engineering proceedings

MDPI

Proceeding Paper

Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing †

Sana Fatima *, Tanazzah Rehman, Muskan Fatima, Shahmeer Khan and Mir Arshan Ali

Department of Software Engineering, NED University of Engineering & Technology, Karachi 75270, Pakistan; rehman4302338@cloud.neduet.edu.pk (T.R.); fatima4300012@cloud.neduet.edu.pk (M.F.); khan4303667@cloud.neduet.edu.pk (S.K.); ali4303674@cloud.neduet.edu.pk (M.A.A.)

* Correspondence: sanafatima@cloud.neduet.edu.pk

† Presented at the 7th International Electrical Engineering Conference, Karachi, Pakistan, 25–26 March 2022.

Abstract: With growing technology, the cloud is becoming a center of sensitive information, making it more open to danger, especially when access to users with malicious plans increases. A huge amount of users use the cloud for various reasons, therefore, data should be safe and protected. In order to provide a safe environment, the aim of this paper is to analyze the well-known symmetric algorithm of the Advanced Encryption Standard (AES) and the Rivest–Shamir–Adleman (RSA) asymmetric algorithm based on time complexity, space, resource and power consumption, and suggest a new hybrid encryption process that is a combination of symmetric and asymmetric cryptographic methods. Based on experimental analysis, this paper proposes a AES cryptographic method as a first choice for data encryption processes for cloud applications and data storage.

Keywords: cloud; security; algorithms; cryptography; AES; RSA

Citation: Fatima, S.; Rehman, T.; Fatima, M.; Khan, S.; Ali, M.A. Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing. *Eng. Proc.* **2022**, *20*, 14. https://doi.org/10.3390/engproc2022020014

Academic Editor: Saad Ahmed Qazi

Published: 29 July 2022

1. Introduction

With the growth of technology, technological infrastructure is also improving on a daily basis. Cloud computing, similarly, has completely transformed the concept of storage. There is a relatively large space available online on the cloud that seems to act as a collection of servers that are organized and arranged properly. The need of the cloud to carry out computational processes is termed as cloud computing, and can be explained as the use of remote servers wirelessly for storing, managing, and processing instead of using local servers on personal computers [1]. The services that are provided by service providers to customers via the internet are mostly covered by cloud services. Software programmers and scientists have devised numerous methods for the security of data in cloud computing, leading to the advent of cryptosystems to safeguard information from falling into the incorrect hands. The methodology part of this paper delves into the intricacies of RSA and AES, two asymmetric and symmetric algorithms, and suggests a better technique for ensuring optimum cloud computing security.

2. Literature Review

2.1. Security of the Cloud

Cloud computing connects the individual use of hardware, software and services that are managed and controlled via another party in a very remote area [1]. The system assures that the users can have access to computer resources and knowledge from any area in the world where the internet is available. Authentication, secrecy, the integrity of information transported, non-repudiation, and storage on distant servers are the security goals of cloud cryptography [2]. This literature study identifies some of the major issues that cloud computing security faces. Many of these flaws are caused by bad systems, human mistakes and, in some cases, cyber bullying. With symmetric and asymmetric

algorithms, cryptography remains the most widely utilized tool for enhancing security measures. Figure 1 shows a brief process of cryptography.

Figure 1. Process of cryptography.

2.2. Asymmetric Algorithms

Asymmetric algorithms involve public and private keys and separate into primary key and secondary key arrangements. The private key is kept secret from other parties and used for decoding while the public key is accessible to everybody and used for encoding [3]. Rivest–Shamir–Adleman (RSA), elliptic-curve cryptography, and asymmetric utilities are a few examples that work with the asymmetric algorithm [4].

2.3. Symmetric Algorithms

Symmetric algorithms, on the other hand, use a single private key to encode and decode data [5]. They can handle large data in terms of computation. Plaintexts are encrypted using symmetric algorithms as a block of fixed digits [1]. The Advance Encryption Standard (AES) cipher text method is a more accurate and elegant cryptographic method.

According to testing results and the text files used, it has been concluded that the AES algorithm outperforms the Data Encryption Standard (DES) and RSA algorithms [6,7].

3. Comparative Analysis

3.1. Advance Encryption Standard (AES)

The AES, known as the Advanced Encryption Standard algorithm, was made and implemented by Joan Daemen and Vincent Rijmen in 2001 [8]. It has a specific block size of 16 bytes (128 bit), variant key sizes of 16 (128), 24 (192) and 32 bytes [7,8] (256 bit), and transformation rounds on a block that are specified using key sizes fixed by numbers. There are 10 rounds for the 16-byte-sized key, 12 rounds for the 24-byte-sized key, and 14 rounds for the 32-byte-sized key. Figure 2 shows a diagrammatic explanation of the AES algorithm [7,8]. Encryption begins and ends by adding a round key and then applying rounds n times, where the final round is different. For decryption, the inverse process is followed.

3.1.1. Key Generation Process of AES Algorithm

A. Byte Substitution (SubBytes)

The substitution of 16 input bytes through a definite table (S-box) generates a matrix of 4×4.

B. Shift Rows

Each row of the 4×4 matrix is moved to the left side. Items are reinserted on the right of the row if they 'fall off'. Movement is carried out as follows:

- First row is not shifted;
- One (byte) position shifts to the left-hand side in the second row;
- Two places shift to the left in the third row;
- Three places shift to the left in the fourth row;
- Finally, a new matrix is generated with a similar 16 bytes but they move with respect to each other.

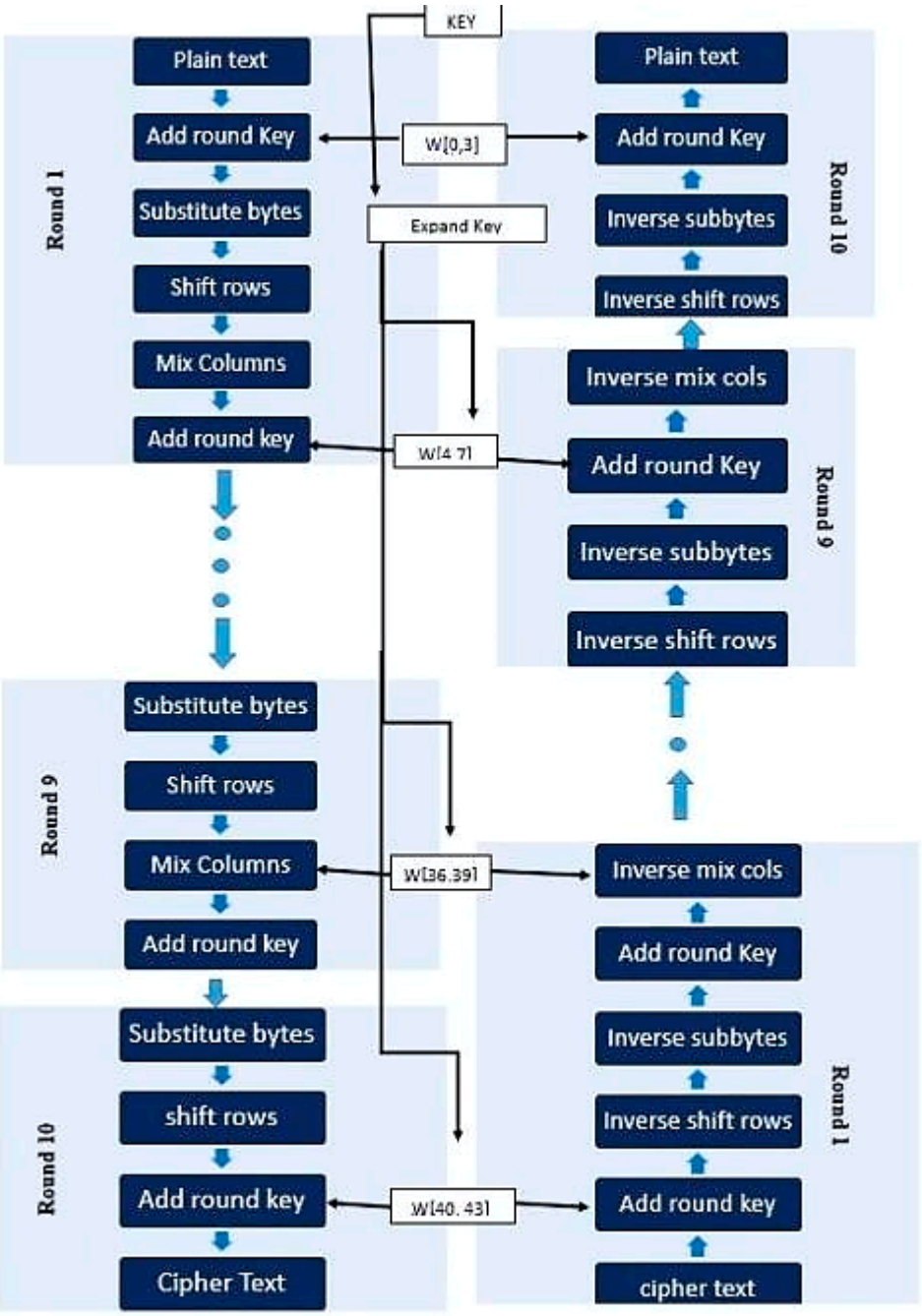

Figure 2. Process of AES algorithm.

C. Mixed Columns

Transformation occurs on every column of four bytes using a specific mathematical function. Four completely new and different bytes are produced, which take the place of the originals. This results in another matrix consisting of 16 new bytes. It is not to be executed in the final round.

D. Addroundkey:

XOR gate is applied to the 16 bytes of the matrix to make 128 bits of the round key. If this process is the last round then cipher text is the final outcome. Otherwise, the resulting 128 bits are then analyzed as 16 bytes and one more similar process begins.

3.1.2. AES Merits and De-Merits

Advantages:

1. AES is faster in comparison with other algorithms;
2. Due to its extra fast speed, it becomes extremely difficult to hack or access the data.

Drawbacks:

1. A high amount of excessive and complex algebra is being used;
2. The deployment and implementation of its software carries some difficulties.

3.2. RSA Algorithm

RSA is the most popular asymmetric or public key cryptography that works on the concept of dual keys [9]. The public key of the sender is utilized for encrypting the text whereas a secret key is utilized for decryption. This is an adaptable and universally used algorithm that depends upon prime factorization and considers large prime numbers for security. It is used for open networks, e-commerce security, virtual private networks, emails, and handling the authenticity of e-documents [10].

3.2.1. Key Generation Process of RSA Algorithm

The algorithm generates two different keys: one is used for encryption and other is used in decryption. The following is the procedure to create the keys:

1. Assign two random large prime numbers, m and n, and calculate p = m * n;
2. Compute the golden ratio of p, φ (p) = (m − 1)(n − 1);
3. Choose integer e such that the greatest common divisor of (φ (p), e) = 1 and 1 < e < ϕ (n);
4. Compute d = e^{-1} mod (ϕ (n));
5. The public key is found from (e, p) and the private key is found from (d, p);

This creates cipher text by applying the public key on plaintext P at the sender side. C = pe mod p.

This finds plaintext by applying the private key on the cipher text at the receiver side. P = Cd mod p.

3.2.2. Rsa Merits and De-Merits

Advantages:

1. It provides a safe, secure and protected transfer of data;
2. It makes it difficult for hackers/crackers to crack the file.

Disadvantage:

1. Time required by RSA is greater and makes the process slow when large data are used.

3.3. Time Complexity Analysis

Asymptotic time complexity of RSA algorithms is concluded to be O({logn}^{3}) for the use of the private key while O({logn}^{2}) is observed for the use of the public key. AES is based on a specific block size, so it is O(m) complexity, where m represents the size of the entered message [4]. Comparing the two time complexities, it can be seen that RSA takes a longer time to encrypt and decrypt data.

3.4. Experimental Analysis

For a better comparison of the RSA and AES algorithms, Windows Azure SDK was required to form the application. By running the application over the cloud, which is a third-party host, values were recorded during the encryption and decryption of messages and the time taken with different key sizes in bits and kilobits for RSA and AES was measure [11]. Figure 3 shows the time taken by the RSA algorithm against the number of bits while Figure 4 shows the time taken by the AES algorithm against kilobits. Comparing the two graphs of RSA and AES, it can be seen that the AES algorithm takes much less time compared to RSA.

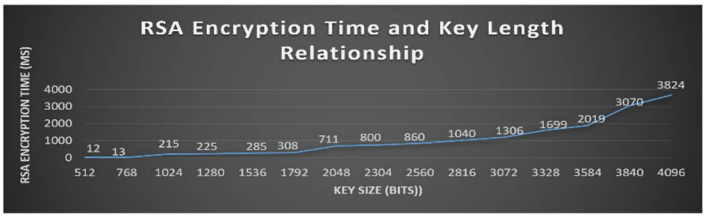

Figure 3. Graph of RSA Algorithm.

Figure 4. Graph of AES Encryption.

Table 1 shows the limitations, parameters and constraints of the AES and RSA algorithms [9,12]. The resources and power consumption of AES are comparatively lower than that of the RSA algorithm while AES is faster than RSA [13].

Table 1. Comparison of AES and RSA algorithms.

FACTORS	AES	RSA
Key length	128, 192, 248 bits	Depends on bits in modulus m = p * q
Rounds	10–128 bits, 12–192 bits, 14–256 bits	1
Block size	128	Minimum 512 bits
Cypher	Symmetric cipher	Asymmetric cipher
Speed	Fast	Slow
Security	Highly secure	Least secure
Power	Low	High
Resource	Consumes more with big data	Very high
Cryptanalysis	Strong against attacks	Brute force attacks hard to accomplish

4. Conclusions

Encryption of the most secure and least time-consuming algorithms is a major need today. The AES algorithm is the method of lesser time complexity and due to its flexible and scalable behavior it is easily implemented, leaving the RSA algorithm behind in terms of memory requirements. The AES algorithm protects data with its high security level and can counterattack against a variety of attacks. Unlike RSA, the AES algorithm requires less storage space while providing a higher performance without any major limitations. However, with fast-paced technology, hybrid models are taking over ordinary security algorithms. Thus, a hybrid model of AES and RSA will increase the security of the cloud overall.

Author Contributions: Conceptualization, T.R.; methodology, S.K. and M.F.; formal analysis, M.A.A.; investigation, S.K.; writing—original draft preparation, T.R.; writing—review and editing, M.F.; supervision, S.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Extracted from the reference papers.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Harfoushi, O.; Obiedat, R. Security in Cloud Computing Using Hash Algorithm: A Neural Cloud Data Security Model. *Mod. Appl. Sci.* **2018**, *12*, 143–150. [CrossRef]
2. Alharabi, M.F.; Aldosari, F.; Alharbi, N.F. Review of Some Cryptographic Algorithms In Cloud Computing. *Int. J. Comput. Sci. Netw. Secur.* **2021**, *21*, 41–50.
3. Emmanuel, A.; Aderemi, O.; Marion, A.; Emmanuel, A. A Note on Time and Space Complexity of RSA and ElGamal Cryptographic Algorithms. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 143–147. [CrossRef]
4. Singhal, S.; Singhal, N. Comparitive Analysis of AES and RSA Algorithms. *Int. J. Sci. Eng. Res.* **2016**, *7*, 149–151.
5. Alabi, O.; Thompson, A.; Alese, B.K.; Gabriel, A.J. Cloud Application Security using Hybrid Encryption. In *Communications on Applied Electronics (CAE)*; Foundation of Computer Science FCS: New York, NY, USA, 2020.
6. Manoj, T.; Manoria, M.; Mishra, B. Analysis and Implementation of AES and RSA for cloud. *Int. J. Appl. Eng. Res.* **2019**, *25*, 3918–3923.
7. Chouhan, T. Enhancement of Cloud Computing Security with Secure Data Storage using AES. *Int. J. Innov. Res. Sci. Technol.* **2016**, *2*, 18–21.
8. Monisha, K.R. Secure cloud computing using AES and RSA algorithms. *Int. J. Adv. Comput. Sci. Cloud Comput.* **2015**, *3*, 77–82.
9. Priya, C.; Kannan, M.; Vaishnavi, S. A comparative analysis of DES, AES and RSA crypt algorithms for network security in cloud computing. *J. Emerg. Technol. Innov. Res.* **2019**, *6*, 574–582.
10. Kanika, T.; Yadav, S.K.; Singh, M. Cloud data security and various security algorithms. *J. Phys. Conf. Ser.* **1998**, *2021*, 012023.
11. Inaam ul haq, M. Analytical comparison of RSA and AES using windows azure for cloud computing environment. *Sci. Int.* **2016**, *28*, 2339–2344.
12. Thakkar, B.; Thankachan, B. A Survey for Comparative Analysis of various Cryptographic Algorithms used to Secure Data on Cloud. *Int. J. Eng. Res. Technol.* **2020**, *9*, 753–756.
13. Semwal, P.; Sharma, M.K. Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing. *Int. J. Emerg. Technol.* **2017**, *8*, 746–750.