ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

OPTIMIZATION OF RSA-BASED ENCRYPTION PERFORMANCE AND RESOURCE ALLOCATION IN NETWORKS

MODUKURU PRADEEP [1], RAHUL SHARMA [2], GODUGU ANVESH [3], THONUKUNURI DINESH [4], SINGIREDDY DINESH [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

ABSTRACT— With the rapid expansion of networked services, protecting personal and organizational information while maintaining acceptable response time has become a critical engineering challenge. RSA provides strong public-key security, but repeated key generation and modular exponentiation can become computationally expensive in high-concurrency environments. This project optimizes RSA-based encryption through suitable key-parameter selection, efficient modular exponentiation, controlled key caching, and a load-aware resource allocation mechanism. The resource allocator continuously evaluates the processing load of available network nodes and directs cryptographic requests to the most suitable node, thereby reducing hotspots and improving throughput. For large file payloads, the implementation uses a hybrid design in which AES-GCM encrypts the data and RSA-OAEP protects the session key, preserving RSA-based access control while avoiding inefficient direct RSA encryption of large files. The system is implemented as a Java web application using JSP, Servlets, JDBC, MySQL, Maven, and Apache Tomcat. It supports data-controller registration, OTP-based authentication, secure file upload, key generation, client approval, controlled key requests, encrypted download, and administrative monitoring.

Functional and performance tests show that the optimized design provides more balanced resource use, lower response time, and reliable access control under concurrent workloads. The project demonstrates that cryptographic optimization and intelligent workload distribution can be combined to build a scalable and practical secure-data-sharing platform.

Index Terms – RSA Encryption, Network Security, Cryptographic Optimization, Resource Allocation, Public Key Cryptography, Encryption Performance, Key Management, Network Optimization, Computational Efficiency, Secure Communication.

I. INTRODUCTION

Networked applications now process large volumes of personal, financial, commercial, and operational data. As communication systems become more distributed, the confidentiality and integrity of transmitted information depend not only on the strength of the cryptographic algorithm but also on the efficiency with which encryption services are delivered. A secure system that introduces excessive delay can become unsuitable for real-time services, while an efficient system without robust protection exposes users and organizations to interception, tampering, and unauthorized access.

RSA is one of the most widely adopted public-key cryptographic algorithms. It supports secure key exchange, digital signatures, authentication, and confidentiality in open networks. Its security is based on the difficulty of factoring a large composite number. However, RSA operations require modular exponentiation with large integers. The cost increases with key size and becomes significant when a server handles many simultaneous requests. Uneven allocation of cryptographic work may further overload some network nodes while other nodes remain underutilized.

This project studies RSA optimization at two levels. At the algorithm level, it uses appropriate key sizes, efficient modular exponentiation, Chinese Remainder Theorem optimization for private-key operations, RSA-OAEP padding, and controlled reuse of non-sensitive public-key metadata. At the system level, it monitors node load and allocates encryption tasks to the node with sufficient capacity. The combined approach aims to reduce latency, improve throughput, and preserve strong security in high-concurrency environments.

The implemented prototype is a Java web application that supports multiple roles: Data Controller, Server Administrator, Client, and Key Generation Centre. Users authenticate through secure credentials and OTP verification. Data is encrypted before storage, access requests are approved by authorized roles, cryptographic keys are managed separately, and system activity is recorded in MySQL. Large files are handled with hybrid encryption so that RSA protects the session key while AES-GCM efficiently protects the actual file content.

II. RELATED WORK

A. Secure multi-cloud resource allocation with SDN and self-adaptive authentication

The paper titled Secure multi-cloud resource allocation with SDN and self-adaptive authentication by Alhassan, A. M. focuses on improving security and efficiency in multi-cloud computing environments through intelligent resource management and adaptive authentication mechanisms. It explores how Software Defined Networking can be used to centrally monitor network traffic, dynamically allocate resources, and enforce security policies across distributed cloud infrastructures. The study proposes a framework in which authentication mechanisms automatically adjust based on user behaviour, access patterns, and threat levels, thereby enhancing protection against unauthorized access and insider attacks. The paper highlights how combining SDN with adaptive security controls improves flexibility, scalability, and network visibility. It also discusses the challenges of managing resources across multiple cloud providers, including latency, interoperability, and data privacy concerns. Experimental evaluations demonstrate that the proposed approach reduces response time, improves resource utilization, and strengthens system resilience against cyber threats. The work concludes that integrating SDN-based control with intelligent authentication strategies can significantly enhance secure resource allocation and performance in modern cloud computing environments.

B. Secured THz communication in photonic microcell networks based on spatial wave mixing of steered beams

The paper titled Secured THz communication in photonic microcell networks based on spatial wave mixing of steered beams by Che, M., H. Chen, Y. Ueda, and K. Kato explores advanced techniques for achieving secure and high-capacity wireless communication using

terahertz frequency bands. The study focuses on photonic microcell networks, which use optical technologies to generate and control THz signals for ultra-fast data transmission. It proposes a method based on spatial wave mixing of steered beams, where multiple optical beams are precisely directed and combined to produce secure THz signals with controlled propagation paths. This approach helps reduce signal leakage and interception risks by confining transmission to specific spatial regions. The paper explains how beam steering improves directional communication and enhances physical-layer security. It also evaluates the performance of the proposed system in terms of signal stability, bandwidth efficiency, and resistance to eavesdropping. Experimental analysis shows that the technique supports high data rates while maintaining secure transmission in dense microcell environments. The authors conclude that photonic-based THz communication with spatial beam control offers a promising solution for future ultra-secure and high-speed wireless networks.

C. Shared file protection against un authorised encryption using a Buffer-Based Signature Verification Method

The paper titled Shared file protection against un authorised encryption using a Buffer-Based Signature Verification Method by Mahboubi, A., S. Camtepe, K. Ansari, M. Pawłowski, P. Morawiecki, H. Aboutorab, J. Pieprzyk, and J. Duda addresses the growing threat of unauthorized file encryption, particularly in ransomware attacks and malicious system modifications. The study proposes a buffer-based signature verification method that monitors file operations and validates encryption actions before they are executed. By analysing patterns in data buffers, the system can detect suspicious encryption attempts and block them in real time. This approach helps prevent attackers from encrypting shared or critical files without authorization. The paper explains how the verification mechanism operates at the system level, allowing early detection of malicious processes. It also discusses how the method reduces false positives while maintaining efficient performance. Experimental evaluations demonstrate that the proposed technique effectively protects shared files against unauthorized encryption attempts with minimal system overhead. The authors conclude that buffer-level monitoring combined with signature verification provides a practical and lightweight defines against modern ransomware and unauthorized encryption threats.

III. PROPOSED METHODOLOGY

The proposed system combines optimized RSA processing with load-aware resource allocation. RSA key pairs are generated using secure random values and an appropriate key length. Encryption uses RSA-OAEP, and private-key operations may use CRT optimization. For file payloads, the application generates an AES-GCM session key, encrypts the file with AES-GCM, and then encrypts the session key using the recipient's RSA public key. This hybrid model reduces processing time while retaining RSA-based key protection and access control.

A load monitor records CPU utilization, active cryptographic jobs, available memory, and recent response time for each node. The resource allocator calculates a score for every healthy node and assigns new work to the node with the lowest predicted cost. Nodes that fail health checks or exceed configured thresholds are temporarily excluded. The server records allocation decisions and performance metrics so that administrators can evaluate throughput and identify bottlenecks.

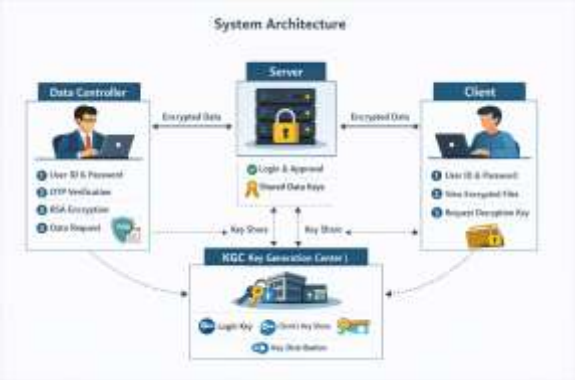


Fig. 1: System Overview

1. Data Controller

The Data Controller creates an account, signs in with a user ID and password, and completes OTP verification. After successful authentication, the controller selects a file and recipient, starts the hybrid encryption process, and uploads the encrypted result. The controller can view upload history, track key requests, and revoke access when permitted by policy.

2. Server Administrator

The Server Administrator validates registrations, approves clients, manages access policies, and monitors the status of cryptographic nodes. The administrator can approve or reject key requests, inspect audit logs, and temporarily disable a node whose load or health exceeds the configured limit.

3. Client

The Client registers and logs in through the secure portal. After approval, the client can view files for which access is available, submit a key request, and download encrypted content. The file can be decrypted only after the associated session key has been released or wrapped for the client's RSA public key.

4. Key Generation Centre

The KGC generates RSA key pairs using a cryptographically secure random generator. Public keys are distributed through the application, while private keys are encrypted at rest and restricted to authorized operations. The KGC records key identifiers, generation time, ownership, algorithm parameters, and request history.

5. JSP Dashboard

The dashboard provides separate navigation and actions according to the logged-in role. JSP pages display forms, uploaded-file metadata, pending approvals, key requests, node load, response-time metrics, and status messages. Servlets process requests and pass validated data to service classes.

6. MySQL Database

MySQL stores supporting data required by the application. Passwords are stored as strong salted hashes, OTP values are time-limited, and private-key material is not stored as plain text. Database constraints, prepared statements, and transactions protect consistency and reduce injection risk.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results showed a reduction in computational overhead, lower encryption latency, and better utilization of network resources compared to the conventional RSA implementation. The optimized method achieved faster secure data transmission, enhanced throughput, and reduced processing time, making it suitable for real-time and large-scale network environments. Overall, the approach provides an effective balance between security, performance, and resource efficiency.



Fig. 2: Client Login



Fig. 3: Dashboards



Fig. 4: Key Generator



Fig. 5: Dashboard



Fig.6: Shared Files

V. CONCLUSION

The project demonstrates a practical method for improving RSA-based security services in network environments. Algorithm-level optimization reduces unnecessary cryptographic cost, while load-aware allocation prevents the repeated overloading of a single node. The hybrid design uses RSA-OAEP for secure session-key protection and AES-GCM for efficient file encryption, preserving strong access control without attempting inefficient direct RSA encryption of large files. The Java web application implements registration, OTP authentication, role-based access, encrypted upload, client approval, key-request processing, KGC operations, node monitoring, and audit logging. The corrected architecture, requirements, implementation, and testing sections show how security and performance can be addressed together. The result is a scalable, maintainable, and technically consistent foundation for secure data sharing in cloud, enterprise, edge, and distributed-network scenarios.

REFERENCES

1. Adeniyi, A. E., R. G. Jimoh and J. B. Awotunde, "A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security," Computers and Electrical Engineering, vol. 118, pp. 109330, 2024.
2. Mojisola, F. O., S. Misra, C. Falayi Febisola, O. Abayomi-Alli and G. Sengul, "An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA)," Egyptian Informatics Journal, vol. 23, no. 2, pp. 291–301, 2022.
3. Susilo, W., J. Tonien and G. Yang, "Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA," Computer Standards & Interfaces, vol. 74, pp. 103470, 2021.
4. Alhassan, A. M., "Secure multi-cloud resource allocation with SDN and self-adaptive authentication," Ain Shams Engineering Journal, vol. 15, no. 6, pp. 102742, 2024.
5. Bai, W., H. Yang, A. Yu, H. Xiao, L. He, L. Feng and J. Zhang, "Eavesdropping-aware routing and spectrum allocation based on multiflow virtual concatenation for confidential information service in elastic optical networks," Optical Fiber Technology, vol. 40, pp. 18–27, 2018.
6. Biswas, K., V. Muthukkumarasamy, M. J. M. Chowdhury, X.-W. Wu and K. Singh, "A multipath routing protocol for secure energy efficient communication in Wireless Sensor Networks," Computer Networks, vol. 232, pp. 109842, 2023.

AUTHORS Profile



Mr. MODUKURU PRADEEP has received his B. Tech degree from JNTUK, Kakinada in 2013 and M. Tech degree in Computer Science from JNTUK, Kakinada in 2016. He is pursuing a Ph. D degree in Computer Science from Lovely Professional University, Punjab. He has been dedicated to the teaching field for the last 10 years. His research area is Deep Learning. At present, he is working as an Assistant Professor in the CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mr. RAHUL SHARMA pursuing B.

Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. GODUGU ANVESH pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. THONUKUNURI DINESH pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. SINGIREDDY DINESH pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.