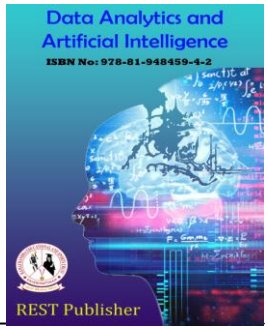
Data Analytics and Artificial Intelligence

Vol: 3(2), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/3/2/18



Data security in cloud computing using RSA Algorithm

***L. Hanupriya, S.I. Anto Ramya**

St. Joseph's College of Arts and Science for Women, Hosur

*Corresponding Author Email: rosehanu06@gmail.com

Abstract. *The capacity of cloud computing, an emerging paradigm, to lower computer costs, has made it the hottest research area of the day. The most fascinating and alluring aspect of modern technology is what it is giving. The services to its customers over the internet on demand. Security has emerged as the primary challenge impeding the implementation of cloud settings because cloud computing stores data and distributes resources in an open environment. Although cloud computing is effective and promising, there are several issues with data security because the cloud user has no physical access to the data. We suggested a technique using the RSA algorithm to assure the security of the data.*

Keywords*— Cloud Computing, Data Security, RSA algorithm, Encryption, Decryption.*

1. INTRODUCTION

Cloud computing is a major driving factor in many small, medium, and large-sized businesses, and as more cloud users seek cloud computing services, the primary worry is the security of their data on the cloud. Data security is always crucial, but because of the critical role of cloud computing and the huge volumes of complex data it transports, the requirement is considerably greater. As a result, worries about data privacy and security are proving to be a barrier to the widespread use of cloud computing services. Before hosting their data or applications in the cloud, any cloud service(s) seeker, whether a person or an organization, should ask the correct questions to the cloud provider. Prospective cloud providers should inform you if they are financially secure. Do they have effective security policies and procedures? Is the infrastructure intended to house your data shared with many other users, or will virtualization separate it? As more businesses shift their data to the cloud, the data undergoes significant changes, and there are several hurdles to solve. Cloud data security requires more than just following adequate data security policies and countermeasures to be effective. The majority of computer based security mechanisms rely on user authorization and authentication.

2. CLOUD DATA SECURITY ISSUES

Privacy and flexibility: There should be some assurance that access to the client's hosted data in the cloud will only be permitted for those with the proper authorization. Another issue that might potentially endanger cloud data is cloud staff having improper access to sensitive client information. To guarantee the security of their data, cloud customers should be given assurances, and appropriate practices, privacy rules, and processes should be in place. The cloud user should have confidence that the data being stored there is private.

Data integrity: Cloud service providers should put in place systems to assure data integrity and be able to trace what happened to a specific dataset and when. This is done by offering data security. The cloud service provider must inform the customer of the type of data being stored in the cloud, its source, and any integrity safeguards that have been implemented. It can be important to keep precise records of the data that was uploaded to a public cloud, when it happened, what virtual memory (VMs) and storage it was stored on, and where it was processed to meet compliance requirements. When such requirements for data integrity exist, it is necessary to preserve the origin and custody of data or information to guard against tampering and to avoid the exposure of data outside of the designated areas (either across other servers or different networks). Integrity is also extended to hold how data is

- stored
- processed and
- Retrieved.

Location and relocation of data: Cloud computing allows for a lot of data mobility. Customers frequently are unaware of where their data is located. However, if an organization has sensitive data stored on a Cloud storage device, it might want to know where it is. Additionally, they might want to identify a preferred site (e.g. data to be kept in India). It

is thus necessary for the Cloud provider and the customer to enter into a written contract specifying the location or known server where the data will remain. Additionally, cloud service providers should assume responsibility for the security of systems (including data) and offer strong authentication to protect client data. The transfer of data between locations is another problem. Data is first kept at a location determined by the cloud service provider as being suitable. But it is frequently relocated from one location to another. Cloud service providers have agreements with one another and share resources.

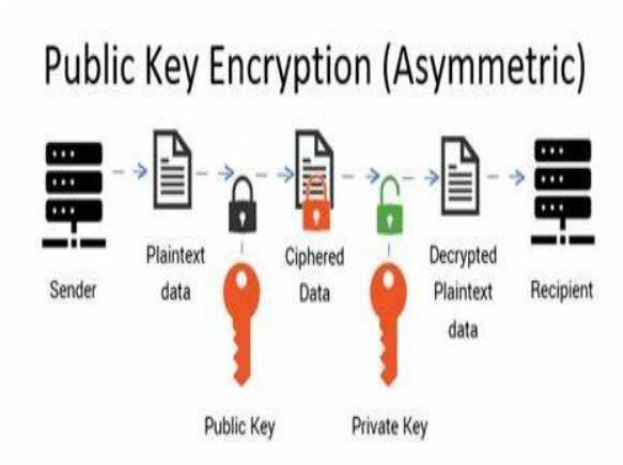
Data accessibility: Customer data is typically stored in sections on several servers that are frequently dispersed over various regions or dissimilar Clouds. As the availability of seamless and uninterruptible supply becomes more challenging in this situation, data availability becomes a significant and genuine concern.

FIGURE 1. CIA Triad of Data Protection Technology

Storage, backup, and recovery: If you decide to migrate your data to the cloud, the cloud provider should have suitable data resilience storage solutions in place. They should be able to provide RAID (Redundant Array of Separate Disks) storage systems at a minimum, while most cloud providers will store data in numerous copies across several independent servers. Furthermore, most cloud providers should be able to offer backup services, which is very significant for organizations that use cloud-based apps since it allows them to roll back to a previous state in the case of a catastrophic hardware failure.

3. RSA, DATA SECURITY

Issues In The Cloud, And Related Work: A. RSA (Ron Rivest, Adi Shamir, and Len Adleman) One of the earliest viable public-key cryptosystems was RSA. It is also commonly used for secure data transfer. The encryption key in such a cryptosystem is public, as opposed to the decryption key, which is kept secret, as illustrated in Fig. 1. RSA is composed of the first initials of Ron Rivest's, Adi Shamir's, and Leonard Adleman's surnames, who originally publicly announced the method in 1977.



In our suggested study, we are employing the RSA method to Encrypt the data to ensure that only the appropriate user has access to it. We prevent unauthorized access to the data by safeguarding it. User data is encrypted before being saved in the Cloud. When necessary, the user submits a request for data to the Cloud provider, who subsequently authenticates the user and distributes the data. RSA is a block cipher in which each message is assigned an integer value. RSA is made up of two parts: a public key and a private key. In our Cloud environment, Public-Key is known to everyone, but PrivateKey is known only to the person who owns the data originally. Thus, the Cloud service provider

does encryption, while the Cloud user or consumer performs decryption. Once encrypted with the PublicKey, the data can only be decrypted with the accompanying Private-Key. RSA algorithm involves three steps:

- Key Generation
- Encryption
- Decryption.

4. PROPOSED WORK

The popular public key algorithm is RSA. The acronym RSA refers to Ron Rivest, Adi Shamir, and Len Adleman, who first discussed it in public in 1977. Our suggested approach makes use of RSA. Algorithm to encrypt the data to offer security and restrict access to the concerned user exclusively. We are preventing illegal access by protecting the data. Before being stored in the Cloud, user data is encrypted. When necessary, a user submits a request for data to a cloud provider, who subsequently authenticates the user and sends the requested data. With the block cypher RSA, each message is assigned an integer. Public-Key and Private-Key make up RSA. Public Key is known to everyone in our cloud environment, but Private-Key is only known to the individual who initially owns the data. As a result, the Cloud service provider performs encryption, and the Cloud user or consumer performs decryption. Data that has been encrypted using a public key can only be decrypted with a corresponding private key.

Key Generation: Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps: 1

- Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
- Compute n = a * b.
- Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
- Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as a Public-Key exponent.
- Now determine d as follows: d = e-1(mod Ø(n)) i.e., d is multiplicate inverse of e mod Ø(n).
- d is kept as a Private-Key component, so that d * e = 1 mod Ø(n).
- The Public Key consists of modulus n and the public exponent e i.e, (e, n).
- The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n). Encryption: Encryption is the process of converting original plain text (data) into cipher text (data).

Steps: 2

- Cloud service provider should give or transmit the Public- Key (n,
- e) to the user who wants to store the data with him or her.
- User data is now mapped to an integer by using the anagreed-uponn reversible protocol, known as the padding scheme.
- Data is encrypted and the resultant cipher text(data) C is C = me (mod n).
- This cipher text or encrypted data is now stored with the Cloud service provider.

Decryption: Decryption is the process of converting the cipher text(data) to the original plain text(data).

Steps: 1

- The cloud user requests the Cloud service provider for the data.
- Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e, C.
- The Cloud user then decrypts the data by computing, m = Cd (mod n).
- Once m is obtained, the user can get back the original data by reversing the padding scheme.

5. EXPERIMENTAL RESULTS

In this section, we are taking some sample data end implementing the RSA algorithm over it.

Key Generation:

- We have chosen two distinct prime numbers a=61 and b=53.
- Compute n=a*b, thus n=61*53 = 3233.
- Compute Euler's totient function, Ø(n)=(a-1)*(b-1), Thus Ø(n)=(611)*(53-1) = 60*52 = 3120.
- Chose any integer e, such that 1 < e < 3120 is coprime to 3120. Here, we chose e=17.
- Compute d , d = e-1(mod Ø(n)), thus d=17-1(mod 3120) = 2753.

- Thus the Public-Key is (e, n) = (17, 3233,) and the the Private-Key is (d, n) = (2753, 3233). This Private-Key is kept secret and it is known only to the user. Encryption: 1. The Public Keyy (17, 3233) is given by the Cloud service provider to the user who wishes to store the data. 2. Let us consider that the user mapped the data to an integer m=65.

Encryption:

- The Public Keyy (17, 3233) is given by the Cloud service provider to the user who wishes to store the data.
- Let us consider that the user mapped the data to an integer m=65.
- Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user. C = 6517(mod 3233) = 2790.
- This encrypted data i.e the cipher text is now stored by the Cloud service provider.

Decryption:

- When the user requests the data the Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid).
- The cloud user then decrypts the data by computing, m = Cd(mod n) = 27902753(mod 3233) = 65.
- Once the m value is obtained the user will get back the original data.

6. CONCLUSION

The concept of cloud computing, which is still developing, views computing as an on-demand service. The moment a company decides to migrate its data to the cloud, it forfeits control over that data. As a result, the value of the data directly affects the level of protection required to keep it secure. Cryptography and trustworthy computing are essential for cloud security. As a result, only the authorized user may access the data in our suggested task. Even if an intruder unauthorized user) takes the data, whether unintentionally or on purpose, he is unable to decode it and retrieve the original data. Therefore, RSA algorithm implementation provides data security.

REFERENCES

[1]. P. Kalpana, “Cloud Computing – Wave of the Future”, International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3, ISSN 2249–071X, June 2012.
[2]. Subedari Mithila, P. Pradeep Kumar, ”Data Security through Confidentiality in Cloud Computing Environment”, Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2, 1836-1840, 2011.
[3]. Zaigham Mahmood, “Data Location and Security Issues in Cloud Computing”, Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.
[4]. Vishwa Gupta, Gajendra Singh, Ravindra Gupta, “Advanced Cryptography algorithm for improving data security”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 1, Jan 2012.
[5]. V. Sandhya, “A Study on Various Security Methods in Cloud Computing”, International Journal of Advanced Research in Computer Science, Volume 2, No.6, Nov-Dec 2011.
[6]. Simarjeet Kaur, “Cryptography and Encryption in Cloud Computing”, VSRD International Journal of Computer Science and Information Technology, Vol.2(3), 242-249, 2012.
[7]. Birendra Goswami, Dr.S.N.Singh, “Enhancing Security in Cloud computing using Public Key Cryptography with Matrices”, International Journal of Engineering Research and Applications, Vol 2, Issue 4, 339-344, July-Aug 2012.
[8]. G. Jai Arul Jose, C. Sanjeev, Dr. C.Suyambulingom, “Implementation of Data Security in Cloud Computing”, International Journal of P2P Network Trends and Technology, Vol 1, Issue 1, 2011.
[9]. William Stallings, “Network Security Essentials Applications and Standards”, Third Edition, Pearson Education, 2007.