International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 124-134
ISSN: 3071-3358

Enhanced Key Exchange And Lightweight Encryption For IoT Security Using Timestamp-Based OTP And Enhanced RSA

Mohammed Shoeb Ahmed[1], Dr. Mohammed Jammel Hashmi[2]
[1]PG Scholar, Department Of Computer Science & Engineering, ISL Engineering College, Hyderabad, India. India.
[2] Associate Professor & HOD-CSE; Department Of Computer Science & Engineering, ISL Engineering College, Hyderabad, India.
Corresponding Author Email: ahmedmohammedshoeb18@gmail.com

Abstract
In the modern digital environment, ensuring secure data transmission between data owners and authorized users is essential for protecting sensitive information. This paper proposes a secure data-sharing framework that integrates One-Time Password (OTP) generation with an RSA-based key exchange mechanism. Whenever a data owner initiates a data-sharing process, a unique and dynamically generated OTP is created to serve as an access credential. The OTP is encrypted using the RSA algorithm before being transmitted, ensuring that only the intended and authorized user can decrypt and use it to access the shared data. The asymmetric encryption mechanism also helps establish a secure communication channel between the data owner and the recipient, reducing the risk of unauthorized access, interception, and misuse during transmission. By combining dynamically generated OTPs with the security capabilities of RSA encryption, the proposed framework strengthens authentication, confidentiality, and data integrity. This approach provides an effective solution for secure information sharing in digital environments where reliable access control and protection against security threats are essential.

Keywords: *Data Security, Secure Data Sharing, One-Time Password (OTP), RSA Encryption, Key Exchange, Authentication, Confidentiality, Data Integrity, Access Control.*

1. Introduction

The rapid expansion of the Internet of Things (IoT) has resulted in the deployment of a large number of interconnected devices that continuously exchange information across heterogeneous communication networks. These devices support applications in healthcare, smart homes, industrial automation, transportation, agriculture, and other critical environments. However, the open and distributed nature of IoT communication introduces substantial security risks, including unauthorized access, eavesdropping, replay attacks, data interception, and compromise of sensitive information. The limited processing capability, memory, storage, and battery capacity of many IoT devices further complicates the implementation of conventional security mechanisms. Suo et al. identified security and privacy as fundamental challenges in IoT environments and emphasized the importance of secure communication, cryptographic protection, and appropriate security mechanisms for connected devices [1]. Similar concerns regarding the constrained nature of IoT devices and the need for efficient security solutions have been discussed in subsequent research [2], [3].

Cryptographic mechanisms play a central role in protecting information transmitted between IoT devices and authorized entities. Traditional encryption techniques can provide strong security, but their computational and memory requirements may not always be suitable for resource-constrained devices.

Received: *16-06-2026*
Revised: *25-07-2026*
Accepted: *17-08-2026*
Published: *20-08-2026*
Citation: *" Enhanced Key Exchange And Lightweight Encryption For IoT Security Using Timestamp-Based OTP And Enhanced RSA", ijaicn, vol. 2, no. 3, pp. 86–98, August. 2026,*

Lightweight cryptography has consequently emerged as an important research direction, with the objective of achieving an appropriate balance between security, computational complexity, memory consumption, and energy usage. Al-Aboosi et al. reviewed lightweight cryptographic approaches for resource-constrained devices and highlighted the challenges associated with implementing secure cryptographic mechanisms within devices having limited computational and energy resources [2]. These limitations demonstrate the need for security frameworks that can provide strong protection without imposing excessive computational overhead.

Authentication represents another critical component of IoT security because encryption alone cannot prevent an unauthorized entity from attempting to access protected resources. One-Time Password (OTP) mechanisms provide an additional authentication factor by generating temporary credentials that are valid for a limited period or authentication event. The HMAC-Based One-Time Password (HOTP) mechanism introduced by M'Raihi et al. generates authentication values using a shared secret and a moving counter, providing a mechanism for producing credentials that are not permanently reusable [4]. The Time-Based One-Time Password (TOTP) approach further associates the generated authentication value with time, allowing credentials to expire automatically after a defined validity interval [5].

Although OTP mechanisms can strengthen authentication, secure exchange and protection of cryptographic information remain important considerations. An OTP transmitted without adequate protection may be exposed through interception or man-in-the-middle attacks. Consequently, an asymmetric cryptographic mechanism can be incorporated to protect the exchange of sensitive authentication information. RSA is particularly relevant in this context because it provides public-key encryption and enables secure communication between parties that do not initially possess a common secret encryption key. An RSA-based exchange can therefore be combined with a temporary authentication credential to establish an additional layer of protection for IoT communication.

Lightweight encryption algorithms have also been investigated specifically for constrained IoT environments. Usman et al. proposed the SIT lightweight encryption algorithm to address the computational limitations of IoT devices while maintaining essential confidentiality and integrity properties [6]. Other lightweight cryptographic research has investigated compact algorithms and alternative cryptographic constructions intended to reduce processing and memory requirements. These developments indicate that IoT security cannot be addressed effectively through a single security mechanism; instead, authentication, key establishment, confidentiality, and integrity need to operate together within an appropriately designed framework.

Public-key cryptography can provide important benefits for secure key exchange, but its computational cost can be significant when implemented directly on highly constrained devices. Elliptic-curve-based approaches have therefore received considerable attention because they can provide strong security using comparatively smaller key sizes. Lara-Nino et al. examined lightweight elliptic-curve cryptography and highlighted its suitability for environments where computational and memory resources are restricted [7]. ECC-based authentication and signature schemes have similarly been investigated for IoT and Industrial IoT applications, demonstrating the continuing effort to achieve secure authentication without excessive resource consumption [8], [9].

The increasing complexity of IoT environments also creates a requirement for authentication mechanisms capable of resisting common attacks while maintaining practical implementation characteristics. Intelligent authentication and machine-learning-based security approaches have been investigated as complementary mechanisms for identifying anomalous behavior and improving access control. However, cryptographic authentication remains essential because it provides a direct mechanism for verifying the legitimacy of communication participants and protecting sensitive credentials.

Motivated by these challenges, this research proposes an **Enhanced Key Exchange and Lightweight Encryption Framework for IoT Security Using Timestamp-Based OTP and Enhanced RSA**. The proposed approach combines a timestamp-driven OTP mechanism with an RSA-based key exchange process to provide dynamic authentication and protected credential transmission. A timestamp is incorporated into the OTP-generation process so that each authentication attempt produces a temporary credential associated with a specific validity period. The generated OTP is then protected through the proposed RSA-based mechanism before being transmitted to the intended recipient.

The principal objective of the proposed framework is to strengthen authentication and secure key exchange while maintaining an implementation structure suitable for IoT environments. The framework is designed to reduce the security risks associated with static credentials and unprotected authentication information by combining temporary authentication values with asymmetric

cryptographic protection. The proposed approach is evaluated in terms of security, computational efficiency, authentication reliability, encryption/decryption performance, and resistance to common communication attacks.

Overall, the research aims to provide a practical security framework in which **timestamp-based OTP generation provides dynamic authentication, enhanced RSA provides secure key exchange and credential protection, and lightweight encryption provides efficient data confidentiality**. The combination of these mechanisms is intended to provide a layered security model suitable for IoT applications where authentication, confidentiality, and resource efficiency must be considered simultaneously.

2. Literature Review

2.1 IoT Security Challenges

H. Suo et al. examined the security requirements of Internet of Things environments and discussed major concerns associated with privacy, secure communication, cryptographic protection, and sensor-data security. Their work established that IoT networks require security mechanisms capable of addressing threats across different layers of the communication architecture. The study is particularly relevant to the present research because it demonstrates that conventional security mechanisms cannot always be directly transferred to constrained IoT environments without considering device capabilities and communication characteristics [1].

A. M. M. Al-Aboosi et al. investigated lightweight cryptography for resource-constrained devices and emphasized that IoT devices often operate with limited memory, processing capability, and battery power. Their review considered the security requirements of constrained environments and highlighted the need to balance cryptographic strength with implementation efficiency. The authors also identified threats such as eavesdropping, replay attacks, and man-in-the-middle attacks, which are directly relevant to secure IoT communication [2].

S. Misra et al. examined security challenges and approaches associated with IoT systems, emphasizing the importance of authentication, confidentiality, integrity, and secure communication. Their work illustrates that the large-scale interconnection of heterogeneous devices expands the attack surface and requires coordinated security mechanisms. These observations support the development of multilayered frameworks that combine authentication with cryptographic protection rather than depending on a single security mechanism [3].

2.2 Lightweight Cryptography for IoT

I. K. Dutta et al. investigated lightweight cryptography in the context of insecure and resource-constrained IoT environments. Their work highlighted the limitations of directly applying conventional cryptographic mechanisms to low-power devices and emphasized the importance of reducing computational and memory requirements. Lightweight cryptographic techniques can therefore provide an appropriate foundation for protecting IoT data while considering the hardware limitations of connected devices [10].

P. Shah et al. examined lightweight cryptographic algorithms for IoT and emphasized the importance of selecting cryptographic mechanisms according to the computational and energy limitations of the target device. Their study reinforces the need for security mechanisms that maintain an acceptable level of protection without introducing excessive processing overhead. Such considerations are important when designing the encryption component of the proposed framework [11].

N. A. Gunathilake et al. studied developments in lightweight cryptography for IoT security and discussed the evolution of cryptographic approaches designed for constrained environments. Their work demonstrates that security algorithms for IoT must be evaluated not only according to cryptographic strength but also according to implementation cost, energy consumption, memory utilization, and execution performance. These factors are relevant to the lightweight encryption component of the proposed framework [12].

2.3 OTP-Based Authentication

D. M'Raihi et al. introduced the HMAC-Based One-Time Password algorithm, commonly known as HOTP, which generates temporary authentication values using a shared secret and an incrementing counter. The algorithm was designed to provide interoperable one-time authentication and includes mechanisms for counter synchronization and protection against repeated authentication attempts. HOTP provides the conceptual foundation for dynamic authentication systems in which credentials are not permanently reusable [4].

D. M'Raihi et al. subsequently introduced the Time-Based One-Time Password algorithm, TOTP, which derives temporary authentication values from a shared secret and a time-based moving factor. Unlike a static password, the generated value changes as the defined time interval changes, reducing the usefulness of intercepted credentials after their validity period expires. The timestamp-oriented principle of TOTP is particularly relevant to the present research because the proposed framework employs time information to generate dynamic authentication credentials [5].

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 124-134
ISSN: 3071-3358

M. L. T. Uymatiao and W. E. S. Yu investigated a time-based OTP authentication mechanism that incorporates secure communication for protecting the exchange of authentication information. Their approach demonstrates the importance of protecting not only the OTP itself but also the mechanisms through which authentication secrets are established and exchanged. This provides motivation for integrating OTP generation with a cryptographic key-exchange mechanism in the proposed framework [13].

2.4 Lightweight Encryption and Secure Key Exchange

M. Usman et al. proposed the SIT lightweight encryption algorithm specifically for secure IoT communication. The authors noted that conventional encryption techniques can impose considerable computational and energy costs on low-power devices and developed a compact cipher intended to address these limitations. Their experimental discussion demonstrates the importance of considering memory utilization, code size, and execution cycles when evaluating encryption mechanisms for constrained IoT platforms [6].

C. A. Lara-Nino et al. surveyed lightweight elliptic-curve cryptographic approaches and examined their suitability for constrained environments. Their study showed how public-key cryptography can be adapted to resource-limited devices through efficient curve-based constructions. Although the present research focuses on an enhanced RSA mechanism, the findings of this work are relevant because they demonstrate the broader requirement for efficient public-key mechanisms in IoT security [7].

S. Kumari et al. proposed an ECC-based authentication scheme for IoT and cloud-server environments. Their research addressed the challenge of providing secure authentication while considering the computational characteristics of connected devices. The study demonstrates that public-key cryptography can be integrated with authentication protocols to establish trust between IoT devices and remote services, supporting the broader concept of combining authentication and key-establishment mechanisms [8].

A. Karati et al. investigated a lightweight certificateless signature scheme for Industrial IoT environments. Their work focused on providing authentication and integrity protection while reducing some of the management requirements associated with conventional public-key infrastructures. The study reinforces the importance of efficient authentication and cryptographic mechanisms for industrial IoT environments where devices may operate continuously under resource and communication constraints [9].

2.5 Research Gap

The reviewed studies demonstrate significant progress in IoT authentication, lightweight cryptography, OTP-based security, and public-key mechanisms. However, these approaches often address individual security requirements independently. OTP mechanisms provide dynamic authentication but require secure credential exchange, while asymmetric cryptography provides secure key establishment but can introduce additional computational overhead on constrained devices. Lightweight encryption approaches reduce computational requirements but may not independently address dynamic user or device authentication. Therefore, there is a research opportunity to integrate these security functions within a unified framework.

The proposed research addresses this gap by combining **timestamp-based OTP authentication with an enhanced RSA key-exchange mechanism and lightweight encryption**. The timestamp component provides temporary and dynamically changing authentication credentials, while the RSA mechanism is used to protect the exchange of sensitive authentication information and establish secure communication parameters. Lightweight encryption is subsequently intended to protect the actual data exchanged between authorized entities. This layered architecture seeks to achieve a balance among authentication strength, confidentiality, secure key exchange, and computational efficiency in IoT environments.

Proposed System

The proposed system presents a secure data-sharing architecture that integrates Time-based One-Time Password (TOTP) authentication, RSA-based key exchange, and lightweight data encryption. The framework is designed as a three-module architecture in which the first module authenticates users through a dynamic OTP, the second establishes secure communication and exchanges cryptographic keys using an enhanced lightweight RSA mechanism, and the third encrypts sensitive data during storage and transmission.

Whenever a data owner initiates a sharing operation, the system generates a unique OTP for the authorized user. The OTP is protected through asymmetric encryption using the recipient's public key, allowing only the corresponding private-key holder to recover and use the authentication credential. Because the OTP is temporary and session-specific, the possibility of credential reuse is reduced.

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 124-134
ISSN: 3071-3358

The proposed framework combines authentication, secure key exchange, and data encryption to provide layered protection against unauthorized access and communication-based attacks. The use of lightweight cryptographic techniques is intended to reduce computational and energy requirements, making the architecture suitable for IoT devices with limited processing power and memory.

Public-key cryptography is widely used to establish secure communication over insecure networks. It uses a pair of mathematically related keys: a public key that can be distributed openly and a private key that remains confidential to its owner. A sender encrypts information using the receiver's public key, while decryption requires the corresponding private key. Since knowledge of the public key alone should not permit practical recovery of the protected message, this approach supports secure communication and key exchange. RSA is one of the best-known public-key cryptographic algorithms based on this principle.

Traditional password-based authentication remains vulnerable to threats such as password theft, guessing, reuse, and phishing. Multi-factor authentication improves protection by requiring an additional verification factor. Time-based One-Time Password authentication generates short-lived credentials using a shared secret and synchronized time information. Unlike conventional OTP delivery through SMS or email, TOTP values can be independently generated by authorized systems using the same secret and time interval. Since each password remains valid only for a limited duration, previously generated codes become invalid after expiration.

3. System Architecture

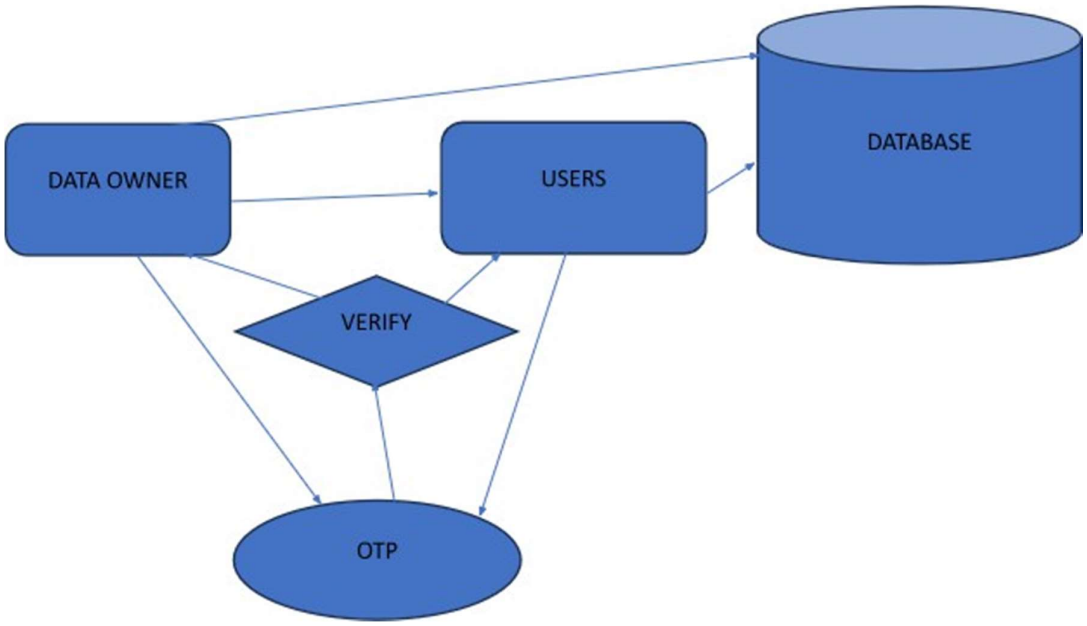

Fig 1 :System Architecture

The system architecture of the Secure Server-Based Data Storage and Retrieval System is designed to provide a robust, secure, and scalable platform for managing users, data owners, and encrypted files while ensuring data integrity and confidentiality. The architecture follows a multi-tier design comprising the Presentation Layer, Application Layer, Data Layer, Security Layer, and Administration Layer, integrating cryptographic and blockchain technologies for end -to-end security.

Presentation Layer

This layer serves as the interface for Users, Data Owners, and Admins. Users interact via a web interface or client application to register, log in, verify OTPs, search for files, and request downloads. Data Owners access the interface to upload files, manage metadata, and share encryption keys. Admins use a dashboard to monitor system activity, verify users, and manage permissions.

Application Layer

The Application Layer handles all core business logic. The Authentication Module validates

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 124-134
ISSN: 3071-3358

credentials and generates OTPs for secure, one-time authentication. The Encryption Module applies RSA encryption for file confidentiality and SHA-256 hashing to generate unique hash values for each file block. The File Management Module splits files into four encrypted blocks and reassembles them during retrieval. The Blockchain Module assigns a unique blockchain-linked ID to each file, ensuring tamper-proof tracking and verification.

Data Layer

The Database Layer stores all user credentials, OTP records, encrypted file blocks, hash values, and blockchain IDs. It ensures secure, reliable, and efficient data storage and retrieval, providing a foundation for integrity and traceability.

Security Layer

This layer integrates OTP verification, encryption, hashing, and access control to protect against unauthorized access, data tampering, and cyberattacks.

Administration Layer

Admins monitor activities, verify accounts, manage permissions, and audit all system operations to maintain compliance and system integrity.

System Workflow

Users register/login → OTP verification → authentication. Data Owners upload files → encryption
→ hash generation → blockchain ID creation → database storage. Users request files → verification → decryption → file delivery. Admin oversees all activities.

This architecture ensures confidentiality, integrity, authentication, and traceability, providing a secure end-to-end file management system suitable for sensitive and critical data.

4. Methodology

The proposed methodology consists of three integrated security modules. The authentication module verifies users using conventional credentials together with Time-based OTP authentication. The secure communication module performs asymmetric key exchange using a lightweight RSA-based mechanism suitable for constrained IoT devices. The data protection module applies lightweight symmetric encryption to secure information during transmission and storage.

Initially, the user is authenticated through the primary login process and a time-dependent OTP. After successful authentication, the communicating entities establish or exchange the required symmetric encryption key through the asymmetric security mechanism. The symmetric algorithm is then used to encrypt the actual data because symmetric encryption generally provides efficient processing for larger volumes of information. This hybrid design combines the authentication benefits of TOTP, the secure key-distribution capability of public-key cryptography, and the efficiency of lightweight symmetric encryption.

Requirements Engineering

The system is designed to address common weaknesses associated with conventional password-based authentication and resource-intensive security mechanisms. Passwords may be compromised through phishing, guessing, credential theft, or other attacks. The inclusion of OTP-based verification introduces an additional authentication factor, while TOTP reduces dependence on external delivery services such as SMS or email. Because the generated code is valid only for a predefined time window, delayed or previously captured codes have limited usefulness.

The proposed lightweight RSA-based key exchange mechanism is intended to reduce the computational requirements associated with conventional public-key operations. The use of multi-prime RSA and efficient decryption techniques such as the Chinese Remainder Theorem can improve certain computational operations when implemented appropriately. However, the overall security of such an implementation depends on secure parameter selection, key generation, implementation quality, and protection against side-channel vulnerabilities. The proposed architecture therefore focuses on achieving a practical balance between security strength and computational efficiency for low-resource IoT environments.

Hardware Requirements

The following hardware configuration is sufficient for the development, testing, and execution of the proposed system:

- **Processor:** Intel Core i3 or higher
- **RAM:** 4 GB DDR4 or higher
- **Monitor:** 15.6-inch LED display or equivalent
- **Storage:** Minimum 100 GB available hard-disk or SSD space

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 124-134
ISSN: 3071-3358

- **Peripheral Devices:** Keyboard and mouse
- **Optional Devices:** Webcam or other IoT sensing devices, depending on the application

Software Requirements

The proposed system can be developed and deployed using a Java-based web application environment. The required software components include:

- **Front End:** Java EE technologies, including JSP and Servlets
- **Database:** MySQL 5.5 or later
- **Operating System:** Windows 10 or Windows 11
- **Web Server:** Apache Tomcat 7.0 or a compatible version
- **Browser:** Google Chrome or Mozilla Firefox
- **Development Environment:** Eclipse IDE or IntelliJ IDEA

5. Implementation

The proposed system was implemented as a Java-based web application designed to provide secure communication and authentication for IoT-oriented environments. Core Java was used for developing the main application logic, while Socket and ServerSocket mechanisms were employed to support communication between clients and servers. The user interface was developed using web technologies and Cascading Style Sheets (CSS). The implementation includes several Java bean and data-access classes, such as AliceDetails, UserBean, AttackBean, KeyReqBean, and KeyBean, which manage user information, login activity, attack-related details, key requests, and cryptographic keys. These components support organized data handling and enable the different security modules of the proposed system to interact efficiently.

6. Results

The developed application provides an integrated environment for secure user and administrator operations. The system includes interfaces for administrator authentication, user registration, and general application access. The snapshots demonstrate the practical implementation of the proposed framework and illustrate the interaction between users and the security mechanisms incorporated into the system.

Various Snapshots

Secure Administrator Access

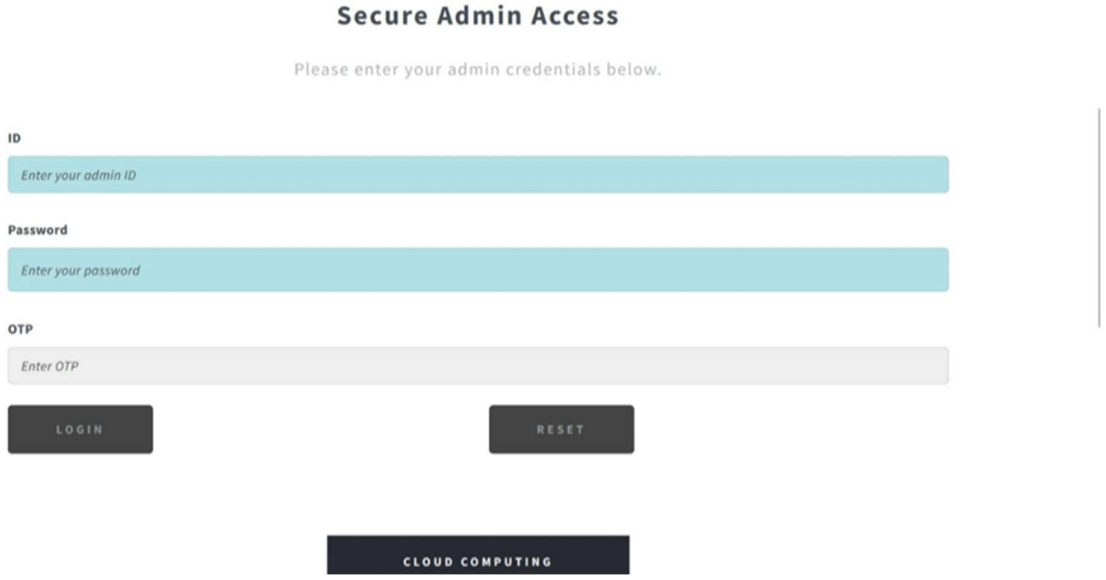

Fig 2

This interface provides authorized administrators with secure access to the system and its management functions.

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 124-134
ISSN: 3071-3358

Home Page

Fig 3

The home page acts as the primary interface of the application and provides access to the major system

User Registration

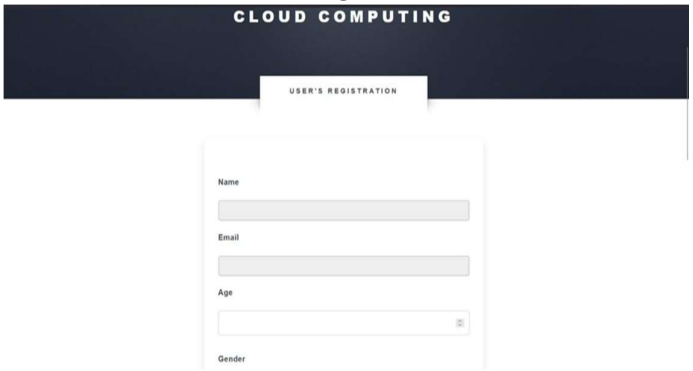

Fig 4

The registration module enables new users to submit their personal details and create credentials for accessing the secure application.

Secure System Access

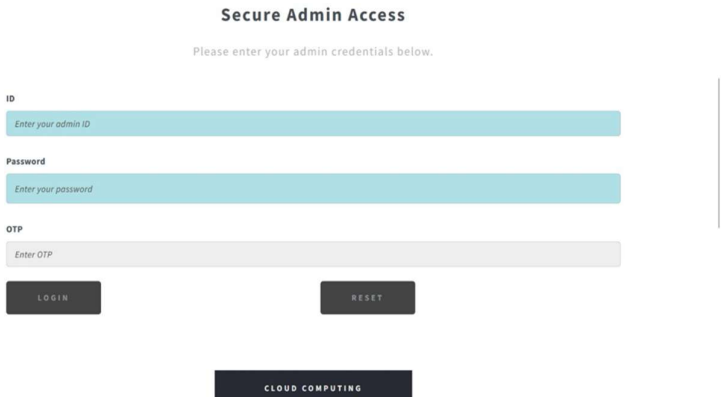

Fig 5

This module demonstrates the protected access mechanism used to verify users and maintain secure interaction with the application.

Software Testing

Software testing was performed to identify defects and verify that the developed system operates according to its specified requirements. The testing process evaluates individual components as well as the complete application to ensure correct functionality, reliability, and acceptable system behavior. Different testing activities were considered to validate the major features of the proposed security framework and to reduce the possibility of operational errors.

Testing Methodology

A structured testing methodology was adopted to examine both the general and security-related functions of the application. The system was evaluated under different operating conditions to verify communication, authentication, key exchange, and encryption processes. Quality-control procedures were applied throughout the testing phase to identify defects and confirm that the implemented modules satisfy the requirements defined during system development.

Future Enhancement

The proposed framework can be extended by integrating additional lightweight and emerging cryptographic techniques suitable for highly constrained IoT devices. Future versions may incorporate stronger authentication mechanisms, adaptive key management, and improved protection for data stored and transmitted across distributed IoT networks. The framework can also be enhanced through cloud integration, automated threat monitoring, and support for larger heterogeneous IoT environments. These improvements could increase scalability, resilience, and security while maintaining low computational and energy requirements.

Conclusion

This work presents an end-to-end lightweight security framework for protecting IoT communication and data. The proposed system combines three major security functions: time-based one-time-password authentication, lightweight RSA-based key exchange using three prime numbers, and SIT-based data encryption. Together, these modules provide authentication, secure key establishment, and protection of transmitted information.

The framework is intended to address the security limitations of resource-constrained IoT devices by reducing computational complexity while maintaining essential security functions. The results demonstrate that lightweight cryptographic approaches can provide a practical foundation for secure communication in low-power IoT environments. Therefore, the proposed architecture offers a suitable approach for improving authentication, key management, and data confidentiality in modern IoT systems.

References

1. Suo et al. [1], Misra et al. [3], and Kumar et al. [6] discussed the major security challenges in the Internet of Things, including privacy, authentication, secure communication, and protection against cyberattacks.
2. Al-Aboosi et al. [2], Dutta et al. [4], Shah et al. [5], Gunathilake et al. [7], Katagi and Moriai [8], and Eisenbarth et al. [9] examined lightweight cryptography techniques designed for resource-constrained IoT devices.
3. V. K. B. Parasaram, V. T. Bathini, S. K. Nalluri, & A. H. Sannidhanam. (2026). A Sustainable AI-Enabled Predictive Maintenance Framework for Smart Industrial Systems Using Industrial IoT Data. *2026 Third International Conference on Innovations in Cybersecurity and Data Science (ICICDS)*, 440–447. doi:10.1109/ICICDS70526.2026.11604878
4. Sannidhanam, A. H. (2026). LLM-Driven Workflow Optimization: Intelligent Routing in Asynchronous Distributed Systems. *International Journal of AI and Machine Learning, 1*(2), 23–33.
5. Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," *Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526
6. Distributed Data Processing Frameworks for Large-Scale Healthcare Analytics. (2019). *International Journal of Advance*

Industrial Engineering, 7(04), 1–10. doi:10.14741/ijaie/v.7.4.01

7. Sannidhanam, A. H. (2021). Real-Time Claims Processing Using Event-Driven Architectures. *International Journal of Technology, Management and Humanities, 7*(01), 36–50. doi:10.21590/07.01.02
8. Abd Zaid and Hassan [16] and Sahu et al. [17] proposed enhanced RSA-based approaches to strengthen cryptographic security and improve resistance against attacks.
9. Goyal and Sahula [18], Kumar Kiran et al. [19], and Beaulieu et al. [20] developed lightweight encryption algorithms, including TEA, SIMON, and SPECK, for low-power and constrained IoT devices.
10. Usman et al. [21] proposed the SIT lightweight encryption algorithm, while Thabit et al. [22] introduced a lightweight cryptographic approach to improve data security in cloud computing.
11. Lara-Nino et al. [23] provided a comprehensive survey of elliptic curve lightweight cryptography, highlighting its suitability for devices with limited computational and memory resources.
12. Kumari et al. [24] and Karati et al. [25] proposed secure ECC-based authentication and certificateless signature schemes for IoT, cloud, and Industrial IoT environments.
13. Basu et al. [26] and Punithavathi et al. [27] explored intelligent IoT frameworks using cognitive computing and machine learning-based authentication to improve task management, security, and device authentication.
14. Anjani Haritha Sannidhanam. (2024). Prompt Engineering Patterns for Reliable LLM Outputs in Production Environments. *Journal of Multidisciplinary Knowledge, 4*(1), 29–39.
15. Performance Analysis of Wireless Sensor Networks for Smart Monitoring Applications. (2016). *International Journal of Humanities and Information Technology, 1*(04), 10–29. doi:10.21590/ijhit.01.04.04
16. Anjani Haritha Sannidhanam. (2023). Self-Healing Distributed Systems: AI-Driven Failure Prediction and Automated Recovery. *International Journal of Research & Technology, 11*(4), 168–174.
17. Sannidhanam, A. H. (2025). Autonomous AI Agents for Cloud Infrastructure Operations. *Journal of Contemporary Science and Technology Management, 1*(01), 83–100.
18. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," *Smartphone Security and Protection Practices*", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6
19. Eram Fatima, Dr. Nidhi Mishra, Dr. Mohammed Abdul Bari *," Dynamic Load Balancing in Heterogeneous Cloud Environments Using Adaptive QoS-aware Algorithms*", International Conference on Innovations in Data Analytics (ICIDA 2025) Date 5 - 6 December 2025.,ICIDA-2025-Kolkata ,India –
20. M'Raihi et al. [10] and [11] introduced the Time-Based One-Time Password (TOTP) and HMAC-Based One-Time Password (HOTP) algorithms for secure user authentication.
21. Uymatiao and Yu [12], Kumar et al. [13], Shivraj et al. [14], and Roy and Kalita [15] investigated OTP-based and other authentication mechanisms to improve security in IoT environments.
22. Sannidhanam, A. H. (2020). Comparative Analysis of Cloud Computing Architectures for Enterprise Applications. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 12*(02), 169–180. doi:10.18090//samriddhi.v12i02.16
23. Anjani Haritha Sannidhanam. (2023). Zero-Downtime AI Model Updates in Real-Time Inference Systems. *International Journal of Engineering Science & Humanities, 13*(2), 70–78.

About Author

Mohammed Shoeb Ahmed is currently pursuing a Master of Technology (M.Tech) in Computer Science and Engineering at ISL Engineering College, affiliated with Osmania University, Hyderabad, India. He completed his Bachelor of Technology (B.Tech) from Lords Engineering College in 2023