International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Providing More Security to Data Stored in Multi-Cloud Environment Using Encryption and Decryption Techniques

Kushala M V[1]
Assistant Professor,
Dept. of AIML,Dr.AIT
kushalmv@gmail.com

Dr. B S Shylaja[2]
Professor,
Dept. of ISE,Dr.AIT,
Shyla.au@gmail.com

Abstract: Because multi-cloud computing may lower service costs in a multi-cloud environment, it is an emergent idea that has become the newest subject of study. Because there is a lack of centralized management and diverse technologies, managing user access across numerous cloud systems is challenging. For uniform rules, native controls from different multicloud providers are insufficient. A centralized framework that unifies security and access controls across all platforms is necessary for a successful multi-cloud security approach. The RSA algorithm is the method used to improve data security. Time complexity, space complexity, and throughput are the three main factors used to evaluate security performance. Research projects involve encrypting data with RSA to restrict access to certain users and thwart unwanted access. The information is multi-cloud stored, encrypted, and released upon user.

Key Words :- Multi-cloud, RSA algorithm, Encryption, Decryption, Time Complexity, Space Complexity.

I INTRODUCTION

Cloud computing is a well-known and quickly expanding sector that is well-known for its ability to save costs and provide on-demand Internet services. However, because data is shared and kept in an open manner, security concerns prevent cloud environments from being widely used. A solution to this problem is suggested that makes use of the RSA algorithm. To ensure that only authorized users may access user data saved in the cloud, this solution encrypts the data before it is placed there. The performance of this approach is assessed by analyzing three important parameters: throughput, space complexity, and time complexity. Users may access their encrypted data by authenticating with the cloud provider, and this security feature boosts data safety by preventing illegal access.

Multi-cloud computing involves the use of different cloud services from different cloud service providers (CSPs). It can be implemented in a private cloud, a public cloud, or a combination of both. Organizations are adopting multi-cloud strategies to access services from multiple CSPs, which helps distribute computing resources, reduce the risk of service outages, and prevent data loss[4].

For companies of all sizes, cloud computing is a driving force, yet data security on the cloud is a big worry. Because of the crucial role of cloud computing and the sophisticated data it processes, this risk is magnified. Concerns about security and privacy are impeding the broader use of cloud services. There are a few key things you should ask yourself before selecting a cloud service. This entails evaluating their security procedures, financial soundness, and if the infrastructure is virtualized or shared with other customers. When data moves to the cloud, it experiences several changes and difficulties. User permission and

authentication are essential components of effective cloud data protection, which goes beyond merely putting security procedures into place. There are several distribution and deployment strategies for cloud computing, including SaaS,IaaS, PaaS, private cloud, public cloud, hybrid cloud and community cloud.

Data processing is becoming more and more in demand in a variety of industries today, including healthcare, business, geography, education, finance, and engineering. Effective data processing is shown to need the use of cloud computing. It serves as a high-performance computing paradigm that facilitates large-scale scientific applications and provides services via the Internet [1]. Six stages in the evolution of computing may be distinguished, as Figure 1.1 illustrates. Users of mainframe computers share a central processing unit (CPU) through terminals in the first stage of the system. The second stage is seeing a rise in the use of standalone PCs. A local area network (LAN) is used to connect personal computers in the third stage. The growth of the Internet and the network of networks is included in the fourth stage. The. Grid computing, or the cooperative use of various high-performance computing resources for specialized tasks, is the fifth phase. The sixth and final step is cloud computing, which offers computer resources as a service over the Internet. No matter where they are or when they need them, users may have their computer resources dynamically allocated to them thanks to cloud computing. Adopting cloud computing can also help government organizations become more efficient since it allows for the dynamic distribution of resources [2].

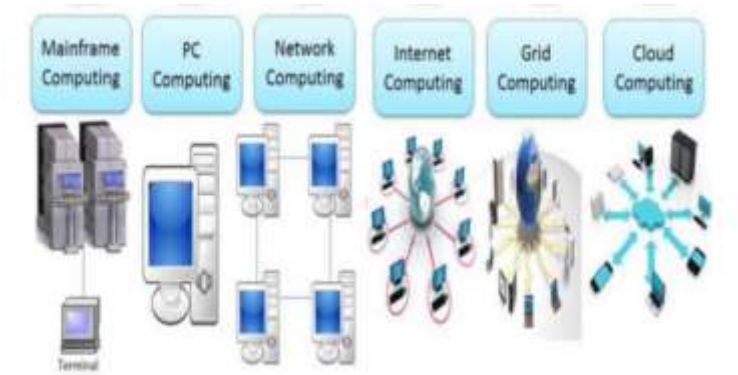


Figure 1.1 : Recent developments in Computing.

Implementing reasonable and efficient VM allocation in Cloud Data Centers (CDC) is indeed crucial for maximizing resource utilization, optimizing performance, and minimizing costs. There are several strategies and techniques that can be employed to achieve this[13]:

Resource Monitoring and Management: Continuous monitoring of resource usage such as CPU, memory, storage, and network bandwidth can provide insights into the current state of the infrastructure[14]. Predictive analytics and machine learning algorithms can be applied to forecast resource demands and identify potential bottlenecks before they occur.

Dynamic Scaling: Implementing auto-scaling mechanisms allows VMs to be provisioned or deprovisioned automatically based on workload demands. The system dynamically adjusts resource allocation, expanding capacity when usage peaks and reducing it during quieter periods.

Load Balancing: Distributing incoming traffic across multiple VM instances helps prevent overloading of any single instance and ensures that resources are utilized evenly. Load balancers can intelligently route requests based on factors such as server response time, current load, and geographic proximity[15].

Placement Policies: Developing intelligent placement policies for VMs involves considering factors such as workload characteristics, resource requirements, affinity or anti-affinity constraints, and data locality. Placement decisions can be optimized using algorithms such as bin packing, which aim to minimize resource fragmentation and maximize utilization.

Virtual Machine Migration: Live migration techniques enable VMs to be moved between physical hosts with minimal disruption to ongoing processes. Migration can be used for load balancing, consolidation of underutilized resources, and maintenance activities such as hardware upgrades or software patching.

Elasticity and Flexibility: Designing the infrastructure to be elastic and flexible allows for rapid provisioning and deprovisioning of resources in response to changing demands. This may involve utilizing containers or serverless computing frameworks in addition to traditional VMs.

Cost Optimization: Considering cost implications in VM allocation decisions is essential for maintaining efficiency. This includes factors such as pricing models (e.g., pay-as-you-go vs. reserved instances), resource utilization, and workload scheduling to minimize idle resources and optimize spending.

Fault Tolerance and High Availability: Ensuring resilience against failures through redundancy and replication of VM instances helps maintain service availability. Strategies such as distributed data storage, fault-tolerant architectures, and automated failover mechanisms contribute to high availability.

By incorporating these strategies into VM allocation policies and management frameworks, cloud providers can achieve optimal resource utilization, performance, and cost-effectiveness in CDC environments. Continuous monitoring, optimization, and adaptation are essential for adapting to evolving workload patterns and technological advancements in cloud computing.

The emergence of cloud computing is changing the business landscape and having varying effects on various groups. Cloud-based IT administration, encompassing processing, storage, and apps, is becoming the norm for IT clients and utilities. Internet and software developers are increasingly using web-scale programming, while infrastructure administrators and suppliers are overseeing massive, scattered data centers connected to IP networks. In summary, cloud computing is transforming the usage and management of IT resources, which has a range of consequences for different stakeholders[3].

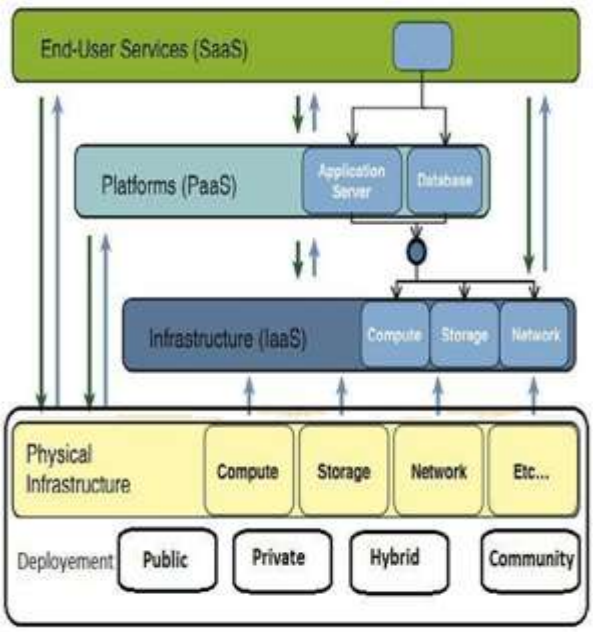


Figure 1.2 : Cloud Computing Architecture.

1.1 Problem Classification

The primary objective of cloud computing is to enhance computational capacity, improve accessibility to cloud services and resources, and ensure secure data transmission and storage, all while minimizing costs and search times[3]. The challenges are as follows,

- ❖ Consistency
- ❖ Limited scalability
- ❖ Data replication
- ❖ Trust,security,and privacy
- ❖ Unreliable availability of cloudresources
- ❖ Portability

II RSA SECURITY ISSUES IN THE CLOUD AND RELATED WORK

2.1. RSA: Ron Rivest, Adi Shamir, and Len Adleman are the names of the three people who invented this ground-breaking public-key cryptosystem. Using a public encryption key and a private decryption key, it is a basic technique for safe data transfer. This approach is still commonly used for cryptography, having

been initially developed by Rivest, Shamir, and Adleman in 1977.

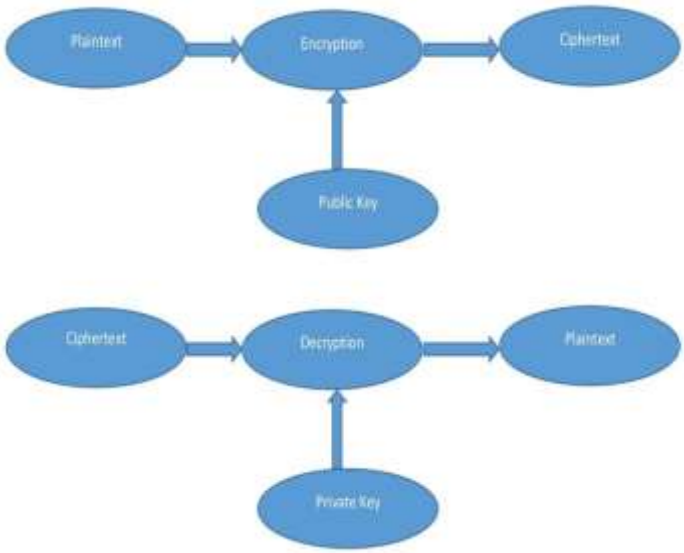


Figure2: Public Key System.

In order to improve security and guarantee that only authorized users may access user data, this paper suggests using the RSA technique to encrypt it. The data is protected from unwanted access by this encryption technique. The user's data is first encrypted before being saved in the cloud. The user asks the Cloud provider for the data when needed, and the provider confirms the user's identity before granting access.

The RSA algorithm uses a block cipher technique in which an integer is assigned to each message. It consists of two main parts: the Private-Key, which is only known to the user who owns the data, and the Public-Key, which is available to everyone. In our cloud system, the cloud service provider handles encryption, and the cloud does decryption.

2.2. RELATED WORK.

Numerous noteworthy studies have been carried out in the areas of cryptographic algorithms and cloud computing security. A security model based on a multilayer encryption and a scrambling algorithm was presented by Malakooti et al. [5]. They used picture data meant for cloud storage to test their hypothesis.Arockiam et al.'s [6] main goal was to combine transposition and substitution ciphers to improve traditional encryption methods. For every alphabet, their suggested technique transforms plain text into an ASCII code value.A multi-agent system and decision-making theory are combined in Yang Xu et al.'s [7] agent-aid model to handle workload balancing problems in big cloud settings. Their concept seeks to improve efficiency and optimize data distribution, especially in applications that need large amounts of data, such as distributed data mining.Mohamed et al.'s assessment [8] looked at eight contemporary encryption methods, such as Blowfish, DES, 3DES, AES, MARS, RC4, and RC6. Their goal was to determine which encryption method will work best and be the most secure for cloud computing architecture.A secure cloud architecture was created by Tirthani et al. [9] to guarantee the safe movement of data between clients and servers. They combined linear and elliptical cryptography techniques, using Elliptic Curve Cryptography for data encryption and the Diffie-Hellman Key Exchange mechanism for secure communications.VeerrajuGampala et al. [10] used elliptic curve cryptography for encryption and digital signatures to investigate data security in cloud computing. Their work, which covers key creation, signature generation, encryption, decryption, and signature verification, focuses on safe data transfer.

III PROPOSED WORK

The suggested solution include encrypting data using the RSA technique to improve security and limit access to authorized individuals. Users can request access to their data, which is verified and provided by the cloud provider, and their data is encrypted before being stored in the cloud. Using the Eclipse IDE and Java, the study will put the RSA algorithm into practice and evaluate its throughput, time complexity, and space complexity[11–12]. The RSA cryptographic system operates through three key phases: generating keypairs, encoding data, and recovering the original message. In this framework, while the encryption key is publicly accessible, the decryption key remains exclusively with the data owner. Within cloud environments, the service provider handles the encoding operations, while users perform the decoding process. RSA's mathematical foundation relies on modular exponentiation, utilizing two

distinct values: a public component 'e' and a confidential component 'd'. When encoding information, the algorithm incorporates a substantial numerical value 'n', which emerges from the initial key generation stage.

Key generation is a crucial step in data encryption, involving collaboration between the Cloud service provider and the user. Here are the key steps involved:

- Select two distinct prime numbers, denoted as 'a' and 'b,' chosen randomly for security, with similar bit lengths.
- Compute 'n' as the product of 'a' and 'b': n = a * b.
- Calculate Euler's totient function, Ø(n), as (a-1) * (b-1).
- Choose an integer 'e' such that 1 < e < Ø(n), and ensure that the greatest common divisor of 'e' and Ø(n) is 1. This 'e' becomes the Public-Key exponent.
- Determine 'd' as follows: d = e^(-1) mod Ø(n), which means 'd' is the multiplicative inverse of 'e' modulo Ø(n).
- Keep 'd' as the Private-Key component, satisfying the equation d * e ≡ 1 mod Ø(n).
- The Public-Key consists of the modulus 'n' and the public exponent 'e,' represented as (e, n).
- The Private-Key consists of the modulus 'n' and the private exponent 'd,' which must be securely kept, denoted as (d, n).

Encryption: Using a series of procedures, plain text data is converted into cipher text data through encryption. First, the user who wants to store data receives a public key (n, e) from the cloud service provider. Next, a padding scheme—a mutually agreed-upon reversible protocol—is used to turn the user's input into an integer. Following encryption, the data is transformed into cipher text data (C), which is expressed using the formula C = m^e (mod n). Ultimately, the cloud service provider stores this encrypted data.

Decryption: Decryption is the procedure of converting encrypted data (cipher text) back into its original plain text form. This process involves the following steps:

- The cloud user initiates a request to the cloud service provider for the data.
- The cloud service provider confirms the user's authenticity and provides the encrypted data, denoted as "C."
- The cloud user proceeds to decrypt the data by performing the computation m = Cd (mod n).
- Once m is derived, the user can retrieve the original data by reversing the padding scheme.

IV IMPLEMENTATION

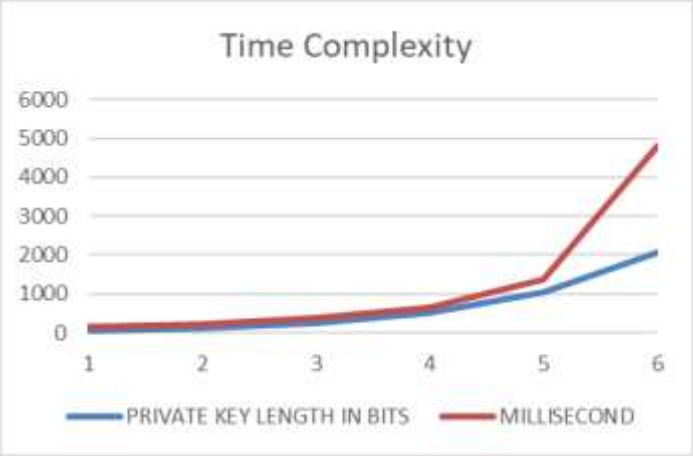
The RSA method must be implemented in this part, and its performance must be evaluated according to a number of criteria, such as throughput, space complexity, and time complexity. The results for these evaluation settings will be obtained by implementing the RSA algorithm in Java within the Eclipse IDE. The efficiency of the algorithm will be determined by analyzing its performance in terms of throughput, space complexity, and time complexity.

Time Complexity: The total number of operations the system performs, each of which requires a certain amount of time, is used to calculate the time complexity of the system. Since the performance of an algorithm might change depending on the amount of the input, time complexity is typically expressed in terms of the worst case, or T(n). An algorithm with T(n) = O(n), for instance, displays linear Time complexity is represented by T(n) = O(n^2), nonlinear complexity by T(n) = O(2^n), and exponential complexity by T(n) = O(2^n). In this instance, we determine time complexity by adjusting the RSA algorithm's Private Key length and calculating the amount of time needed to execute it.

By varying the length of the private key in bits and timing how long it takes for each key length to execute, one may evaluate the temporal complexity of RSA. An overview of the different key lengths in bits and the associated execution durations is given in Table 1.

Table 1 Time Complexity

PRIVATE KEY LENGTH IN BITS	MILLISECOND
64	85
128	90.33
256	109.33
512	141.67
1024	362.67
2048	2746.67



In addition to time complexity, space complexity is an important parameter for evaluating algorithm performance. It measures the amount of memory needed for an algorithm to function. Optimized algorithms try to use as little memory as possible.

Big O notation is commonly used to characterize space complexity. It indicates how the amount of memory needed increases with issue size. For instance, O(N^2) suggests that four times as much memory would be required if the issue size (n) doubles. We have looked at the link between the runtime memory usage of the system and the length of the private key in bits. The private key lengths in bits and the associated system memory consumption are compiled in Table 2.

Table 2 Space Complexity

Private Key Length Bits	Run Time Memory
128	345128
256	347224
512	347320
1024	348040
2048	348608
4096	349488
8192	351048

In communication systems, throughput is the rate at which data is delivered successfully over a noisy channel; it is commonly expressed in bits per second or packets per second. Higher throughput indicates more system efficiency. Throughput is calculated by dividing the total data in bytes by the encryption time. Throughput and message signal are compared for message sizes of 32, 64, 128 and 256 bytes in the accompanying table. To create an avalanche effect in cryptographic algorithms, it is essential to comprehend input and output sizes. Table 3 with different data lengths illustrates how security against brute-force attacks is improved by a greater ciphertext size relative to plaintext.

Table 3: Throughput

	Throughput for different Private Key Length				
Data Bits	128 bits key length	256 bits key length	512 bits key length	1024 bits key length	2048 bits key length
32	205.13	186.04	136.75	102.56	48.854
64	457.14	372.09	256	205.13	71.99
128	914.28	684.49	514.056	315.27	182.33
256	1641.02	1361.70	1094.02	684.49	443.67

V CONCLUSION

A developing idea, multi-cloud computing provides on-demand computing services. A corporation loses control over its data when it moves to the cloud, therefore security measures must be as high-value as the data. Multi-Cloud security is based on encryption and trusted computing.

Our suggested method prevents unauthorized intruders from decrypting collected data by limiting

data access to authorized users only. We evaluated the performance taking throughput, time complexity, and space complexity into account. Through the analysis of several factors, including the length of the private key and the message packet, we were able to conclude that the RSA encryption technique is a workable option for secure communication in cloud computing.

REFERENCES

[1] Than MyoZaw Min Thant S. V. Bezzateev"Database Security with AES Encryption, Elliptic Curve Encryption and Signature 2019 Wave Electronics and its Application in Information and Telecommunication Systems", (WECONF) Year: 2019 ISBN: 978-1-7281-2288-5 DOI: 10.1109/IEEESaintPetersburg, Russia, Russia.

[2] Feng Sheng Wu "Research of Cloud Platform Data Encryption Technology Based on ECC Algorithm", 2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)Year: 2018 ISBN: 978-1-5386-8031-5 DOI: 10.1109/IEEEChangsha, China.

[3] ShrutiBhawsar and Kushal Joshi, "A Review on Clouds Security Based Encryption and Decryption Techniques", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 10 Issue 02, February-2021.

[4] Kushala M V and Dr. B S Shylaja, " Recent Trends on Security Issues in Multi-Cloud Computing: A Survey", IEEE International Conference on Smart Electronics and Communication (ICOSEC), DOI: 10.1109/ICOSEC49089.2020.9215303.

[5] Dr. Mohammad V. Malakooti, NilofarMansourzadeh, "A Robust Information Security Model for Cloud Computing Based on the Scrambling Algorithm and Multi-Level Encryption", Proceedings of the International conference on Computing Technology and Information Management, Dubai, UAE, 2014, Islamic Azad University, UAE branch, Dubai, UAE.

[6] Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[7] Yang Xu, Lei Wu, LiyingGuo, Zheng Chen, Lai Yang, Zhongzhi Shi, "An Intelligent Load Balancing Algorithm Towards Efficient Cloud Computing", AI. for Data Center Management and Cloud Computing: Papers from the 2011 AAAI Workshop (WS-11-08).

[8] EmanM.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby, "Enhanced Data Security Model for Cloud Computing", the 8th International Conference on Informatics and Systems (INFOS2012) 16 May, Cloud and Mobile Computing Track.

[9] Neha Tirthani, Ganesan R, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography", School of computing Science and Engineering, VIT, Chennai campus.

[10] VeerrajuGampala, SrilakshmiInuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[11] Li Dongjiang, Wang Yandan, Chen Hong, "The research on key generation in RSA public- key cryptosystem", Department of Computer Science, North China Electric Power University, Beijing, China, Fourth International Conference on Computational and Information Sciences 2012.

[12] Ahmed E. Youssef, Manal Alageel, "A Framework for Secure Cloud Computing", Dept. of Information Systems, King Saud University, Riyadh, 11543, KSA.

[13] Peiyun Zhang, Senior Member, IEEE, MengChu Zhou, "An Intelligent Optimization Method for Optimal Virtual Machine Allocation in Cloud Data Centers" VOL. 17, NO. 4, OCTOBER 2020.

[14] Z. A. Mann, "Allocation of virtual machines in cloud data centers—A survey of problem models and optimization algorithms," ACM Comput. Surv., vol. 48, no. 1, pp. 1–28, Aug. 2015.

[15] P. Zhang and M. Zhou, "Dynamic cloud task scheduling based on a two-stage strategy," IEEE Trans. Autom. Sci. Eng., vol. 15, no. 2, pp. 772–783, Apr. 2018.