SECURITY AND PRIVACY ON DATA IN CLOUD COMPUTING USING AES AND RSA ENCRYPTION TECHNIQUE

[1]Renuka S. Durge, [2]Vaishali M. Deshmukh
Sant Gadge baba University Amravati, Computer Science and Engineering, Amravati, India[1], Sant Gadge baba University Amravati, Computer Science and Engineering, Amravati, India[2]
renuka434@gmail.com[1], vmdeshmukh@mitra.ac.in[2]

ABSTRACT

Cloud computing paradigms are becoming extremely popular as a result of technical innovation and constant change. The primary goal of a cloud computing system is to give consumers pay-per-use access to on-demand processing and storage resources. It makes it affordable for small firms to use top-notch infrastructure. However, because Significant issues and obstacles for smart systems to continuously transfer generated data to the cloud computing resources, which a third-party provider maintains, including the cloud resource sharing property, data privacy and security. To address difficulties with data security, numerous encryption approaches have been developed. Cryptography is crucial for securing our data while it is being transmitted online. Text, image, audio, and video data are all made secure using cryptography. The basic objective is to keep data secure from unauthorized access while it is being sent and rendered unreadable. The role of cryptography essential function in achieving information secrecy, authenticity, integrity, and non-repudiation. Comparative examination and research of the cryptographic algorithms i.e. Advanced Encryption Standard (AES) and RSA algorithm (Rivest-Shamir-Adleman) is proposed in this work.

Keywords-Cryptographic Algorithms, Symmetric Key Cryptography, Encryption, Decryption, RSA, AES.

I. INTRODUCTION

Cloud computing has attracted a lot of scientific attention, due to the wide range of services it offers, The main concerns with cloud computing are its privacy and security. Security has many different meanings, including confidentiality, availability, and integrity. A perfect security system must efficiently ensure each security aspect. So, focuses solely on data security. Information technology has frequently faced serious problems with data security. Because the data is dispersed throughout the globe in the cloud computing environment, it becomes especially serious. The two main reasons users have privacy and data security concerns with cloud technology are data security and privacy protection.

Data security and privacy protection are becoming more crucial for the future growth of cloud computing technology in government, industry, and business, even if numerous techniques on the issues of cloud computing have been researched in both academics and industries. Both the hardware and the software in the cloud architecture are affected by difficulties with data security and privacy protection. This study intends to improve data security and privacy protection for a reliable cloud environment by reviewing various security strategies and difficulties from both software and hardware sides for securing data in the cloud. Therefore, we conduct a comparative review of the prior research on the data security and privacy protection strategies employed in cloud computing. [1]All technologies share the concern of data security. When used in an unregulated context like cloud computing, it poses a serious difficulty. A lot of datacenters throughout the world are used to store data. Virtual machines are used to calculate data. To meet their demands, users can establish many virtual machines with various capabilities and numbers [2]. When data calculation and storage are delegated to a third party, that entity also assumes responsibility for the data's security and compliance. The user submits his data to the datacenter, which the storage service stores and manages, before performing the calculation in the cloud. This information is subsequently forwarded to the virtual machines using the appropriate distributed technology for parallel

processing. After processing is complete, consumers can download and view the outcomes. Any private or personal information may be revealed throughout this process.

II. LITERATURE REVIEW

Ankit Fadia and Jaya Bhattacharjee [3] provide instructions on how to encrypt data in a way that keeps it safe from prying eyes. With the growing need to protect one's privacy in communications and transactions, it defines encryption, explains how it works, and provides examples of both. The idea of creating a key, cryptography, the most widely used encryption algorithms, how encryption functions, digital signatures, digital certificates, and most significantly, were all discussed.

By carefully monitoring the time necessary to carry out private key operations, Paul C. Kocher [4] describes how attackers may be able to determine fixed Diffe-Hellman exponents, factor RSA keys, and crack other cryptosystems. RSA and Diffe-Hellman attack prevention methods were also explained.He concluded by stating that some cryptosystems must be updated to defend against the attack, and future protocols and algorithms must include safeguards against timing attacks.

MM. AbdElnapi Noha [5], he employs RSA, AES, and a hybrid hash function in his Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing. Hybrid encryption offers improved performance, but its execution time is longer than that of RSA and AES.

Zaid Kartit [6] he employs homomorphic encryption while applying an encryption algorithm for data security in cloud storage when uploading and downloading files. Although the algorithm technique is quick to use in both upload and download directions, it is not very efficient.

A method called as the Enhanced Mutual Trusted Access Control Algorithm was put forth by Sarojiniet.al in [7]. (EMTACA).In order to prevent security-related problems in cloud computing, this technique establishes a mutual trust between cloud consumers and cloud service providers. In order to provide enhanced guaranteed and trusted cloud services among users in a cloud environment, a system that includes the EMTACA algorithm is proposed. The findings of this study demonstrated that the three most crucial aspects of data security—confidentiality, integrity, and availability—were attained.

"Research on data security technology based on cloud storage," Rongzhi Wang [8]. The POR system based on trusted log is based on the conventional POR system, trusted the log, and combined with the DSBT scheme, trusted architecture to achieve light weight, computational efficiency but also improve the quality, reach a consistent level.As the central component of the cloud storage prototype system, it introduces the implementation of the DSBT system based on trusted log and POR system. The system has a straightforward three-party security model, with Cassandra serving as the foundational platform for distributed storage; the subsystem is required to execute the logic module. It focuses on the interplay between the DSBT and POR modules as well as their design philosophy.

Security Algorithms for Cloud Computing, by Akashdeep Bhardwajm [9]. In order to identify the appropriate methods based on the parameters as follows, authors compared symmetric encryption techniques and encoding algorithms utilizing size and time. x File Size: indicates that a file of various sizes will be taken. Computing for Encryption Time: the length Encoding and Calculation Time: the amount of time an encoding algorithm needs to create a hash code. AES is a strong contender for key encryption, whereas MD5 is faster when encoding, according to the authors' analysis of symmetric algorithms for various encryption and encoding techniques.[10] presents security guidelines for cloud computing by Dimitra A. Geogiou. The security policies' goals are to safeguard

individuals and information, establish guidelines for acceptable user conduct, reduce risks, and aid in monitoring regulatory compliance.

On Software as a Service, they concentrated. And gave a thorough assessment and analysis of previous studies about cloud computing security. Dimitra reviewed the threats that are now present and concentrated on those that do not apply to traditional systems. The time it takes an algorithm to convert plain text into a cypher text.

A approach for evaluating various cloud hazards was developed in order to be able to discover new rules that were intended to be incorporated into the cloud policy. This study examined the security requirements for cloud service providers using the European E-Health System as a case study.November [11] Sheenal Malviya In order to provide dynamically secure group data sharing and access services in a decentralized manner, the Secure Data Sharing Scheme using Cryptographic Algorithm for Cloud Storage uses an earlier algorithm that is suitable for numerical data encryption but is ineffective for text-based cryptography.

Sayyid Sheik [12] December. Adaptive Block Based Data Encryption, Cloud Data Compression, and the Potential to Reduce Accessing Time between Cloud Clients via Cloud Servers are Methods to Secure the Data in Cloud Data Storage. However, these Methods Require a Longer Execution Time While Matching the Missing Storage Values.

Doaa Khudhur [13] "Using the whirlpool hash function for card number encryption to improve e-banking security." By hashing sensitive data like credit card numbers and account passwords, it has improved the security of e-banking systems using the MD5 message digest and Whirlpool. The only fields chosen to be hashed using Whirlpool are the card number and three-digit card verification code; all other fields are stored in plain text.Improve the Integrity of Data Using Hashing Algorithms, P Varaprasada Rao [14], Comparative analysis on all hash functions, MD5 hash function is more quickly, A hash for a password is produced and saved in a database; it cannot be reversed. Develop Cloud Security in Cryptography Techniques Using the DES-3L Algorithm Method in Cloud Computing, by Dr. D. Arivazhagan [15]Any files that are uploaded from the client are encrypted using the DES (Three Level Algorithm) algorithm to protect the privacy of the user. The Byte Insertion Encryption method is used, and the random data key generator provides the key. bites are created from the key. Bite insertion method encrypts a file by inserting a data key.The safer and more dependable triple DES Encryption algorithm is used for this encryption. Only the verified consumer can access the data because of the Multilevel Encryption and Decryption technique. Regardless of how the intruder (unapproved client) obtained the data, it would still be necessary for him to convert it at each measurement, which would be incredibly difficult without a genuine key.

III. OVERVIEW OF CRYPTOGRAPHIC ALGORITHM

A. Advanced Encryption Standard (AES)

Block-oriented symmetric key encryption is done using AES. It was created in 2000 and is thought to be a more secure algorithm than the Data Encryption Standard (DES). The replacement permutation network design approach serves as the foundation for AES.

It employs a 128 bit data block at a time, a key length of 128, 192, or 256 bits, and 10, 12, or 14 rounds. An array of bytes is used to divide up a data block. Such bytes are represented using polynomial representation as finite field elements.

The input is split into 16 bytes and then organized column-wise into a 4x4 matrix [6]. The state matrix is the name given to this matrix.The original 128-bit key is organized into a 4x4 matrix and partitioned into 16 bytes, just as 128-bit data. KeyMatrix is the name of this matrix.

These two matrices serve as the algorithm's essential inputs.

1) An initial round of AES encryption (0)

2) Nine general rounds (numbered 1 through 9) and

3) a conclusion (10)

The two matrices are simply XORed in round (0) using the AddRoundKey transformation. Round 1 receives Round 0's output as its input. Each round is made up of four unique, standardised, and invertible transformations, as depicted in the accompanying diagram: Subbytes, ShiftRows, MixColumn, and AddRoundKey [7][8].

B. Algorithm RSA (Rivest-Shamir-Adleman)

RSA is one of the primary algorithms used in encrypted connections and digital certificates. The 1977 invention of the public key algorithm by Ron Rivest, Adi Shamir, and Leonard Adelman (RSA). Calculating modular exponentiation is RSA's primary operation. RSA can be slow in contexts with restrictions since its foundation is arithmetic modulo large numbers [9]. Particularly, additional processing power and time will be needed when RSA decrypts the cypher text and creates the signatures. One method to quicken RSA decryption is to reduce modules in modular exponentiation. The security of RSA is determined by an integer.The method gains additional power and effectiveness through the generation of random prime numbers.

In RSA, the processes listed below are used to create the public and private keys [10]:

Step 1: First, choose two significant prime numbers, p and q, such that they are not equal.

Step 2: Determine n=p*q.

Step 3: Determine (pq)=(p-1)* (q-1)

Choose the public key e such that gcd ((n), e) = 1; 1 in step 4.

Choose the private key d such that d*e mod (n) = 1 in step 5.

Encryption: Calculate cipher text C from plaintext message M such that C=M ^e mod n

Decryption: M=C^d mod n=M^ed mod n

In the AES method, the same key is utilised for both encryption and decryption [11].Public keys and private keys are used in the RSA technique, respectively, for encryption and decryption. The chosen prime numbers p and q affect how quickly keys are generated and increase security. [12]

A. Encryption Phase

1. Phase 1 of encryption begins by applying the advance encryption standard algorithm to a text file that is being used as input (T0).

2. Using a secret key that gives the AES algorithm to encrypt the text (T1).

3. Only encrypting the AES key using ECC.

4. Using the RSA technique to encrypt (T1) and the ECC key.

5. This reveals the encoding key and the final encrypted text (Tf).

B. Decryption Phase

1. The first phase of decryption will use a reverse-order method.

2. Use the RSA encoding and decryption keys.

3. The T1 and ECC keys are provided.

4. Use the ECC algorithm to decrypt the encoding key.

5. Use the AES technique to decrypt T1 and recover T0's plaintext.

Comparative analysis of both the algorithms, The encryption speed of the AES algorithm is substantially faster than the RSA algorithm, according to algorithm analysis and prior studies. The RSA method can perform digital signature and identity authentication and is suitable for encrypting small amounts of data, whereas the AES algorithm is best for encrypting huge files or data. While the AES key distribution is quite challenging, the RSA algorithm has a minimal number of keys and the key management is simple. In conclusion, it is possible to protect the distribution of the AES key by encrypting both the AES key and the data using the RSA public key.

IV. CONCLUSION

Although sharing resources and providing on-demand services without having to spend a lot of money on creating the infrastructure and purchasing resources are advantages of cloud computing, several security issues must be solved before offloading data produced by smart devices. Many encryption algorithms and data privacy models have been put forth in the literature to deal with the problems that have arisen, but there are still areas that need further research. After evaluating several encryption algorithms for the data distributed by various appliances in the smart architecture, it can be said that choosing an algorithm based on the demands of the organisation must strike a delicate balance between complexity and security. There is no such thing as the "best" or "one-size-fits-all" algorithm; each algorithm must be evaluated on its own merits and Demerits. An algorithm with less complexity might not be suitable for highly sensitive material and will often take longer to encrypt or decode data. One of the most unique symmetric encryption techniques is the Blowfish one. The AES is the most secure symmetric algorithm when processing speed and time are constrained. Because the public-private key pair security of the RSA algorithm is more assured, it is suited for sharing confidential information in situations where it must remain secret. Currently, research is being done to create an encryption algorithm that performs well and grows well with the growth of data produced quickly by intelligent systems.

V. FUTURE SCOPE

The biggest barrier preventing smart systems management from moving their data to the cloud is data security. To prevent a third party from hacking authentication information, keys used for data encryption and decryption should be more securely stored. By accomplishing this, we can prevent data manipulation. Data security can be achieved by combining several encryption methods, but performance will suffer as a result of the longer encryption and decryption times. Parallel data encryption can be taken into consideration in upcoming development for optimal throughput.

REFERENCES

1. Arjun, U., Vinay, S.: A short review on data security and privacy issues in cloud computing.In: IEEE International Conference on Current Trends in Advanced Computing, pp. 1–5.IEEE March (2016)
2. Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. J. Internet Serv. Appl. 4, 5.(2013)
3. Ankid Fadia, Jaya Bhattacharjee, “Encryption, Protecting Your Data”, Vikash Publishing House Pvt Ltd, 2007, ISBN: 812592251-2
4. Paul C. Kocher, "Timing Attacks on Implementations of DiffeHellman, RSA, DSS, and Other Systems", Cryptography Research Inc., San Francisco, USA.
5. Noha MM. AbdElnapi. “A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing”., International Journal of Computer Science and Information Security, Vol. 14 (4) , April 2016.
6. Zaid Kartit “Applying Encryption Algorithm for Data Security in Cloud Storage” https://www.researchgate.net/publication/301324486. ,January 2016.

7. Sarojini G. et.al (2016) Trusted and Reputed Services using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud, 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016).
8. Rongzhi Wang,"Research on data security technology based on cloud storage" 13th Global Congress on Manufacturing and Management, GCMM 2016., Available online at www.sciencedirect.com.
9. Akashdeep Bhardwaj., "Security Algorithms for Cloud Computing", International Conference on Computational Modeling and Security (CMS 2016).
10. Dimitra A. G. (2017) Security Policies for Cloud Computing, Available: http s:// www.dion e.li b.u nip i .gr/xmlui/bitstream/handle/unipi/11007/Georgio u_Dimitra.pdf?
11. Sheenal Malviya "Secure Data Sharing Scheme using Cryptographic Algorithm for Cloud Storage "International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 20 (2018) pp. 14799-14805.
12. Saidhbi Sheik "A Way to Secure the Data in Cloud Data Storage by Using Cloud Data Compression Mechanism" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-4S2, December 2018.
13. Doaa Khudhur, "Enhancing e-banking security: using whirlpool hash function for card number encryption", International Journal of Engineering & Technology, 7 (2.13) (2018) 281-286
14. P Varaprasada Rao, "Improve the Integrity of Data Using Hashing Algorithms" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-7, May, 2019.
15. Dr. D. Arivazhagan., "Develop Cloud Security In Cryptography Techniques Using DES-3L Algorithm Method In Cloud Computing", International Journal Of Scientific & Technology Research Volume 9, Issue 01, January 2020.