WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Securing the Sensitive Data Transfer in Cloud using AES and RSA Algorithms

Lalita Panika[1], Varun Maharana[2], J Kirti Rao[3], Harsh Chandrakar[4], Simran Dey Biswas[5]

[1]*Assistant Professor, Bhilai Institute of Technology, Raipur, Chhattisgarh, India*
[2,3,4,5]*Student, Bhilai Institute of Technology, Raipur, Chhattisgarh, India*
DOI: https://doi.org/10.55248/gengpi.5.0124.0127

A B S T R A C T

In recent years, cloud computing technology has made major advances. Whether it is made use by enterprises for storing and and managing large amounts of data or in a commercial open-for-all (SaaS) modal that the common people use to store data in the cloud using minimal cost services like Google Drive, Dropbox, etc. Here, we present a method of protection of such sensitive data that is quite frequently sent and received between the client and the server. The target data can be of any kind but here we have made emphasis on the sensitive data only, for example, passwords, text conversations, etc. The data is encrypted or decrypted before sending it through the insecure channel i.e. internet. AES and RSA algorithms are both applied for encryption and decryption at the client and well as the server side. The k eys thus generated are stored in respective files in a secure fashion at both ends. We compared the performance of many symmetric and asymmetric algorithms and chose AES and RSA respectively due to their best outcomes in all parameters. The cloud service provider that is made use of is Amazon Web Services (AWS). This kind of double encryption when applied to any kind of data, even though generic, makes it more confidential and increases integrity of the data.

Keywords: AES, RSA, Security, Double Encryption, Cloud Storage, AWS.

1. Introduction

The study and application of secure communication methods known as cryptography enable the conversion of data into an unintelligible format so that only those with the proper authorization can decipher it. Preserving data's secrecy, integrity, and authenticity while it's being stored or transmitted is its fundamental objective.

A vast array of computing resources, including servers, storage, databases, networking, software, and more, may be accessed and used by users via the internet thanks to a technology called cloud computing. Users can access these resources on-demand from a distance rather than owning and maintaining real hardware or software.

1.1 Types of Cryptography

There are mainly three different types of cryptography, mentioned as follows:

1. **Symmetric Key Cryptographic Algorithms:** These algorithms utilize a singular, unique key for both encryption and decryption processes, providing data with authentication and authorization. Prominent instances include the Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES). These symmetric-key algorithms are widely deployed in cloud computing environments to fortify cryptographic operations.
2. **Asymmetric Key Cryptographic Algorithms:** Employing distinct pairs of keys for encryption and decryption, this algorithmic paradigm safeguards data within cloud-based settings. Key algorithms utilized in cloud computing encompass the Digital Signature Algorithm (DSA), RSA, and Diffie-Hellman Algorithm.
3. **Symmetric Key Cryptographic Algorithms:** These algorithms utilize a singular, unique key for both encryption and decryption processes, providing data with authentication and authorization. Prominent instances include the Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES). These symmetric-key algorithms are widely deployed in cloud computing environments to fortify cryptographic operations.

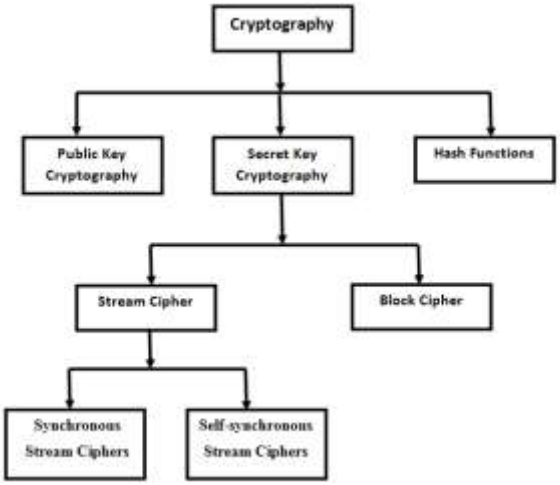

Fig. 1 – Classifications in cryptography.

1.2 Overview of AES algorithms

Some features of the AES algorithm are as follows:

- AES algorithm is the method of lesser time complexity and due to its flexible and scalable behavior it is easily implemented.
- The AES algorithm protects data with its high security level and can counterattack against a variety of attacks.
- AES algorithm requires less storage space while providing a higher performance without any major limitations.

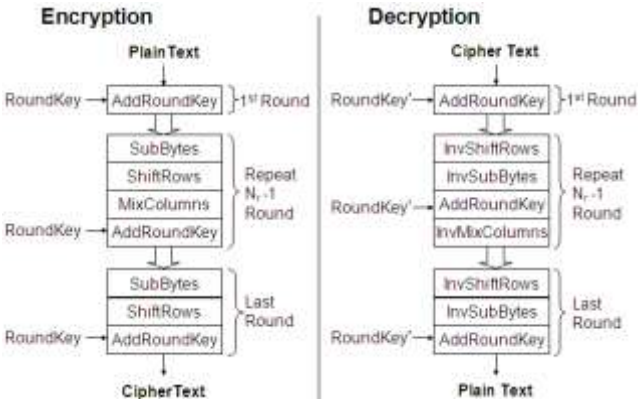

Fig. 1 – AES Encryption-Decryption Process

Overview of the RSA Algorithm

Some features of the RSA algorithm are as follows:

- It uses both public key and private keys for encryption and decryption.
- The algorithm uses logarithmic functions to keep the working complex enough to withstand brute force and streamlined enough to be fast post-deployment.
- RSA can also encrypt and decrypt general information to securely exchange data along with handling digital signature verification.

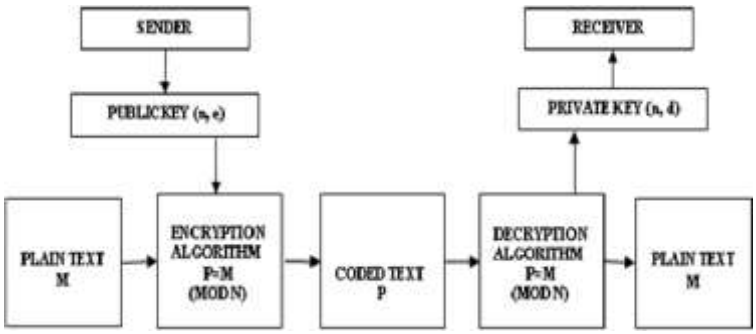

Fig. 2 – RSA Encryption-Decryption Process

2. Literature Review

Data security was revolutionized by carefully combining and utilizing the strengths of both the AES and RSA encryption algorithms. The thorough analysis raised the bar for data security and provided a detailed illustration of file encryption in their in-house program. The results demonstrated the dual encryption methodology's strength and effectiveness, opening the door for improved data security in cloud environments and highlighting its potential in today's cybersecurity environments. [1]

A new method for incorporating hybrid cryptography into data masking was presented to make the smooth migration of big data sets between cloud environments possible. This novel hybrid algorithm resulted from combining several different cryptography techniques and proved to be a reliable solution. The technique brought in a new era of data transfer security and flexibility by giving customers the option to both mask and encrypt particular data segments. Because of its many facets, users could take a customized strategy that strengthened the security and integrity of data while it was in transit by allowing them to choose protect critical information. In addition to addressing the difficulties that come with transmitting large amounts of data, this innovative algorithmic fusion gave consumers a powerful tool to guarantee complete data safety and privacy within. [2]

The idea presents a novel method of enhancing cloud computing data security by using password-preserving mechanisms. The core of this invention is an algorithm that has been painstakingly designed to maintain a careful balance between optimal performance and strong security safeguards. This approach puts a strong emphasis on password-preserving techniques so as to protect data integrity without sacrificing system performance. This striking combination of increased security and optimized efficiency is a big step toward solving the complex problems with cloud-based data protection. The suggested approach seeks to protect sensitive data while simultaneously guaranteeing quick access and processing, which would promote a positive synergy between data security and computational efficiency in cloud environments. A well-rounded solution like this is essential for protecting cloud-based infrastructures from any security flaws. [3]

Malicious software programs have been discovered to employ malware obfuscation techniques in real-world circumstances. Still, more testing and improvement into several categories of methods is necessary. These cases highlight how important it is to learn more about the complex field of virus obfuscation. The goal of validation and improvement work is to classify and distinguish between different kinds of malware obfuscation tactics. This improved classification attempts to offer a more thorough knowledge of the various tactics hostile entities employ to hide their code and avoid detection. Thorough validation and classification efforts play a crucial role in improving cybersecurity defenses by enabling focused countermeasures against the dynamic obfuscation strategies used by contemporary malware strains. [4]

We urgently need to find the fastest and safest encryption techniques available. The AES algorithm outperforms the RSA algorithm in terms of memory requirements and has a lower time complexity. It is also easier to implement because of its scalable and flexible behavior. With its high security level, the AES algorithm guards data and is capable of counterattacking against many types of attacks. The AES algorithm performs better than RSA and has no significant drawbacks, requiring less storage space. But as technology advances quickly, hybrid models are replacing traditional security methods. [5]

Table 1 – Comparison of AES and RSA algorithm

Factors	AES	RSA
Key length	128, 192, 248 bits	Depends on the size of modulus m = p * q
Rounds	1-128 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
Power	Consumes more with big data	Very high
Cryptanalysis	Strong against attacks	Brute force attacks hard to accomplish

Simply tested the RSA encryption technique using varying browser options, implemented it with JavaScript, and measured the performance. The Opera Web browser has the lowest response time across all character lengths, according to research findings. The Web browsers Maxthon and IE6 require the longest possible response times to process RSA algorithms, regardless of the letter length. Firefox performs worse than Chrome and Safari. [6] We can arrange the browsers with the fastest reaction times for the maximum character length (1024 characters) as follows:

Table 2 – Browser Response Time

S. No	Browsers Name	Response Time in ms
1	Opera	109
2	Chrome	142
3	Safari	181
4	Firefox	1859
5	IE6	2282
6	Maxthon	2297

3. Methodology

Our aim is to achieve the double encryption of the data that is being sent and received between the frontend and the backend cloud, or the client side and the server side. As shown in the diagram, first the data that comes from the client side which is to be sent through the internet to the cloud is first encrypted and converted into cipher text or encrypted format and then is being sent through the insecure internet to the cloud where it is first decrypted in order to convert it to its original format, after which the cloud service may encrypt the data on its own in order to store it in their respective database services.

Similarly, when the data has to be sent from the backend or the cloud to the client side, it is first encrypted before it is sent to the insecure internet channel. When the data reaches the client side in an encrypted format it is first decrypted and then it is put into use.

The both encryption and decryption process combines the usage of both the algorithms i.e. AES (Advanced Encryption Standard) algorithm and RSA (Rivest-Shamir-Adleman) algorithm. Hence, a hybrid approach of combining both the algorithms for the encryption and decryption of the algorithms has been put into practice.

First, while encrypting the plain text, it is run through the AES Encryption algorithm to implement the symmetric key cryptography. Then, the encrypted string is again rerun through the RSA Encryption algorithm to encrypt it even more using asymmetric key cryptography.

Similarly, while decryption, the encrypted cipher text is run through the RSA Decryption algorithm and then again it is run through the AES Decryption algorithm in order to fully convert it into the original plain text.

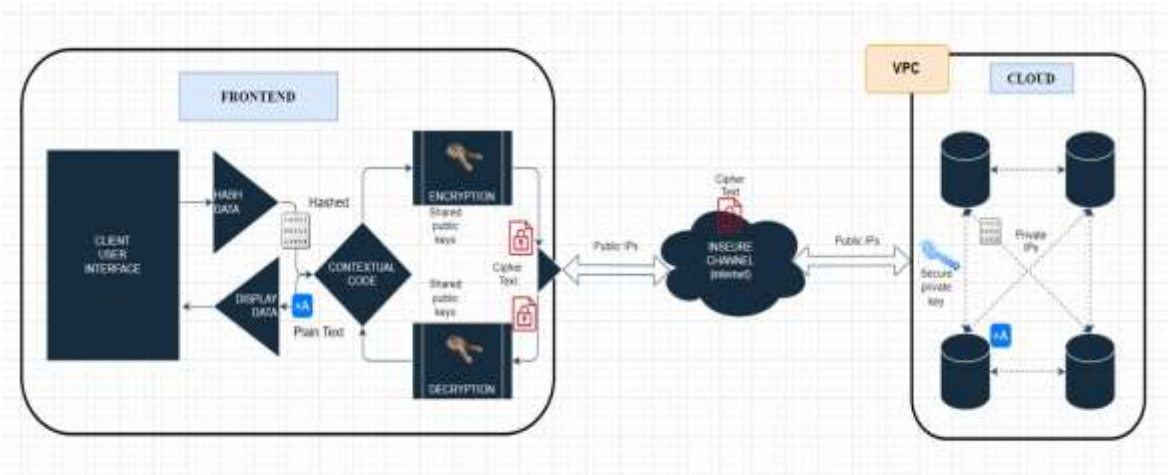

Fig. 3 – Conceptualized flow chart

3.1 Hybrid Implementation Process

The hybrid implementation process of the concept is depicted in the following diagram:

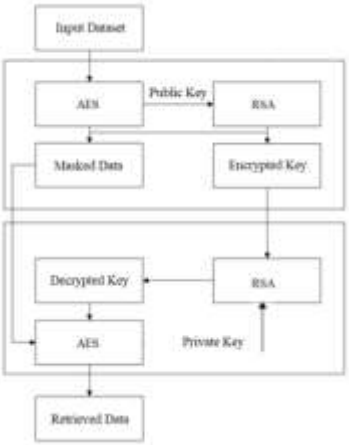

Fig. 4 – Hybrid implementation flow chart

4. Conclusions

In conclusion we can say that after implementing the hybrid encryption decryption algorithm i.e. combining AES and RSA algorithms both, we generate a comparatively much stronger encryption on the data that we need to transfer over the internet. Similarly, the encrypted data can be decrypted and then used in the client as and when needed. Using this approach, we improvise the standalone qualities of both the algorithms and hence improving efficiency overall.

References

[1] Jaspin, K., Selvan, S., Sahana, S., & Thanmai, G. (2021, March). Efficient and secure file transfer in cloud through double encryption using AES and RSA Algorithm. In 2021 international conference on emerging smart computing and informatics (ESCI) (pp. 791-796). IEEE. Basapur, S. B., & Shylaja, B. S. (2021). A Hybrid Cryptographic Model Using AES and RSA for Sensitive Data Privacy Preserving. Technology.
Bhargav, A. J. S., & Manhar, A. (2020). A review on cryptography in cloud computing. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 6(6), 225-230.

[2] Asghar, H. J., Zhao, B. Z. H., Ikram, M., Nguyen, G., Kaafar, D., Lamont, S., & Coscia, D. (2023). Use of cryptography in malware obfuscation. Journal of Computer Virology and Hacking Techniques, 1-18.

[3] Fatima, S., Rehman, T., Fatima, M., Khan, S., & Ali, M. A. (2022). Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing. Engineering Proceedings, 20(1), 14.

[4] Patidar, P. C., & Jain, N. Performance Measurements of RSA Algorithm on Web Browsers.