Comparative Analysis of AES and RSA Algorithm for Cloud File Transfer

Malathi R[1], Srinivasan P[2], Sudha C[3], Elakiya V[4]

[1,2,3,4]Department of Computer Science Engineering,CK college of Engineering and Technology

ABSTRACT

Cloud computing improvements have resulted in information being contracted by cloud services. Dropbox and Google Drive are cloud storage services that provide users low-cost storage. We provide a way of protecting files by encrypting and decrypting them, which provides an enhanced level of security. We use the Double encryption approach to encrypt the files that we upload to the cloud. The file is encrypted twice, one after the other, using the two algorithms. The file is encrypted using the AES method first, followed by the RSA algorithm. During the algorithm's execution, the corresponding keys are created. This strategy raises the level of security. The parameters covered here include security level, speed, data confidentiality, data integrity, and cypher text size. Our method is more efficient as it satisfies all the parameters where the conventional methods failed to do so. DropBox is the cloud service we utilised to store the file's content, which is encrypted using the AES and RSA algorithms.

IndexTerms - DES, AES, RSA, Encryption, Decryption, Secret Key and Cryptography.

I.INTRODUCTION TO CLOUD COMPUTING

The study of computing services delivered over the cloud (Internet), such as servers, storage, databases, networking, software analytics, and intelligence, is known as cloud computing. Cloud computing is an alternative to an on-site data centre. Everything in an onsite data centre must be managed, including obtaining and installing hardware, configuring virtualization, installing the operating system, and any other software required. Creating the network, configuring the firewall, and configuring the storage. The cloud environment provides a readily accessible web gateway that allows the user to control compute, storage, network, and application resources.

II.LITERATURE REVIEW

To provide a comprehensive understanding of the comparability of these concepts, this section delves into the existing literature, conducting a thorough survey and comparative analysis of cryptographic methods. The survey encompasses various aspects of cryptographic concepts employed for authentication and protection against third-party interference. Notably, AES and DES have been widely implemented across numerous sites due to their ability to instill confidence in secure communication. This confidence ensures that messages are shared exclusively with trusted individuals.

III.DEPLOYMENT MODELS

Deployment models define the sort of access to the cloud environment, that is, how the cloud is discovered. The cloud divides accessibility into four categories: There are four types of education: private, public, hybrid, and community.

Public cloud: This cloud is open to the public. Clients can register with the cloud through the internet and access cloud resources on a pay-per-use basis. This Cloud computing is not as secure as private cloud computing. It may be accessible to all. Because of its openness, the internet attracts people. It is considerably less. Private cloud is more customisable than public cloud. The cloud infrastructure is made up of a major Cloud Service Provider owns and manages (CSP).The cloud provider is in responsible of creating and maintaining the general public cloud and its IT resources. The open cloud is also known as the external cloud. Resources are powerfully provisioned on a self-benefits basis. Across the web. As an example, consider email, Google AppEngine, Microsoft Azure, or Azure from Microsoft and Amazon Elastic Compute Cloud (EC2).

Private cloud: A private cloud is one that is set up specifically for an organisation within its own data centre. The organisations handle all of the cloud resources that they own. When compared to an open or hybrid cloud, the private cloud provides higher security. Private cloud resources are not as cost-effective as public cloud resources, but they are more productive than open cloud resources. The cloud is managed by an organisation and only serves it; it might reside within or beyond the organization's boundaries. The private cloud, often known as the internal or corporate cloud, provides assisted devices to a limited number of people inside a firewall.

Community cloud: A group of organisations collaborate to construct and provide a similar cloud architecture, as well as policies, requirements, values, and concerns. The community cloud develops into a level of economic scalability and democratic balance. The cloud infrastructure could be provided by a third-party vendor or by one of the community's organisations. The cloud is managed by a few organisations and supports a specific community with a similar interest. The private cloud is more secure than the public cloud.

Hybrid cloud: A hybrid cloud is a combination of public, private, and community clouds. However, private cloud is used for vital activities, whereas public cloud is used for non-critical activities. Because public cloud is more expensive than private cloud, hybrid cloud can save money. Because hybrid cloud models rely on internal IT infrastructure, it is critical to ensure excess across data centres.

IV.SERVICE MODELS

A cloud can connect with a customer (client or application) in an assortment of courses through abilities called services. Services Models are the functional models where the Cloud Computing is based. Across the web, three major types of services have emerged or model of services have emerged.

1. Infrastructure as a Service (IaaS).
2. Platform as a Service (PaaS).
3. Software as a Service (SaaS).

Infrastructure as a Service **(Iaas)** : Cloud computing services include physical and virtual computers, extra capacity storage devices, and so on. Hypervisors handle the virtual computers, which are organised into pools and governed by operational emotionally supportive networks. It is the responsibility of cloud customers to install working framework images as well as their application code on virtual machines. IaaS enables cloud providers to easily locate infrastructure over the Internet. Customers can access storage, bandwidth, monitoring services, IP addresses, firewalls, virtual machines, and other IaaS resources on a monthly basis. The consumer must pay for the amount of time he or she has access to a resource. Examples include Windows Azure and Amazon EC2.

Platform as a service **(PaaS)**: This is the distribution of an application development and deployment platform via the internet as a service to developers, who can then use the platform to easily build, launch, and manage SaaS applications. It also provides the necessary tools for application development and deployment. The main component of PaaS features a point-and-snap device that allows non-designers to create web apps. Buyer does not need to acquire pricey servers, equipment, power, or data storage. As a result, scaling down or scaling up based on application resource needs is not difficult.Force.com, Google, Apache StratosApp, Engine, Windows Azure, and AWS Elastic Beanstalk are a few examples.

Software as a Service **(SaaS)**: It is the delivery of applications (e.g., ERP or CRM) to end users via the web via browsers. Cloud users can use that which is already installed and operational on the cloud infrastructure. In this approach, there is no need to install and operate the software application on individual PCs. Also eliminated is the need for software maintenance and support. Some SaaS applications, such as an Office Suite, are not flexible. In each situation, SaaS provides an Application Programming Interface (API) that allows developers to create a customised application. Google Apps and Microsoft Office 365 are two examples.

V.CHARACTERISTICS OF CLOUD COMPUTING

Cloud computing have some of the following characteristics in order to meet client or user requirements and to provide qualitative services.

1. High scalability: On-demand delivery of resources on a massive scale without the need for human coordination with each service provider.
2. High availability and reliability: Because server availability is more reliable and high, the risks of infrastructure disappointment are reduced.
3. Agility: It distributes resources to users and works swiftly.
4. Multi-sharing: By utilising distributed computing, various customers and applications can function more effectively and at a lower cost.
5. Maintenance: Because cloud computing programmes do not need to be installed on each computer and may be accessed from multiple locations, they are easier to maintain.
6. Low cost: It saves money because the corporation no longer has to put up its own infrastructure. It pays based on the amount of resources consumed.
7. Pay-per-use services: APIs (Application Programming Interfaces) are provided to clients in order for them to access cloud services and pay on the basis of service usage.
8. On-Demand Self Service: Cloud Computing enables clients to access services and resources on demand without requiring human interaction with cloud service providers.

VI.CHALLENGES OF CLOUD COMPUTING

Cloud computing is a trendy issue right now, and there is a lot of confusion about how to manage its features and resources. As technology advances, so does the necessity for companies to employ the most up-to-date Cloud frameworks. Cloud solutions provide advantages such as data security, flexibility, efficiency, and high performance. Among its benefits are smoother operations and increased enterprise cooperation while lowering costs. However, the Cloud is not without flaws, particularly in terms of data management and privacy concerns.

1. Data Protection and Privacy

When working with Cloud settings, data security is a big concern. It is one of the most difficult difficulties in cloud computing since users must accept responsibility for their data, and not all cloud providers can guarantee 100% data privacy. Cloud privacy leaks are commonly caused by a lack of visibility and control mechanisms, a lack of identity access management, data misuse, and cloud misconfiguration. Insecure APIs, malicious insiders, and oversights or carelessness in Cloud data management are other issues.
Solution: To avoid security risks, configure network hardware and apply the most recent software updates. Some methods for preventing data security threats include using firewalls, antivirus, and increasing bandwidth for Cloud data availability.

2. Environments with Multiple Clouds

Configuration problems, a lack of security patches, data governance, and a lack of granularity are all common cloud computing issues and challenges in multi-cloud settings. It is challenging to track multi-cloud security needs and apply data management standards across many boards.
Solution: For businesses, implementing a multi-cloud data management solution is an excellent place to start. Not all solutions will provide certain security features, and multi-cloud settings are becoming increasingly sophisticated and complex. Terraform and other open-source solutions provide you a lot of power over multi-cloud infrastructures.

3. Performance Challenges

The performance of Cloud computing solutions is dependent on the vendors who provide these services to clients, and if a Cloud vendor fails, the business suffers as well. It is one of the most significant difficulties related with cloud computing.
Solution: Sign up with Cloud Service Providers who have policies in place for real-time SaaS monitoring.

4. Lack of Knowledge and Expertise

Another typical obstacle in cloud computing is the difficulty in locating and hiring the right Cloud talent. In the industry, there is a scarcity of professionals with the necessary qualifications. Workloads are increasing, as is the quantity of tools released onto the market. Enterprises require specialist knowledge to use these tools and determine which ones are best for them.
Solution: Hire cloud professionals with DevOps and automation specialisations.

5. Reliability and Availability

Cloud service unavailability and reliability are two important issues in these ecosystems. To keep up with increasing business requirements, organisations are pushed to seek greater computing resources. When a Cloud vendor is hacked or otherwise compromised, the data of organisations who use their services is compromised. It is only one of several cloud security concerns and issues that the industry is facing.
Solution: Using the NIST Framework standards in cloud systems can significantly improve both features.

6. Password Security

Account managers use the same passwords to administer all of their Cloud accounts. Password management is a crucial issue, and users frequently resort to using overused and weak passwords.

Solution: To secure all of your accounts, use a robust password management solution. Use Multifactor Authentication (MFA) in addition to a password manager to increase security. Cloud-based password managers that are effective warn users of security dangers and leaks.

7. Cost Management

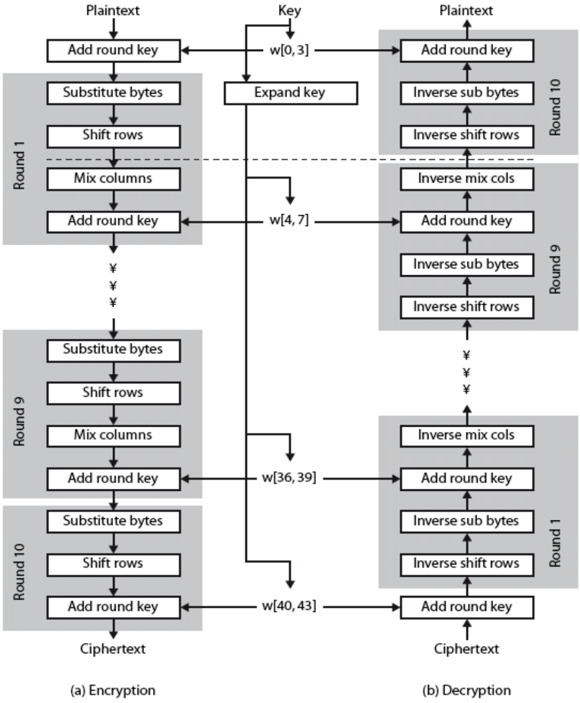
Even while Cloud Service Providers (CSPs) provide services on a pay-as-you-go basis, the prices can pile up. Hidden costs manifest themselves in the form of underutilised resources in businesses. Solution: Auditing systems regularly and implementing resource utilization monitoring tools are some ways organizations can fix this. It's one of the most effective ways to manage budgets and deal with major challenges in cloud computing.

8. Inadequate knowledge

Cloud computing is a highly competitive field, and many professionals lack the necessary skills and experience to work in it. There is also a significant supply-demand imbalance for certified individuals, as well as a large number of job openings.

VII.AES ALGORITHM:

This section provides a high-level overview of the AES algorithm. AES operates on fixed block sizes of 128 bits, with key sizes of 128, 192, or 256 bits. It employs a substitution-permutation network (SPN) structure and consists of multiple rounds, each with distinct transformation steps such as SubBytes, ShiftRows, MixColumns, and AddRoundKey. These steps together create confusion and diffusion, which are fundamental principles of modern cryptographic algorithms.



(a) Encryption (b) Decryption

Fig 1: Block Diagram for AES Encryption and Decryption

Encryption and Decryption:

The encryption process involves several rounds of transformations applied to the plaintext using the generated round keys. Each round utilizes the four main operations (SubBytes, ShiftRows, MixColumns, and AddRoundKey) to scramble the data. This section elaborates on the steps involved in AES encryption. AES decryption is essentially the reverse of the encryption process. It involves applying the inverse of each transformation step in the reverse order. The decryption process is as secure as encryption and ensures the original plaintext is accurately retrieved.

VIII.RSA ALGORITHM:

RSA (Rivest-Shamir-Adleman) is one of the most widely used asymmetric encryption algorithms, known for its robustness and secure data transmission. RSA is based on the mathematical properties of large prime numbers and their computational complexity. The algorithm involves key generation, encryption, and decryption processes. Key generation includes the selection of large primes, calculating public and private keys, and ensuring their security.

Encryption and Decryption:

RSA encryption uses the recipient's public key to encrypt plaintext data. This section describes the encryption process, which involves converting the plaintext into a numerical representation, raising it to the power of the recipient's public key, and taking the modulo of the result with the public modulus. RSA decryption, on the other hand, uses the recipient's private key to recover the original plaintext from the encrypted data. This section explains the decryption process, which involves raising the ciphertext to the power of the recipient's private key and then taking the modulo of the result with the private modulus.

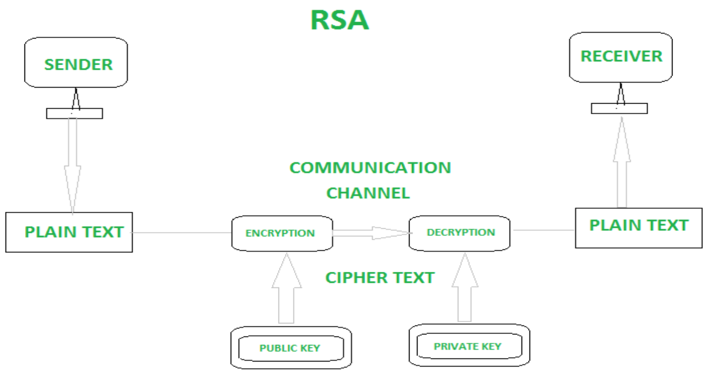


FIG 2:Encryption and Decryption Using RSA

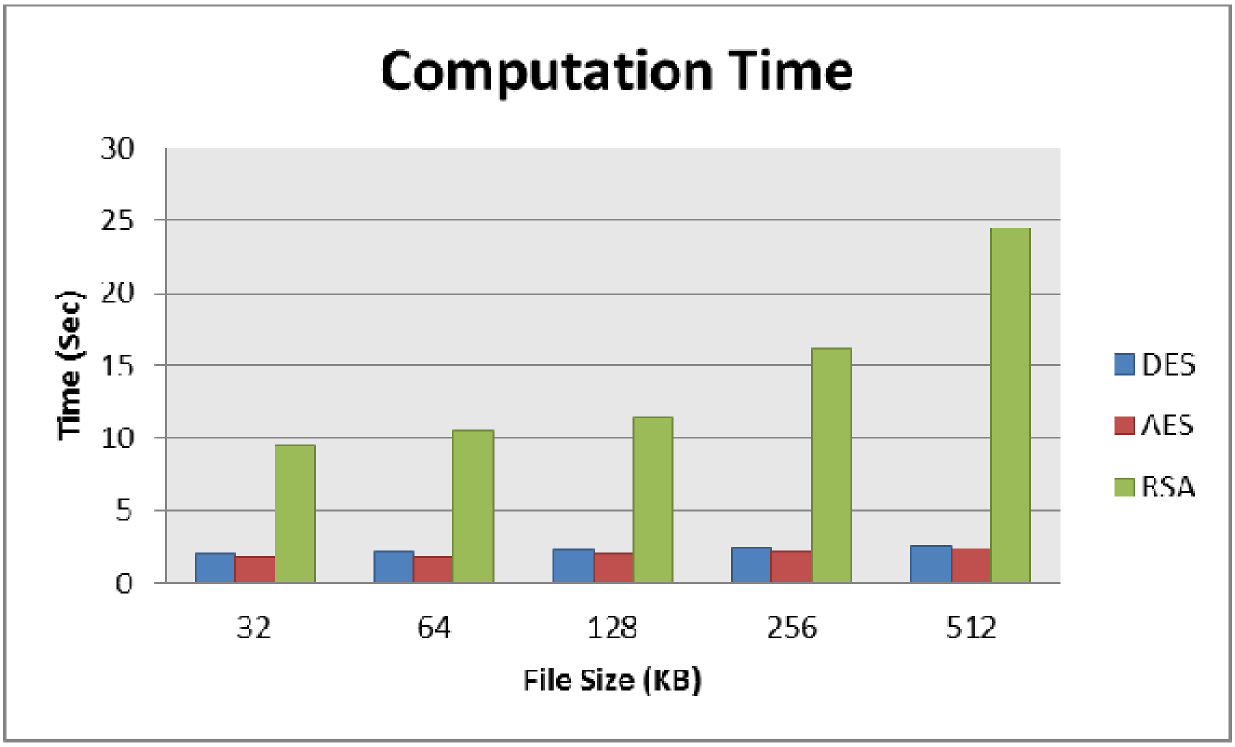
IX.SECURITY AND RECOMMENDATION

Both RSA and AES-256 are considered secure when implemented correctly with appropriate key lengths. However, AES-256 is generally preferred for securing data at rest and data in transit due to its efficiency and robustness. For secure communication, AES-256 with proper key management is often a better choice, as it provides faster encryption/decryption and requires fewer computational resources compared to RSA. RSA is more commonly used for key exchange and digital signatures, which are essential for establishing secure communication channels but might not be as efficient for bulk data encryption.

X.DIFFERENCE BETWEEN AES AND RSA ENCRYPTION

Attribute	AES	RSA
Type	Symmetric key encryption	Asymmetric (public key) encryption
Key Length	128, 192, or 256 bits	1024, 2048, or 4096 bits (common)
Speed & Efficiency	Fast and efficient for bulk data	Slower, not suited for large data
Use Cases	Encrypting files, databases, and channels	Key exchange, authentication, signatures
Encryption Process	Substitution-permutation network	Modular exponentiation
Key Distribution	Requires a secure method to share the secret key	No need to securely share the public key
Computational Complexity	Relatively low	High, especially for large key lengths
Attack Resistance	Vulnerable to brute-force attacks, but still secure	Vulnerable to advances in factoring techniques
Key Management	Easier, as only one key is involved	More complex due to separate public and private keys
Suitability for Hardware	Well-suited for hardware implementation	Hardware implementation can be more challenging
Quantum Resistance	Vulnerable to quantum attacks (e.g., Grover’s algorithm)	Potentially vulnerable to quantum attacks
Example	Secure file storage and communication	Secure email and digital certificates

XI.COMPARITIVE ANALYSIS



XII.CONCLUSION

RSA is generally considered more efficient than AES for data encryption due to its symmetric nature and faster cryptographic operations. However, the choice between RSA and AES ultimately depends on the specific use case and the cryptographic requirements of the application. RSA is still essential for tasks like key exchange and digital signatures, while AES is the preferred choice for securing data at rest and data in transit. It is also important to note that proper key management and implementation practices significantly impact the overall security of both algorithms.

REFERENCES

1. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES—The Advanced Encryption Standard. Springer.
2. National Institute of Standards and Technology (NIST). (2001). FIPS PUB 197: Advanced Encryption Standard (AES)
3. Kumari, S., & Ahuja, A. (2017). A Comprehensive Survey of RSA and Its Security Aspects. International Journal of Computer Applications.
4. Saxena, A., Kumar, M., & Gupta, M. (2019). A Comprehensive Survey on RSA Cryptosystem and Its Security Issues. International Journal of Computer Applications.
5. Lim, C. C., & Lee, S. S. (2014). A Survey on the Security of RSA Cryptosystem. International Journal of Cryptography and Information Security.
6. Adhikari, M., & Biswas, G. P. (2018). A Comprehensive Survey on Advanced Encryption Standard (AES). International Journal of Computer Applications.
7. Saripalli, P., & Srikanth, S. (2016). A Survey on the Advanced Encryption Standard. International Journal of Computer Applications

8. Kou, W., & Sun, Y. (2019). A Review of Advanced Encryption Standard (AES) Algorithms. International Journal of Advanced Computer Science and Applications.
9. U. Kumar and M. Prakash, "A Hybrid Encryption Algorithm for Secure Data Storage on Cloud", International Journal of Creative Research Thoughts (IJCRT), vol. 8, no. 2320-2882, 2020.
10. Anjali Patil, Nimisha Pa.tel, Dr. Hiren Patel "Secure data sharing using cryptography in cloud environment", 2016 .
11. Kota Chandu, SECURE FILE STORAGE IN THE CLOUD USING HYBRID CRYPTOGRAPHY, Aurora's Technological & Research Institute Date Written: September 4,2022.
12. K.Jaspin,ShirleySelvan,Sahana.S,Thanmai. G, "Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm" ,International Conference on Emerging Smart Computing and Informatics "(ESCI),2021.
13. Yahia Alemami, Ali M. Al-Ghonmein, Khaldun G. Al-Moghrabi, Mohamad Afendee Mohamed, "Cloud data security and various cryptographic algorithms", International Journal of Electrical and Computer Engineering (IJECE), 2023.