes the RSA techniques in generating key so the time is decreased. the other thing is the use of bigger blocks than used in blowfish which gives more security to the data than RSA and blowfish.

TABLE (1) SHOWS A COMPARISON OF THE BLOWFISH ALGORITHM WITH DIMENSIONS OF GENERAL ENCRYPTION ALGORITHMS.

Characteristic	Blowfish	RSA	Proposed System
Speed	Slow encryption / decryption (1nn for 5kb file)	Fast in decryption and encryption(0. 43nn for 5kb file)	Medium speed in decryption and encryption(0. 62nn for 5kb file)
Memory size	9.38 kb	31.5 kb	6kb
Key size	From 32 bytes to 448 bytes,	From 515 to 4096	From 16 bytes to 224 bytes,
Block Size	64	variable-length block sizes	512

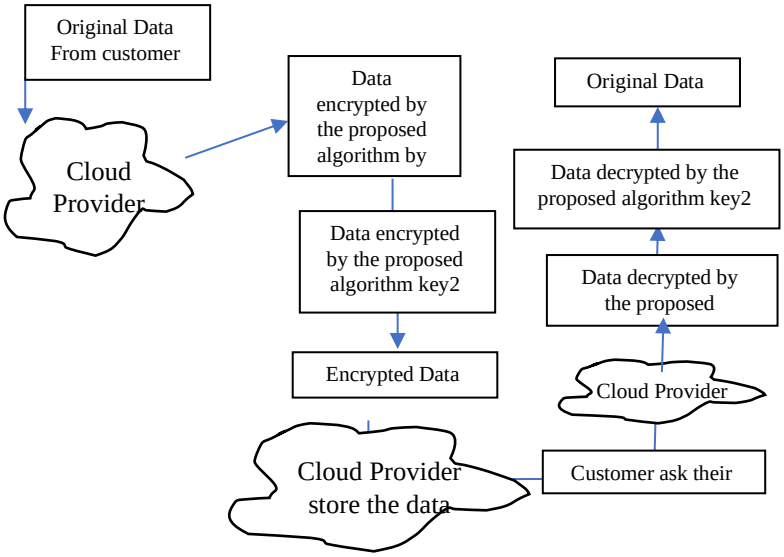
The key size is less which takes less time and less memory and its changes every time when send the file in the cloud which gives the data strong security against many attacks.

The new proposed system generates two keys (to apply the encryption process twice) to use for the encryption and decryption process by creating an instance from the key generate class then converting keys to secret keys which is one of the RSA techniques. This is useful for raw secret keys that can be represented as a byte array and have no key parameters associated with them. when the user enters the data to be encrypted the new proposed system applies twice the encryption process. The first call to this function the first key and the plaintext are passed. The second call to this function the second key and the text that return from the first encryption process are passed.

After finishing the encryption process must reinitialize to cipher instance at decryption mode by calling init( ) Function. Init( ) function takes two parameters: Cipher modes: Specifies details about how the algorithm should decrypt. , Decryption keys.

In the decryption, the function applies two times the decryption process. The first call to this function the second key and the ciphertext are passed. The second call to this function the first key and the text that return from the first decryption process are passed.

FIG 1 THE FLOWCHART OF THE PROPOSED ALGORITHM.



VI. CONCLUSION

The use of the cloud has become necessary for companies and organizations, large and small, and even for individuals. The innovation of encryption mechanisms and increased security is necessary to protect data within the cloud and increase confidence when moving and saving data in it.

In the proposed new algorithm which takes from Blowfish and uses the (RSA) mechanism for generated the two keys, we find the security it is increased and become more difficult to open the file by an unauthorized user and protected from the attacks.

VII. ACKNOWLEDGMENT

The authors would like to express their gratitude for providing administrative and technical support from King Khalid University and Al Neelain University.

REFERENCES

[1] Q. K. Kadhim, R. Yusof, H. S. Mahdi, S. S. A. Al-Shami, and S. R. Selamat, “A review study on cloud computing issues,” in *Journal of Physics: Conference Series*, 2018, vol. 1018, no. 1, p. 012006.

[2] V. Agarwal, A. K. Kaushal, and L. Chouhan, “A Survey on Cloud Computing Security Issues and Cryptographic Techniques,” in *Social Networking and Computational Intelligence*, Singapore, 2020, pp. 119–134. doi: 10.1007/978-981-15-2071-6_10.

[3] H. Abroshan, “A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 6, 2021.

[4] H. Tabrizchi and M. K. Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, 2020.

[5] S. K. Singh and D. K. Singh, “Cloud computing: Security issues and challenges,” *Int. J. Adv. Eng. Technol.*, vol. 10, no. 3, p. 338, 2017.

[6] “(PDF) Data Security Protection in Cloud Computing by using Encryption.” https://www.researchgate.net/publication/332819788_Data_Security_Protection_in_Cloud_Computing_by_using_Encryption (accessed Jun. 30, 2021).

[7] T. F. G. Quilala, A. M. Sison, and R. P. Medina, “Modified blowfish algorithm,” *Indones J Electr Eng Comput Sci*, vol. 11, no. 3, pp. 1027–1034, 2018.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 01, January-2022

[8] P. Chinnasamy and P. Deepalakshmi, "Design of secure storage for health-care cloud using hybrid cryptography," in *2018 second international conference on inventive communication and computational technologies (ICICCT)*, 2018, pp. 1717–1720.

[9] S. B. Nalawade and D. H. Gawali, "Design and implementation of blowfish algorithm using reconfigurable platform," in *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)*, 2017, pp. 479–484.

[10] I. G. Amalarethinam and H. M. Leena, "Enhanced RSA algorithm with varying key sizes for data security in cloud," in *2017 World Congress on Computing and Communication Technologies (WCCCT)*, 2017, pp. 172–175.

[11] R. S. Cordova, R. L. R. Maata, and A. S. Halibas, "Blowfish Algorithm Implementation on Electronic Data in a Communication Network," in *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, 2019, pp. 1–4.

[12] P. J. Sun, "Privacy protection and data security in cloud computing: a survey, challenges, and solutions," *IEEE Access*, vol. 7, pp. 147420–147452, 2019.

[13] G. P. Kanna and V. Vasudevan, "A new approach in multi cloud environment to improve data security," in *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, 2017, pp. 7–12.

[14] M. Buvana, "Optimize Cryptography Algorithm for Efficient Data Security on Cloud Computing," *Turk. J. Comput. Math. Educ. TURCOMAT*, vol. 12, no. 1S, pp. 459–464, 2021.

[15] R. S. Abdeldaym, H. M. Abd Elkader, and R. Hussein, "Modified rsa algorithm using two public key and chinese remainder theorem," *IJ Electron. Inf. Eng.*, vol. 10, no. 1, pp. 51–64, 2019.