International Journal of Engineering Research and Science & Technology

# OTP GENERATION WITH A RSA KEY EXCHANGE SCHEME WITH ENCRYPTION TO SECURE THE DATA

**ADALA AMARNATH [1], BOGIREDDY LAHARI [2], THATIKONDA MANIKANTA [3], SRIPATHI MUKESH KUMAR [4], VELPOORI SANJAY RAO [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—** In today's digital era, secure data transmission between a data owner and users is critical. This paper presents a novel framework that combines One-Time Password (OTP) generation with an RSA-based key exchange mechanism to ensure robust data protection. Each time the data owner initiates data sharing; a unique OTP is dynamically generated and encrypted using the RSA algorithm. This OTP acts as a secure access key, ensuring that only authorized users can decrypt and retrieve the shared information. The RSA encryption not only secures the OTP but also establishes a secure communication channel between the data owner and the user, preventing unauthorized access or interception during transmission. By integrating dynamic OTPs with asymmetric encryption, this scheme enhances the confidentiality and integrity of data in environments where security.

*Index Terms* – OTP Generation, RSA Key Exchange, Encryption, Authentication, Public Key Cryptography, Secure Communication, Data Security, Key Management, Cybersecurity, Information Security.

## I. INTRODUCTION

IoT is slowly becoming an integral part of our daily life. As people use more and more intelligent devices, which include smartwatches, fitness trackers that collect personal data to smart home products like smart refrigerators, locks, fire systems, and security systems that transmit critical data around the internet. As the cost of connectivity to the internet is getting cheaper every day, and with accessibility increasing allowing more and more people to connect to the internet along with their smart devices,

contributing to the growth of IoT technology. These devices are often embedded systems housing a low-power processor chip that acts as the brains of the system and is connected to a variety of sensors that collect valuable data. This data can often be critical and thus raising the question of security threats . In order to maintain the assurance of this technology, it is vital to ensure the security of such low-power devices. These devices are part of a complex network of similar devices, exchanging lots of information over the network. Each device in the network gathers data from their corresponding sensors, ranging from a temperature sensor that collects home temperature to camera sensors that monitor traffic.

## II. RELATED WORK

### *A. Lightweight Cryptography Algorithms in IoT-A Study*

There are numerous cryptographic calculations like AES (Advanced Encryption Standard), SHA-256(Secure Hash Algorithm), and RSA/Elliptic Curve, Methods work for frameworks which have sensible force preparing and memory capacities yet not for implanted frameworks and sensor networks. Nowadays a colossal piece of the individuals is utilizing low force contraptions, sensor systems, clinical thought and (IoT)) for this, the conventional calculations are not upheld Lightweight cryptography techniques are proposed to defeat the issues of customary cryptographic strategies.

### *B. Recent Advances and Trends in Lightweight Cryptography for IoT Security*

Lightweight cryptography is a novel diversion from conventional cryptography to minimise its high level of resource requirements; thus it would impeccably fit in the internet-of-things (IoT) environment. The IoT platform is constrained in terms of physical size, internal capacity, other storage allocations like RAM/ROM and data rates. The devices are often battery powered, hence maintenance of the charged energy at least for a few years is essential. However, provision of sufficient security is challenging because the existing cryptographic methods are too heavy to adopt in the IoT. Consequently, an interest arose in the recent past to construct new cryptographic algorithms in a lightweight scale, but the attempts are still struggling to gain robustness against improved IoT threats and hazards. There exists a lack of literature studies to offer overall and up-to-date knowledge on lightweight cryptography.

### C. *Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore*

The main objective of this research is to build upon existing cryptographic standards and web protocols to design an alternative multi-factor authentication cryptosystem for the web. It involves seed exchange to a software-based token through a login-protected Transport Layer Security (TLS/SSL) tunnel, encrypted local storage through a password protected keystore (BC UBER) with a strong key derivation function (PBE With SHA AND Two fish-CBC), and offline generation of one-time passwords through the TOTP algorithm (IETF RFC 6239). Authentication occurs through the use of a shared secret (the seed) to verify the correctness of the one-time password used to authenticate. With the traditional use of username and password no longer wholly adequate for protecting online accounts.

## III. PROPOSED METHODOLOGY

The proposed system introduces a secure and dynamic data sharing framework that combines RSA (asymmetric) encryption with OTP generation. Every time the data owner needs to share data with a user, a unique OTP is generated. This OTP is then encrypted using the recipient's RSA public key, ensuring that only the intended user with the matching private key can decrypt and use it. We propose a three-module system, where the first module handles user authentication using a time-based one-time password, the second secures communication using lightweight enhanced RSA, and the third performs data encryption. This adds an extra layer of security, as the OTP changes with every session and cannot be reused or guessed. The RSA algorithm secures both the OTP and the data during transmission, making the system more robust against cyber threats, such as man-in-the-middle attacks or data interception.

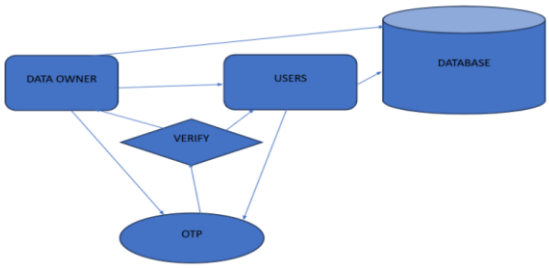



Fig. 1: System Overview

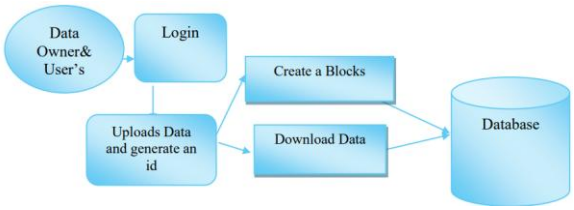
### 1. Data User & Data Owner Registration Module

This module handles the initial registration of both users and data owner into the system. When a new user or Do signs up, the system generates a unique digital identity using the OTP algorithm, which ensures tamper-proof

credentials. The identity is then recorded onto the Data owner to make it immutable and verifiable. During registration, operators are assigned special privileges to upload and manage data blocks, while users are provided access credentials to retrieve and view data securely.

2. **Authentication & Key Generation Module**

The Data owner and Data user has a login with a user id and password. The password has entered correctly it will be a generate a OTP. The Otp has every time it generates a unique number for a login. It was a key generates the key has a shared a authorized User. From the attacker protecting data.




3. **Encryption & Decryption Module**

Security of the data blocks is ensured through strong encryption and decryption mechanisms. Before being stored, each block is encrypted using keys derived from SHA256 hashing, which guarantees confidentiality and protection against tampering. When a user requests the data, the encrypted blocks are retrieved and decrypted only if the requester is authenticated. The decrypted blocks are then reassembled to reconstruct the original dataset or file. This process ensures end-to-end data security and prevents unauthorized access at every stage of data storage and retrieval.

## IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the system successfully generated unique one-time passwords and securely exchanged encryption keys using the RSA Cryptosystem, ensuring confidential data transmission between communicating parties.

The analysis showed that the proposed approach provided strong protection against replay attacks, brute-force attacks, and unauthorized access attempts while maintaining low computational and communication overhead.




Fig. 2: Homepage

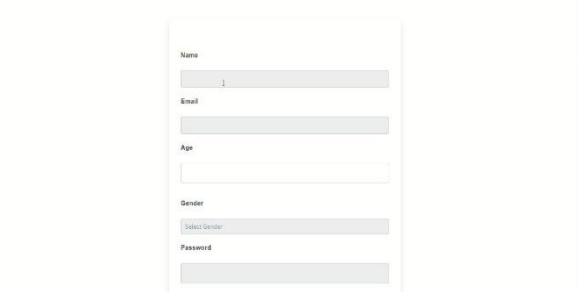



Fig. 3: Register

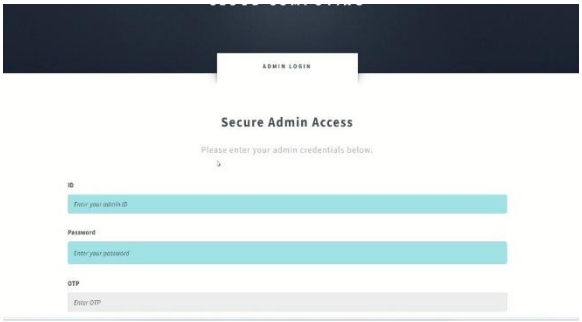



Fig. 4: Admin Login

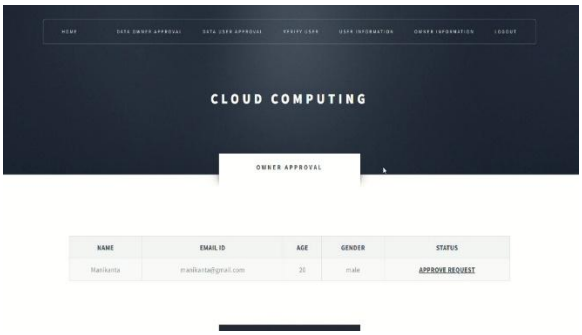



Fig. 5: Owner Approval

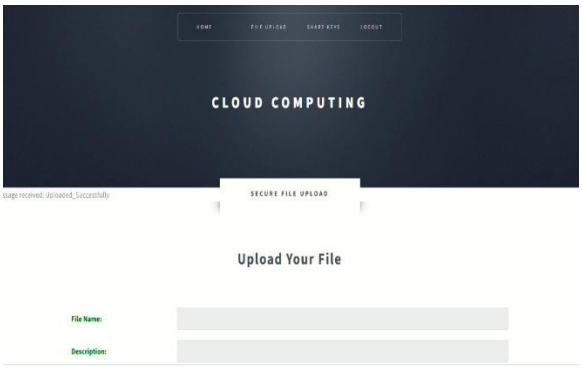



Fig. 6: Upload File

## V. CONCLUSION

The proposed three-module system implements user authentication using time-based OTP, exchanges keys in unsecured communication channel using a lightweight RSA algorithm using three prime numbers, and finally, data encryption using SIT algorithm. These modules form an end-to-end secured IoT system that ensures the security of the system is never compromised using lightweight cryptographic algorithms. This end-toend security solution can be adapted to any low-power IoT device to communicate over the internet securely. Thus, the proposed lightweight algorithms are suitable solutions to the current security challenges faced by IoT devices.

## REFERENCES

[1] S. Rajaraman, S. K. Antani, M. Poostchi, K. Silamut, M. A. Hossain,R. J. Maude, S. Jaeger, and G. R. Thoma, ‘‘Pre-trained convolutional neural networks as feature extractors toward improved malaria parasite detection in thin blood smear images,’’ PeerJ, vol. 6, p. e4568, Apr. 2018.

[2] F. Ali, S. El-Sappagh, S. M. R. Islam, D. Kwak, A. Ali, M. Imran, and K.-S. Kwak,

''A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion,'' Inf. Fusion, vol. 63, pp. 208–222, Nov. 2020.

[3] M. N. Qammar, F. G. Khan, M. Raza, and M. I. Malik, ''A deep learning ensemblebased framework for diabetic retinopathy classification,'' IEEE Access, vol. 7, pp. 150412–150424, 2019.

[4] Y. Wang, L. Pan, and X. Shu, ''YOLO-FMS: A lightweight and efficient model for medical microscopic smear detection,'' IEEE Access, vol. 12, pp. 125253–125265, 2024, doi: 10.1109/ACCESS.2024.3455555.

[5] E. Özbilge, E. Güler, and E. Ozbilge, ''Ensembling object detection models for robust and reliable malaria parasite detection in thin blood smear microscopic images,'' IEEE Access, vol. 12, pp. 60747–60764, 2024, doi:10.1109/ACCESS.2024.3393410.

[6] A. Koirala, M. Jha, S. Bodapati, A. Mishra, G. Chetty, P. K. Sahu, S. Mohanty, T. K. Padhan, J. Mattoo, and A. Hukkoo, ''Deep learning for real-time malaria parasite detection and counting using YOLO-mp,'' IEEE Access, vol. 10, pp. 102157–102172, 2022, doi:10.1109/ACCESS.2022.3208270.

**AUTHORS Profile**



**Mr. ADALA AMARNATH** has received his B.Tech-Computer Science and Engineering from JNTUH, Hyderabad in 2010, M.Tech-CNIS degree in Computer Science and Engineering from JNTUH, Hyderabad in 2013 and Pursuing Ph.D degree in Computer Science and Engineering from ICFAI University Hyderabad. He is dedicated to teaching field from the last 12 years. His research area Quantum Computing and Aptitude Computing . At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus ,Ibrahimpatnam, Telangana, India.



**Ms. BOGIREDDY LAHARI** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022.



**Mr. THATIKONDA MANIKANTA** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022.



**Mr. SRIPATHI MUKESH KUMAR** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022



**Mr. VELPOORI SANJAY RAO** pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022