IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of
Information Technology & Computer Engineering

ISSN 2347–3657

Volume 9, Issue 2, 2021

https://doi.org/10.62647/ijitce.2021.v9.i2.pp11-22

Improving Cloud Computing Data Security with the RSA Algorithm

Akhil Raj Gaius Yallamelli,
DevOps Engineer
Pixar Cloud Inc – Newark, DE.
Email ID: akhilyallamelli939@gmail.com

ABSTRACT

The handling, analysis, and access of data by enterprises has been completely transformed by cloud computing, which provides many benefits. But it also poses serious security risks, especially when it comes to data protection, confidentiality, integrity, availability, and location. Strong security measures are crucial to addressing these issues and guaranteeing the dependability of cloud services. The RSA (Rivest-Shamir-Adleman) algorithm is one useful tool for improving data security in cloud computing settings. By using prime factorization complexity for both encryption and decryption, the popular asymmetric cryptographic technique RSA provides secure communication on erratic networks. A vital component of cryptography, RSA was created in 1977 and improves digital privacy, integrity, and authenticity by doing away with the requirement for shared secret keys. Its adaptability may be seen in a number of digital applications, such as internet connection security protocols and email security. Cryptographic libraries like OpenSSL and Bouncy Castle, which provide key generation, encryption, decryption, and digital signature verification features, are necessary for the implementation of RSA encryption in cloud computing. Working together, researchers, cloud providers, and cybersecurity specialists can create RSA-based security solutions that are specifically designed for cloud environments. Data security is further strengthened by major cloud providers like Microsoft Azure and Amazon Web Services including RSA encryption capabilities. Encouraging cloud computing providers to handle, transfer, and store data securely is the main goal of RSA integration. RSA encryption improves total data security and dependability in cloud environments by guaranteeing data confidentiality, integrity, and availability. For RSA implementation to be optimized and regulatory standards compliance to be ensured, more research and development is necessary due to persistent issues including scalability and effective key management.

Keywords: Cloud Computing, RSA Algorithm, Data Security, Encryption, Decryption, Key Management, GDPR, HIPAA, PCI DSS, Asymmetric Cryptography, Redundancy, Public Key, Private Key.

1. INTRODUCTION

Businesses now store, analyze, and access data in a completely new way thanks to cloud computing. Nevertheless, serious security issues, particularly with regard to data privacy, confidentiality, integrity, availability, and location, come along with cloud computing's

advantages. Given these difficulties, it is critical to have strong security measures in place to guarantee the reliability of cloud services. Using the RSA (Rivest-Shamir-Adleman) algorithm is one such method for improving data security in cloud computing settings.
One popular asymmetric cryptographic algorithm that helps with safe communication over unreliable channels is the RSA algorithm. Confidentiality, integrity, and authentication are provided via the encryption and decryption operations, which rely on the mathematical complexity of prime factorization. When it comes to cloud computing, RSA encryption can be quite helpful in protecting data that is sent to and stored on the cloud.

Developed in 1977 by Rivest, Shamir, and Adleman, the RSA algorithm is a keystone of cryptography that brought public-key encryption. By eliminating the need for a shared secret key, this innovation improves digital privacy and integrity and enables safe communication. The fact that RSA is so widely used in digital environments—from email security to digital signatures and internet connection security via SSL/TLS protocols—demonstrates how versatile this technology is. Its resistance to cryptographic assaults and versatility across platforms and applications are the main reasons for its continued significance. Overall, RSA's influence extends beyond the period of its creation, acting as a cornerstone for contemporary encryption methods and influencing the state of secure communication in the digital era.

Cryptographic libraries and frameworks are frequently needed when implementing the RSA algorithm for data security in cloud computing environments. OpenSSL, Bouncy Castle, and the Cryptography API libraries for programming languages like Python and Java are well-liked options. These technologies offer key generation, encryption, decryption, and digital signature verification—all crucial functions for RSA operations. Cloud service providers and consumers can guarantee strong encryption procedures and protect sensitive data from manipulation or illegal access by utilizing these software solutions. These libraries' accessibility also makes it easier to include RSA encryption into cloud-based applications, encouraging safe communication and data security in dispersed computing settings.

Researchers, cloud service providers, and cybersecurity experts work together to use RSA encryption to improve data security in cloud computing environments. RSA-based security solutions customized for cloud settings are developed and implemented with assistance from academic institutions, research groups, and industry specialists. To improve data security for their clients, cloud service providers—such as well-known firms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)—integrate RSA encryption capabilities into their cloud infrastructure.

The principal aim of integrating the RSA algorithm into cloud computing is to address the security issues that arise from handling, transferring, and storing confidential information in cloud settings. By ensuring that data is only available to authorized users, RSA encryption helps to improve data

https://doi.org/10.62647/ijitce.2021.v9.i2.pp11-22

confidentiality and lowers the likelihood of both illegal access and data breaches. Furthermore, data integrity is checked using RSA digital signatures and hash functions, which also help to detect any illegal changes or tampering and preserve the reliability of data stored in the cloud. Additionally, to increase data availability and guard against downtime, data loss, and service interruptions, RSA-based security measures are used. This improves overall data security and reliability in cloud computing environments by guaranteeing continuous access to cloud services and resources.

Even though RSA encryption has been extensively studied for data security in cloud computing, there are still several issues that need to be resolved. Scalability is a crucial component, since many RSA implementations now in use may not be able to handle the demands of massive cloud systems and huge data transaction volumes. Research is required to create scalable RSA-based systems that can satisfy the performance demands of contemporary cloud infrastructures. Furthermore, preserving data security in the cloud depends on effective and safe key management. To reduce key-related risks and vulnerabilities, more study on key generation, distribution, rotation, and revocation is required. Furthermore, adherence to legal mandates like GDPR, HIPAA, and PCI DSS is crucial. To guarantee data security and privacy in cloud environments, more investigation is required to make sure that RSA-based security solutions comply with these standards.

Problem Statement: Even with improvements in RSA encryption methods for cloud computing, there are still several obstacles to overcome to guarantee complete data security. One such issue is restricted scalability, which can cause performance bottlenecks in large-scale cloud systems where current RSA implementations may not be able to meet the scaling requirements. Furthermore, cloud systems provide challenges for safely and effectively maintaining RSA keys, especially when it comes to key generation, distribution, and revocation. Furthermore, RSA-based security systems implemented in the cloud have continued issues in maintaining compliance with industry standards and regulatory requirements. This necessitates constant monitoring and adherence to data protection legislation. To overcome these obstacles and enable the efficient implementation of RSA encryption to support data security in cloud computing, more research and development work is needed to improve scalability, optimize key management procedures, and guarantee adherence to data protection laws.

2. LITERATURE REVIEW

For cloud computing digital signatures, Somani et al. (2010) recommend using RSA encryption to improve data security. They emphasize the use of digital signatures as a means of authenticating documents and tackle the emerging challenges associated with cloud environments by concentrating on cryptographic solutions to ensure data integrity. They provide an effective way to reduce security threats in their suggestion.

https://doi.org/10.62647/ijitce.2021.v9.i2.pp11-22

An Enhanced RSA technique with changeable key sizes to improve encryption strength and flexibility is presented by Amalarethinam and Leena (2017) for cloud data security. Designed to meet the dynamic dangers and scalability requirements of cloud computing, it uses cutting-edge cryptography to guarantee strong data protection. In addition to highlighting the need of adaptable encryption techniques in cloud security policies, their idea provides a workable way to reduce security concerns.

Lenka and Nayak (2014) suggest integrating the MD5 algorithm with RSA encryption to improve data security in cloud computing. The goal of this integration is to improve the integrity and confidentiality of data that is transferred and stored in cloud settings. Through the use of asymmetric key cryptography, RSA encryption guarantees secure data transmission and storage, and the MD5 algorithm makes data integrity testing easier by generating message digests. Their method offers a workable alternative to reduce vulnerabilities and protect sensitive data in cloud-based systems, addressing growing concerns about security threats in cloud computing.

The use of the RSA method to strengthen data security in cloud computing systems is examined by Singh et al. (2016). Their research explores how RSA may improve security, with an emphasis on exploiting asymmetric encryption to transmit and store data securely. They examine RSA's suitability for resolving security issues in cloud contexts and highlight its cryptographic power in maintaining the secrecy and integrity of cloud-based data. The study highlights the significance of strong encryption techniques in protecting sensitive data in the cloud and provides workable implementation solutions for RSA encryption into cloud security frameworks.

In order to improve data security in cloud computing environments, Kaur and Singh (2013) explore the application of encryption algorithms. Their research looks at different algorithms such as AES, RSA, and others, with the goal of using cryptographic approaches to protect sensitive data on the cloud. They go over data encryption, data encryption key management, and decryption procedures while taking compatibility, scalability, and performance into account when choosing an algorithm. Effective methods for incorporating encryption algorithms into cloud security frameworks are provided in order to reduce the risks associated with data security.

Kumar and Shafi (2020) present a secure and effective cloud computing data storage solution via a modified RSA public key cryptosystem. Through the use of RSA encryption for safe data transfer and storage, their method seeks to improve the effectiveness and security of data storage systems. They talk about how the RSA algorithm can be changed to meet the unique needs of cloud computing environments and assess how well the suggested fix reduces the risks associated with data security. Furthermore, useful implementation techniques for incorporating the altered RSA cryptosystem into cloud storage infrastructures are offered.

AbdElminaam (2018) suggest creating new hybrid cryptography techniques to improve cloud computing security. Their work presents new hybrid cryptography algorithms designed to improve cloud security by fusing the best features of various cryptographic approaches to tackle security issues unique to clouds. In order to guarantee the privacy and accuracy of data stored in the cloud, they investigate hybrid encryption techniques that take key management and algorithmic performance into account. In addition to offering useful implementation methodologies for incorporating hybrid cryptography algorithms into cloud security frameworks, the study addresses the possible influence of hybrid cryptography on reducing data security concerns in cloud computing.

Gupta et al. (2018) suggest augmenting the RSA method by utilizing a multi-threading approach to strengthen data security in cloud storage that is outsourced. Their work presents a multi-threading paradigm designed to maximize parallel processing for RSA encryption and decryption processes. They investigate multi-threaded techniques that take concurrency and key management into account while designing algorithms to increase performance and scalability in cloud systems. In addition to offering useful implementation solutions for incorporating the multi-threading model into cloud storage designs, the study addresses the possible effects of multi-threading on reducing data security threats in cloud storage.

Hyseni et al. (2018) present a new approach designed to improve sensitive data security in cloud computing settings. Their suggested methodology focuses on resolving vulnerabilities and reducing risks related to data breaches and unauthorized access in order to improve security for processed and stored sensitive data in the cloud. They examine cutting-edge encryption methods, access restrictions, and data security measures while taking industry best practices for model design and regulatory compliance into account. The study explores how the suggested approach may protect sensitive data in cloud environments and offers workable deployment techniques to successfully improve cloud security.

RSA encryption and steganography techniques are included in Pant et al. (2015) thorough three-step data security paradigm for cloud computing. Their methodology integrates strong data encryption and decryption procedures using RSA encryption, specifically designed to improve security in cloud situations. Furthermore, data is hidden in digital media through the use of steganography techniques, which improves confidentiality. In addition to examining realistic deployment scenarios and implementation tactics, the study addresses the model's efficacy in protecting sensitive data from cyber attacks and illegal access. Moreover, utilizing the suggested paradigm to further improve data security in cloud computing, future research topics and possible obstacles are investigated.

To improve data secrecy in cloud computing contexts, El Makkaoui et al. (2017) suggest a quick cloud-RSA system. To enhance performance in cloud environments without sacrificing security, their innovative plan focuses on streamlining the RSA encryption and decryption procedures. We examine methods for effectively speeding up RSA operations. The study examines feasible deployment scenarios and execution methodologies, as well as the possible advantages of the fast cloud-RSA scheme in reducing cloud-based data security threats. Additionally, the usefulness and efficiency of the method in increasing data confidentiality in cloud computing environments is evaluated.

RSA encryption and hash functions are integrated by Garg and Sharma (2014) to provide an effective and safe data storage solution for Mobile Cloud Computing (MCC) environments. Their method is centered on using RSA encryption to guarantee data security both during transmission and storage in the cloud. Hashing functions are also used to protect against manipulation and verify data integrity. The study takes into account the resource limitations and performance optimizations specific to mobile devices while discussing the efficiency and security advantages of integrating RSA and hash functions in MCC. Moreover, deployment issues and realistic implementation methodologies for the suggested solution in MCC contexts are discussed.

3. METHODOLOGY

3.1. Data Encryption Using RSA

An asymmetric cryptographic technique called RSA (Rivest-Shamir-Adleman) is frequently used for safe data transfer. It ensures that data can be securely transferred across an unsecure channel by using two keys: a private key for decryption and a public key for encryption. The following outlines the procedures for utilizing RSA encryption in cloud computing settings.

Key Generation

i. Creating a prime number involves producing two big numbers, p and q.

ii. Compute *n*: calculate *n* as the outcome of p and $q(n = p * q)$.

iii. Calculate Totient function $\emptyset(n)$: compute $\emptyset(n)$ as $(p - 1) * (q - 1)$.

iv. Choose public exponent *e*: select an integer e such that $1 < e < \emptyset(n)$ and $gcd\, gcd\, (e, \emptyset(n)) \ = 1$.

v. Find the private exponent *d:* calculate *d* as the inverse modular multiplicative of e modulo $\emptyset(n)$ $(d \equiv e^{-1}\, mod\, \emptyset(n))$.

Encryption Process

i. Message Conversion: Change the message *M* from plaintext to an integer m so that $0 \leq m \leq n$.

ii. Ciphertext Calculation: Use the public key *(e, n)* to calculate the ciphertext *c:* $c = m^e \, mod\, n$.

Decryption Process

i. Recover Original Message: With the private key *(d,n),* compute the original message m: $m = c^d \mod n$.
ii. Convert to Plaintext: Return the integer m to the message M in plaintext.

3.2. Implementation in Cloud Computing

Integrating encryption and decryption procedures into cloud service providers' data handling protocols is necessary to implement RSA in cloud computing settings. This guarantees the preservation of data security in the cloud during its entire lifecycle.

Data Upload

Transmission and encryption are the two essential phases in the upload of data. To guarantee that only individuals with permission can access the client's data, it is first encrypted using their public key. The data is transformed via this encryption process into a safe format that is difficult for unauthorized parties to read. Second, the encrypted data is transferred across the internet to cloud storage. This guarantees the data's protection throughout the upload procedure, preventing any possible interception or unwanted access while it's in transit.

Data Storage

Redundancy and integrity checks are two essential procedures for cloud data storage. First, in order to offer redundancy and high availability, cloud services keep encrypted data across several servers. This implies that even if one server fails, other servers can still access the data. Second, to ensure that the data hasn't been altered, routine integrity checks are carried out. By identifying and resolving any irregularities or unauthorized modifications, these checks aid in maintaining the dependability and security of the data that has been saved.

Data Access

Downloading and decrypting are the two primary processes in data access. The client first performs a download to obtain the encrypted data from the cloud storage. The data is then returned to its original, readable state by the client using their private key to decrypt it. This decryption process makes sure that only authorized users can safely access and use the data because only those who have the matching private key can decrypt the encrypted data.

3.3. Key Management

Effective key management is essential in the cloud computing environment to guarantee the security of data encrypted with the Rivest-Shamir-Adleman (RSA) algorithms. This includes a number of crucial procedures that are designed to maintain the secrecy and integrity of encrypted data, including key creation, distribution, storage, rotation, and revocation.

Key generation is the process of employing safe libraries to create cryptographic keys. These libraries ensure that the produced keys are long enough and complicated enough to resist possible assaults, which means strong security.

The safe distribution of public keys to those who are allowed is known as key distribution. In the meantime, private keys are safely stored on the client side and need to be kept private. The best practice is to keep them in hardware security modules (HSMs), which provide increased defense against unwanted access attempts.

One preventive strategy to lessen the hazards of key compromise is key rotation. New key pairs must be created on a regular basis, and authorized parties must get the updated public keys securely. In order to maintain data privacy, the matching private keys on the client side are changed securely at the same time to match the new key pairs.

Mechanisms for revocation of keys are essential for invalidating compromised or out-of-date keys. This guarantees that sensitive data cannot be decrypted using compromised keys, protecting the integrity and confidentiality of the encrypted data. These kinds of procedures are necessary to keep up a strong security posture in cloud environments where safeguarding data is critical.

3.4. Scalability and Performance Optimization

Load balancing is facilitated by dividing up the work of encryption and decryption among several servers. By distributing the workload evenly among the available resources, this method avoids bottlenecks. This keeps no single server overloaded and improves system performance as a whole.

Parallel Processing: Handling massive volumes of data efficiently is made possible by utilizing parallel processing techniques. Parallel processing promotes optimal resource utilization and minimizes processing time by concurrently executing encryption and decryption processes across multiple cores or servers. By using this method, encryption and decryption operations are kept from becoming a performance snag, especially when working with large datasets.

Resource Allocation: To ensure peak performance, dynamic computing resource allocation based on demand is essential. Cloud settings are able to guarantee the effective operation of encryption and decryption operations by keeping an eye on workload fluctuations and modifying resource allocation accordingly. The system may scale resources up or down as needed thanks to this adaptive resource allocation technique, which maximizes performance without wasting any resources.

3.5. Compliance with Regulatory Standards

To preserve data security and privacy, it is crucial to make sure that RSA-based security implementations in the cloud adhere to industry standards and legal obligations like GDPR, HIPAA, and PCI DSS.

Sustaining strong security in cloud systems requires constant monitoring. This entails routinely evaluating security procedures to guarantee adherence to legal requirements and identify any potential weaknesses that can jeopardize data integrity.

Ensuring adherence to regulatory mandates is largely dependent on reporting and auditing. Audits are carried out on a regular basis to assess key management procedures, encryption and decryption methods, and instances of compromised keys or data breaches. Subsequently, comprehensive reports are produced to exhibit compliance with regulatory guidelines and to furnish transparency concerning the security protocols put in place.

Initiatives to raise awareness and provide training are essential for encouraging a security-conscious culture among cloud service providers and customers. Organizations can improve their comprehension of data security best practices by offering thorough training sessions and educating people about the need of adhering to regulatory standards. This gives businesses the ability to apply and manage security procedures in an efficient manner, lowering the possibility of data breaches and guaranteeing the integrity and confidentiality of private data kept on cloud servers.

The cloud computing environment's implementation of an RSA-based encryption system is depicted in the high-level architecture diagram below.

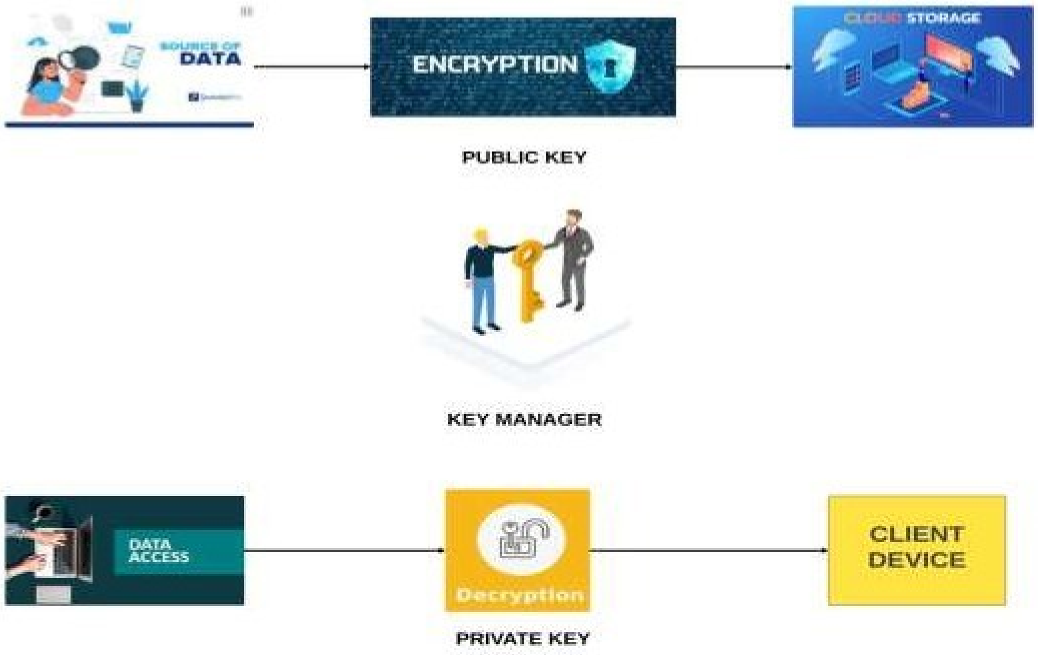

Figure 1: Architecture for Secure Data Transmission and Storage.

Figure 1 presents the Architecture for Secure Data Transmission and Storage, outlining a comprehensive system to ensure data security in cloud computing environments. The architecture starts with the Data Source, representing the origin of the data, which must be encrypted before being transferred to the cloud. This data source can be any device owned by the user, a local server, or any other data-generating entity. Before transfer, data is encrypted using the client's public key, ensuring its security during transmission and storage in the cloud. Encrypted data is then hosted on multiple cloud servers to provide redundancy and availability, with regular integrity checks to ensure data remains intact.

The Key Manager is responsible for the creation, distribution, storage, rotation, and revocation of keys. Private keys are securely stored on the client side, while public keys are distributed to authorized parties. The key manager enhances security through regular key rotation and key revocation procedures. When a client needs access to the data, the encrypted data is downloaded from the cloud storage. The client then uses their private key to decrypt the downloaded data, recovering the original plaintext information. The Client Device, which refers to the device or system the client uses to access and decrypt the data, ensures that only authorized users can decrypt the data because the private key is securely stored on this device.

https://doi.org/10.62647/ijitce.2021.v9.i2.pp11-22

This architecture uses RSA-based encryption to significantly improve data security in cloud computing environments. It ensures that data remains private, integral, and accessible only to authorized users. The scalability and performance optimization strategies, combined with key management procedures, ensure that the RSA implementation is robust and efficient, meeting the demands of modern cloud infrastructures and adhering to legal requirements.

4. RESULT AND DISCUSSION

Data security and privacy are greatly improved in cloud computing when RSA-based encryption is used. It ensures that only authorized users can access data by securely transferring it via insecure channels using asymmetric encryption techniques like RSA. RSA encryption is based on key generation, which is the process of generating prime numbers and determining public and private keys. Security is maintained throughout the data lifecycle in cloud computing by integrating RSA encryption into data handling methods. Overall security is improved by access protocols, redundancy checks in storage, and encryption during upload. Scalability, performance optimization techniques, and efficient key management procedures are essential. Adherence to regulatory guidelines such as GDPR, HIPAA, and PCI DSS necessitates periodic audits. In cloud contexts, RSA-based encryption provides a dependable means of protecting sensitive data, satisfying the needs of contemporary cloud architecture, and abiding with legislation.

5. CONCLUSION

In summary, there are strong solutions available to handle security issues including data privacy, integrity, and availability when the RSA algorithm is used in cloud computing environments. Cloud service providers can guarantee safe data storage and transmission while abiding by legal requirements by putting RSA encryption into practice. The reliability and efficacy of RSA implementation in cloud infrastructures are further improved by efficient key management procedures in conjunction with scalability and performance optimization techniques. To advance the security and dependability of cloud computing systems, it is imperative that research and development activities be continued in order to solve current problems, enhance scalability, optimize key management, and guarantee compliance with changing data protection legislation. In the future, post-quantum cryptography methods might be investigated to fortify RSA-based encryption against new dangers. Furthermore, improving security posture and adaptability in cloud environments can be achieved by incorporating machine learning algorithms for anomaly detection and dynamic key management.

7. REFERENCE

1. Somani, U., Lakhani, K., & Mundra, M. (2010, October). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing.

In 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010) (pp. 211-216). Ieee.

2. Amalarethinam, I. G., & Leena, H. M. (2017, February). Enhanced RSA algorithm with varying key sizes for data security in cloud. In 2017 World Congress on Computing and Communication Technologies (WCCCT) (pp. 172-175). IEEE.
3. Lenka, S. R., & Nayak, B. (2014). Enhancing data security in cloud computing using RSA encryption and MD5 algorithm. International Journal of Computer Science Trends and Technology, 2(3), 60-64.
4. Singh, S. K., Manjhi, P. K., & Tiwari, R. K. (2016). Data security using RSA algorithm in cloud computing. International Journal of Advanced Research in Computer and Communication Engineering, 5(8), 11-16.
5. Kaur, M., & Singh, R. (2013). Implementing encryption algorithms to enhance data security of cloud in cloud computing. International Journal of Computer Applications, 70(18).
6. Kumar, Y. K., & Shafi, R. M. (2020). An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem. International Journal of Electrical and Computer Engineering, 10(1), 530.
7. AbdElminaam, D. S. (2018). Improving the security of cloud computing by building new hybrid cryptography algorithms. International Journal of Electronics and Information Engineering, 8(1), 40-48.
8. Gupta, P., Verma, D. K., & Singh, A. K. (2018, January). Improving RSA algorithm using multi-threading model for outsourced data security in cloud storage. In 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 14-15). IEEE.
9. Hyseni, D., Luma, A., Selimi, B., & Cico, B. (2018). The proposed model to increase security of sensitive data in cloud computing. Int. J. Adv. Comput. Sci. Appl, 9(2), 203-210.
10. Pant, V. K., Prakash, J., & Asthana, A. (2015, October). Three step data security model for cloud computing based on RSA and steganography. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 490-494). IEEE.
11. El Makkaoui, K., Beni-Hssane, A., Ezzati, A., & El-Ansari, A. (2017). Fast cloud-RSA scheme for promoting data confidentiality in the cloud computing. Procedia computer science, 113, 33-40.
12. Garg, P., & Sharma, V. (2014, February). An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function. In 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) (pp. 334-339). IEEE.