Enhancing RSA for Secure Key Exchange in Cloud

[1] Omprakash Maru, [2] Dr. Ramesh Vishwakarma

[1] Research Scholar, [2] Guide, Rabindranath Tagore University, Bhopal

ABSTRACT: The security of cloud computing is one of the primary challenges that is holding down the adoption of cloud computing, and the industry continues to struggle with issues pertaining to data protection and privacy. It is of the utmost importance that the introduction of a more advanced model does not cause any disruption to the essential capabilities and features that are now included into the existing model. Any new model that aims to improve upon the characteristics of an existing model must make certain that other significant elements of the old model are not put in jeopardy or compromised in any way via the implementation of the new model.RSA is a highly prevalent method for asymmetric key encryption. The suggested study aims to enhance the RSA algorithm in order to improve data security in cloud computing. The encryption and decryption operations rely on prime numbers. The method being suggested demonstrates superior performance compared to Conventional RSA encryption method.

Keyword: Cloud, RSA, secure key exchange

INTRODUCTION

Cloud computing is the most recent and rapidly developing technology. It enables shared memory management across the network and provides a limitless capacity for storage. The cloud server provides a new service paradigm by enabling data to be organized, controlled, and backed up remotely. This is made possible with the cloud server. Additionally, customers of cloud services have the ability to utilise the internet to access certain services whenever they want and from wherever they are. As one of the numerous benefits that cloud computing technology offers, the availability of services at a cheap cost and around the clock is of particular significance. Cloud computing originates from the basic architecture of a sophisticated information system and serves as its foundation. The user, the client, and the cloud service provider (also known as a CSP) are the three functional aspects that are at the heart of the concept with regard to cloud computing. Santos and Bartolini's 2017 research A cloud service provider (CSP) is an organization that is responsible for the management of a cloud storage server (CSS) and has a significant amount of computing power and storage capacity in order to protect an organization's data.

Utilizing Public key cryptography as an idea allows for the elimination of the constraint that classical cryptography had, which is that it can only be used for communication between two parties. Numerous algorithms make use of public keys in their operations. Out of all of them, the RSA algorithm is the one that is used the most frequently. Both the Merkle Hellman-Knapsack algorithm and the Mc Eliece algorithm are remarkable examples of public key cryptosystems. Both of these algorithms are notable. A discussion of the concept of RSA as This section of the article has provided a public key algorithm.

The Cryptography Algorithm, or RSA

One of the asymmetric key algorithms most frequently employed to guarantee the secrecy of encrypted communications is RSA. Three scientists, Adi Shamir, Leonard Adleman, and Ron Rivest made the effort to publish this concept. Through the use of the first letter of each of these three individuals' surnames, the name of the RSA Algorithm was conceived. Additionally, Rivest and Shamir were both working in the field of computer science at the same time. Adleman was a mathematician. 1977 was the year when they came up with the RSA Algorithm. When it comes to the encryption and decryption of real-time communication channels, this method is still considered to be among the most secure currently available. The process of decryption really takes more time than the encryption technique, despite the fact that the encryption operation could be finished more rapidly. It is typically the cryptosystem that offers the highest level of security; but, due to Due to the fact that the size of the key determines the system's security, employing it requires more computation time. It is recommended by RSA that a bigger key size be used to guarantee data security going forward (S. Shin, 2021). Following the completion of the RSA literature study, which will be discussed in the subsequent chapters, we will next provide an improved version of RSA.

For the purpose of computing RSA, We utilize integers modulo n = p * q. In this case, two big prime numbers, p and q, are kept under wraps. In order to encrypt a message, it is necessary to multiply it by a modest public exponent, which is denoted by the letter e. The multiplicative reversal (d = e-1 (mod (p-1)*(q-1))) must first be calculated by the recipient in order to decode the encrypted text. This is done in order to decode the cypher text. One possible way to express this is as follows:

E * d = mod (p-1)*(q-1)

(Its existence depends on e being chosen appropriately.)

C * d = m * e * d = m (mod n) is the result of this.

Only the letter d is included in the private key, and furthermore only the letters n and e are included in it. It is possible that the letters p and q are not included. An obstacle for the attacker is that figuring out e's reverse d shouldn't be any simpler than factorizing n. It is recommended that the key size, which is also frequently referred to as the modulus size, be more than 1024 bits, which is equivalent to a magnitude of 10300. This will ensure that a fair margin of security is maintained. For example, keys with a size of 2048 bits should be able to ensure security for decades.

Step-by-step instructions

Create two massive, nearly identical, randomly generated primes, p and q.

- Find n = p * q and f = (p - 1) * (q - 1).
- Select an integer e at random so that for each e < e< f, gcd(e; f) = 1.
- Using the extended Euclidean approach, find the unique integer d, 1 < d< f, such that e * d = 1 (mod f).

The letter d is that which is used to symbolize the private key, while the letters n and e are used to represent the public keys. Throughout the process of generating an RSA key, the letters n represent the modulus, while the symbols e and d represent the encryption and decryption exponents, respectively. In addition, the letters n stand for the modulus.

The encryption and decryption procedure

Therefore, in order for B to encrypt a message for A, which A will then decode, B must do the following actions:

- Obtain A's actual public key (n; e).
- Enter an integer m to represent the message in the range of 0 to n - 1.
- Deduct c (mod n) from m * e.
- Send A the encrypted text c.

A must do the below steps in order to obtain plain text m from c:

- The private key d may be used to obtain m = c * d (mod n).

Mathematical evidence for the decryption process

When e * d = 1 (mod f), it is suggested that there exists an integer k such that e * d = 1 + k * f.

Given that gcd(m; p) = 1, Fermat's theorem may be used to obtain m * (p - 1) = 1 (mod p).

Raising both sides of this congruence to the power of k * (q - 1) and then multiplying both sides by m using the previously mentioned procedure will get the desired result.

k * (p-1) * (q-1) is equal to m (mod p).

On the other hand, this last congruence is again valid if gcd(m; p) = p. This is thus because, modulo p, both sides equal 0. Thus, in every case, m * e * d = m (mod p).

Using the same reasoning, we get m * e * d = m (mod q).

Lastly, since p and q are different primes, it can be shown that m * e * d = m (mod n).

M (mod n) = c * d = (m * e) * d as a result

The table below displays the RSA algorithm.

Table 1: A representation of the RSA algorithm

The receiver generates the key						Sender wishes to send	Sender does encryption using public keys of receiver	Receiver does the decryption using secret key of the receiver
p(secret)	q(secret)	n(public) such that n=p*q	(secret) in such a manner that φ = (p-1)(q-1)	such that for e(public), GCD(e, φ)=1.)	such that for d(secret), e*d mod n=1.	Plain text or original message	Cipher text as prepared and sent by the sender such that Y=Xemodn	Original text as computes by the receiver such that X=Ydmodn
5	7	35	24	5	5	3	33	3
5	11	55	40	7	23	4	49	4

7	17	119	96	7	55	3	45	3
7	11	77	60	7	43	5	47	5
7	17	119	96	5	77	2	32	2

REVIEW OF THE LITERATURE

In the year 2019, An paper titled "Modified RSA algorithm using two public keys and Chinese remainder theorem" was published in the International Journal of Electronics and Information Engineering. Abdeldaym, Rasha Samir, Hatem Mohamed Abd Elkader, and Reda Hussein wrote this article. This model needs four prime numbers in order to work with the RSA method. Sending the receiver two public keys is preferable to sending them only one public key at a time. Unfortunately, there is a speed problem. To address this, The RSA decryption process was sped up by applying the Chinese remainder theorem. Unlike the RSA algorithm cryptographic system, which generates a single public key for encryption, the proposed technique generates two public keys and sends them separately. Therefore, to shorten the time needed for decryption, the Chinese remainder theorem is applied. By utilizing two different public key pairs, this method provides an additional enhancement to the security of the RSA algorithm. The work that will be done in the future will be centered on working on the attacks that are feasible on RSA, with the goal of providing a more secure RSA cryptosystem and improving its performance.

Soma Ghosh (2015) The security of a network is often built on authentication, which has the potential to begin with a straightforward username and password. One-factor authentication, which consisted of a single login and password, was used in this instance; nevertheless, in general, one-factor authentication did not fulfill the aim of providing complete security for the transfer of sensitive data.For the purpose of transmitting the data, which is often more sensitive, we were required to encrypt the data using an algorithm (such as aES or DES) and then send it over the network. After that, one day, as a result of using high-speed computers, these algorithms were susceptible to being assaulted. Within the scope of this study, we put up the concept of utilizing a mixture of AES, DES, and RSA and inserting it into the Feistal framework. The algorithm would have been an effective and dependable encryption standard if it had been a combination of three powerful encryption approaches. Specifically, the goal of this project would be to construct and design a hybrid AES-DES-RSA method for the purpose of ensuring data security.

Shashikant Kuswaha, Praful B.Choudhary (2015) It was more vital than ever before to ensure the safety of data in a society that is becoming more and more dependent on electronic information. Numerous aspects of our personal and professional lives were dependent on computers, mobile devices, and the Internet at that time; thus, there was a substantial amount of information that needed to be safeguarded. It is essential to ensure the safety of all types of data before sending them over the network because of the vast volume of data that is communicated over the network. Security controls are the means by which this is accomplished. Data security issues are growing more and more important, and it is a difficult task to safeguard the information that will be transferred over the network. The many types of cryptographic algorithms that were given at the time offered a high level of security to the information that was stored on networks; nevertheless, they also had a few limitations. The purpose of this study was to present a novel hybrid cryptographic algorithm with the intention of enhancing the strength of existing methods. A mixture of two different cryptographic methods, RSA and aES, was employed in the construction of the particular algorithm. The newly developed hybrid cryptographic approach was developed with the intention of improving both security and integrity.

EvequeMutabaruka (2015) The enhanced Encryption Standard and Rivest Shamir Adleman, which are symmetric and asymmetric encryption procedures, were utilized in this hybrid encryption approach that was proposed by the researchers. This was successful because it included analyzing how to encrypt data using symmetric keys, and then using asymmetric encryption to distribute the keys. Examine the measures that may be taken to protect both the data and the key itself by utilizing hybrid encryption, with the possibility of making it substantially more secure. The RSA asymmetric algorithm, the AES symmetric algorithm, the hashing function, and the digital signature are the practical methods that we utilize to improve the data security. This improvement is based on the fact that cryptography is able to fulfill the security criteria. Additionally, we compare and contrast the two algorithms, as well as the security features, and we do an analysis on the functionalities. Once we have finished talking about it, we will create a hybrid encryption method.

Using data categorization as its foundation, A cloud computing paradigm was established by Lo'ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, and Fahed Al-Dosari (2015). The goal of this model is to decrease the amount of overhead and processing time during cloud computing. There were three layers of encryption for the data: the basic level, which was used to encrypt the general kind of data; the confidential level, which was used for material with a medium degree of confidentiality; and the very confidential level, which was used to handle the most essential data.

The employment of hybrid security approaches, such as the Fiestel, XOR operations methods, Encryption/Decryption utilizing Blowfish algorithm, RSA algorithm, and RSA Digital Signature algorithm, was proposed by Jasleen Kaur and Dr. Sushil Garg (2015) in order to increase the safety of data that is kept on cloud computing.

The symmetric Data Encryption Standard (DES) and the asymmetric cryptographic technique (RSA) were both discussed in the article that was written by Professor R.R. Tuteja and Shakeeba S. Khan (2015). In addition, they provided an explanation of how to combine two distinct techniques, including DES and RSA, to eliminate the challenges related to cloud storage security.

RSA Algorithm

The Hybrid Encryption method encrypts a key using the RSA algorithm. The recipient receives the key encrypted when it is sent to them. The RSA system is a block cipher where the cipher texts and the plain text are integers for some 'n' between 0 and n-1. This system was developed by the RSA.

RSA Algorithm Explanation and Illustration

Step 1: User "A" selected two big prime numbers. Pa and qA

Step 2: User 'A' chooses a random number, Ca, that is unlike (pA-l)(qA-l) from any aspect.

Step 3: User "A" calculates \(nA) = nA+1-PA-qA and nA= PAqA.

Step 4: The muhiplicative inverse of eA modulo φ (nA) is computed by user "A": dA = modulo φ(nA) e-1A

Step 5: The public key pair KE,A = (nA, eA) and the private key pair KD,A = (nA, dA) are generated by user "A".

f(P) ≡ Pea mod nA is the encryption transformation, whereas f -1 ≡ CdA = mod nA is the decryption transformation.

Each block that makes up the encrypted plain text has a binary value that is smaller than a certain number "n." The value of nA must be known both the sender and the recipient. The sender knows the value of eA; only the receiver knows the value of dA. Thus, the public key encryption technique is made up of the public key KE,A = (nA, eA), and the private key pair KD,A = (nA, dA).

Using a random number generator, user 'A' selected the random number Ca. One example of this would be a computer program that creates a series of numbers in a way that is hard for anybody to copy or anticipate. Such a sequence is likely to include all the statistical characteristics that are connected to a really random sequence.

The real power of RSA's security method lies in the difficulty of factoring huge numbers The most well-known technique for factoring is quite sluggish It would take around thirty thousand MIPS (the amount of operations that a computer that is working at years would perform in a year) to factor a 512-bit integer using the most well-known approaches.

Exponentiating large quantities

huge numbers are needed for operations like encryption, decryption, signing, and signature verification. These may be generated by taking a huge number, raising it to a large power, and then calculating the remainder mod a large integer. Even in the most straightforward manner, these actions would be costly due to the large number of integers needed for RSA to work properly. Multiplying 123 by itself 54 times yields 12354 mod 678, which is the easiest to compute. This will provide a large product (about 100 digits), which you may divide to determine the residual by dividing by 678. RSA requires the numbers to be on the order of 150 digits in order for them to be safe, yet a machine could easily accomplish this task. It would be impossible to use this strategy to raise a number with 150 digits to 150 digits of power since it would exhaust the capacity of the computer. The following are some pointers that will help you complete the computation in EESP more quickly. A large number of smaller integers are used to split the power value:

123^2 = 123.123 = 15129 - 213 mod 678

$123^3 = 123^{2} \cdot l23 = 26199 = 435 \bmod 678$
Mod 678, 1236 = (1233)2 = 4352 = 189225 = 63
1236 x 2 = 632 x 3969 x 579 mod 678 = 12312
$123^{13} = 123^{12} . l23 = 579.123 = 71217=27 \bmod 678$
12313)2 T = 272 = 729 = 51 mod 678 = 12326
31.123 = 6273 = 171 mod 678 12327 = 12326. 123
Mod 678: 12354 = (12327)2 = 1712 = 29241 = 87

Applying this strategy results in a reduction of the computation to a total of eight divisions and eight multiplications. Within the realm of public key cryptography, it is not necessary to alter either the private or the public keys on a consistent basis. It is possible to find prime numbers in a time-efficient manner by applying a variety of theorems, including the Chinese Remainder Theorem, Euler's Theorem, Fermat's Theorem, and the Theorem.

The prime numbers "p" and "q" are longer, which makes it more difficult to calculate the values of "d" and "e." To get the value of "d," use the formula ed=l mod (p(n)), and to discover the value of "e," use any number that is relatively prime to (p-1) (q-1). The method developed by Euclid is utilized in order to determine "e" and "d."

There are two different techniques to make sure that 'e' and (p-1) (q-1) occupy about prime positions.

- Choose 'p' and 'q' first, then choose 'e' at random. Determine whether 'e' is more prime than (p-1) (q-1). If not, substitute another "e."
- Don't choose "p" and "q" at first. Alternatively, start with "e" and carefully evaluate "p" and "q" to make sure that (p-1) and (q-1) are relatively prime to "e."

The Hybrid Encryption Technique: Cryptanalysis

1. The public key cryptography system provides the authentication method.
2. A high degree of security as a result of extensive testing of the AES-Rijndael algorithm.
3. The RSA technique uses minimal computer resources while providing a high level of security.
4. We do not require any resynchronization.

CONCLUSION

The most recent advancements in scientific and technical applications communication are playing a significant role in businesses that conduct their transactions online. Shared via the network are all of the transactions that take place all over the world. The wireless technology is now capable of reaching practically every area on the surface of the world, giving it the ability to reach virtually every site. As a result of the volatile nature of the modern-day business climate, Businesses now have no choice but to reveal confidential information to their partners, suppliers, and consumers. Large organizations can only do this by giving their networks Internet connectivity, even though they have already invested a larger sum of money in the process of network construction.

REFERENCE

[1]. E. Ochoa-Jimenez, L. Rivera-Zamarripa, N. Cruz-Cortes and F. RodriguezHenriquez, “Implementation of RSA signatures on GPU and CPU architectures," IEEE Access, 2020, vol. 8, pp. 9928-9941.

[2]. T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann and L. Uhsadel, “A survey of lightweight-cryptography implementations," IEEE Design & Test of Computers, 2007, vol. 24, no. 6, pp. 522-533.

[3]. M. Mumtaz, J. Akram and L. Ping, “An RSA based authentication system for smart IoT environment," in Proceedings of IEEE 21st International Conference of High Performance and Computing Communication, 2019, pp. 758-765.

[4]. B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey and S. Linkman, “Systematic literature reviews in software engineering: A systematic literature review," Information Software Technology Journal, 2009, vol. 51, pp. 7-15.

[5]. M. S. A. Mohamad, R. Din, and J. I. Ahmad, “Research trends review on RSA scheme of asymmetric cryptography techniques," Bulletin of Electrical Engineering and Informatics, 2021, vol. 10, pp. 487-492.

[6]. M. Rashid, M. Imran, A. R. Jafri, and T. F. Al-Somani, “Flexible architectures for cryptographic algorithms: A systematic literature review," Journal of Circuits, Systems and Computers, 2019, vol. 28, pp. 200 - 205.

[7]. S. S. Al-Kaabi and S. B. Belhaouari, “Methods toward enhancing RSA algorithm: A survey," International Journal of Network Security & Applications, 2019, vol. 11, pp. 53-70.

[8]. P. P. Santoso, E. Rilvani, and A. B. Trisnawan, “Systematic literature review: Comparison study of symmetric key and asymmetric key algorithm," IOP Conference Series: Materials

Science and Engineering, 2018, vol. 420, pp. 757-763.

[9]. C. Vyas and J. Dangra, “A review of modern cryptography techniques with special emphasis on RSA," International Journal of Engineering Technology Research & Management, 2021, vol. 4, pp. 2348-2355.

[10]. S. Saxena and B. Kapoor, “State of the art parallel approaches for RSA public key based cryptosystem," International Journal of Computer Science and Application, 2015, vol. 5, pp. 81-88.

[11]. P. O. Asagba and E. O. Nwachukwu, “A review of RSA cryptosystems and cryptographic protocols," West African Journal of Industrial and Academic Research, 2014, vol. 10, pp. 30-36.

[12]. J. J. Quisquater and C. Couvreur, “Fast decipherment algorithm for RSA public-key cryptosystem," Electronics Letters Wiley, 2021, vol. 6, pp. 905- 911.

[13]. T. Takagi, “Fast RSA-type cryptosystem modulo," IEEE Access, 2021, vol. 6, pp. 318-326.

[14]. T. Collins, D. Hopkins, S. Langford, and M. Sabin, “Public key cryptographic apparatus and method," IEEE Access, 2015, vol. 8, pp.123-139.

[15]. D. Pointcheval, “New public key cryptosystems based on the dependent- RSA problems," IEEE Access, 2019, vol. 18, pp. 239-254.

[16]. A.K. Lenstra and B. M. M. Weger, “Twin RSA," Advances in Cryptology, 2021, vol. 15, pp. 222-228.