IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13380

OTP GENERATION WITH RSA KEY EXCHANGE SCHEME WITH ENCRYPTION TO SECURE DATA

A. Sunitha[1], Bikash Kumar Sah[2], D. Rishi[3], B. Venkat Pavan[4]

Assistant Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad[1]

Students, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad[2-4]

Abstract: In modern digital communication systems, ensuring the secure transmission of sensitive data is a major challenge due to increasing cyber threats and unauthorized access. This paper proposes a secure data protection framework that integrates One-Time Password (OTP) generation with an RSA-based key exchange scheme. In the proposed system, whenever a data owner initiates a data-sharing process, a unique OTP is dynamically generated to authenticate the user. The generated OTP is then encrypted using the RSA encryption algorithm before transmission. The RSA key exchange mechanism ensures that only the intended recipient possessing the correct private key can decrypt the OTP and access the shared data. This approach provides a dual layer of security by combining dynamic authentication with strong asymmetric encryption. As a result, the system significantly enhances data confidentiality, integrity, and protection against interception or unauthorized access during transmission. The proposed scheme can be effectively applied in secure communication systems, cloud data sharing platforms, and authentication-based applications.

Keywords: One-Time Password (OTP), RSA Encryption, Key Exchange, Data Security, Secure Communication.

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 [1,2]. 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. These sensors generate a humongous amount of data, and this data is communicated between other devices over the internet. Thus, IoT is changing the landscape of the conventional internet to the next level by connecting everything to the internet. So, security concerns related to data. confidentiality, integrity, and authentication must be considered seriously. These devices must be able to safeguard the privacy of the user data and should not compromise the integrity of the system. Nevertheless, due to its nature of openness in terms of connectivity, IoT introduces new security challenges since it is inherently vulnerable to various threats like information leakage and unauthorized usages [3,4]. One backdrop of IoT devices is that they are prone to physical attacks resulting in exposure of data stores in the components. Also, IoT devices are most commonly connected via wireless networking, making them vulnerable to security attacks and unauthorized access, resulting in data loss, data leakage, and damage to the entire network. Encryption would solve this problem of data security for regular devices like computers and smartphones, but using the same cryptographic algorithms for IoT devices which are embedded systems, is questionable since the hardware architecture in these devices is more diminutive and low-powered [5,6]. Hence to address these security concerns, there is a need to use the appropriate cryptographic algorithms to maintain the integrity of the system. However, conventional cryptographic algorithms are not suitable for these smart devices since they are constrained by energy consumption, computational power, memory utilization, network bandwidth. Hence the cryptographic solutions must be appropriate for low-resource hindered devices, unlike conventional algorithms that use a lot of energy and computational power performing many rounds of encryption [7–9]. This paper presents a three-module system to meet the above requirements as efficiently and reliably as possible. The proposal is to implement various lightweight cryptographic encryption and

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13380

security algorithms so that the data being transferred between these IoT devices is secure and not vulnerable to breaches. The main focus is to implement these algorithms into one shared platform for all IoT devices.

Most of the secure authentication mechanisms in recent times often adopt a time based, one-time password system [10, 11]. In such a time-based One Time Password (OTP) authentication system as used in [12], the implementation is accomplished at the application level. Two applications, a server application that is running and a client application, are used in the entire process. The server application keeps accepting connection requests, and when a connection request from a client is sent to the server, it gets accepted and connects to the server.

II. RELATED WORK

The rapid expansion of the Internet of Things (IoT) has created new challenges in ensuring secure communication and protecting sensitive data transmitted between connected devices. Researchers have proposed various cryptographic mechanisms to address these security concerns, particularly focusing on lightweight cryptography and improved authentication techniques suitable for resource-constrained environments.

Several studies have explored the use of lightweight cryptographic algorithms for IoT devices. The conducted a comprehensive study on lightweight cryptography algorithms for IoT environments. Their work highlights that conventional cryptographic techniques such as AES, RSA, and SHA-256 are computationally expensive for embedded devices with limited processing power, memory, and battery life. The authors emphasize the need for optimized cryptographic approaches that balance security and performance for IoT-based systems.

Proposed a lightweight cryptographic algorithm for enhancing data security in cloud computing environments. Their algorithm uses substitution–permutation networks and logical operations such as XOR and shifting to achieve strong confusion and diffusion properties while maintaining high efficiency.

Although these approaches provide valuable contributions toward improving IoT security, several limitations still remain. Many existing systems either rely on static encryption keys or lack dynamic authentication mechanisms, making them vulnerable to attacks such as key interception, replay attacks, and unauthorized access. Therefore, integrating dynamic OTP-based authentication with asymmetric encryption techniques such as RSA can significantly enhance the confidentiality, integrity, and security of data communication in IoT systems**.**

III. LITERATURE SURVEY

Title: Lightweight Cryptography Algorithms in IoT-A Study.
Author: P. Shah, M. Arora and K. Adhvaryu.
Year: 2024.
Description:
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. This contains imperatives identified with physical size, preparing necessities, and memory limitations. These research paper investigations the different encryption methods and features the upsides and downsides of each approach.

Title: Recent Advances and Trends in Lightweight Cryptography for IoT Security.
Author: O. Yessenbayev, D. C. D. Nguyen, T. Jeong, K. J. Kang, H. R. Kim, J. Ko, J.-Y. Park, M.-S. Roh, and M. Comuzzi,
Year: 2024
Description:
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

DOI: 10.17148/IARJSET.2026.13380

literature studies to offer overall and up-to-date knowledge on lightweight cryptography. Therefore, this effort is to bridge the areas in the subject by summarising the content we explored during our complete survey recently. This work contains the development of lightweight cryptographic algorithms, its current advancements and futuristic enhancements. In contrast, this covers the history, parametric limitations of the invented methods, research progresses of cryptology as well as cryptanalysis.

Title: "Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore.
Author M. L. T. Uymatiao and W. E. S. Yu
Year: 2024
Description:
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 (PBEWithSHAANDTwofish-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, and with regulators worldwide toughening up security requirements (i.e. BSP 808, FFIEC), this research hopes to increase research effort on further development of cryptosystems involving multi-factor authentication.

Title: "Efficiently improving the security of OTP.
Author: D. Kumar, A. Agrawal and P. Goyal
Year: 2025
Description:
The easy, convenient and remote access to internet is definitely changing the way we live. It has also become a major factor in the financial lives of millions. Using the Internet to carry out online banking simplifies our financial affairs when compared to the traditional banking method. The inclusion of Online Banking by different sectors like health, financial, educational institutions etc. which accounts for most of the population has not only increased its importance but at the same time has attracted the cyber criminals to take the advantage of the loopholes in the process of online transaction. The cybercriminals can make use of these loopholes and carry out transaction which might not come in the knowledge of user and the bank. Recent studies have shown that the OTP which was developed as a part of two factor authentication is vulnerable to attacks. In this paper, we present a new framework for enhancing authentication during online transaction which secures our OTP.

Title: Lightweight Cryptography for Resource Constraint Devices: Challenges and Recommendation
Author Y. Jiang, X. Xu, H. Gao, A. D. Rajab, F. Xiao, and X. Wang.
Year: 2023
Description:
In the recent few years, data communication through the Internet of Things (IoT) network is increased exponentially. However, the data is prone to several attacks on the network. The most popular attacks are eavesdropping, replay, man-in-the-middle attack, etc. To prevent these attacks, cryptography algorithms are used. The devices are deployed in the IoT network are resource constraint, limited memory, and low battery life. Therefore, the National Institute of Standard and Technology (NIST) recommended the lightweight cryptography algorithm to provide security in these devices. In this paper, we have reviewed the recent lightweight cryptography algorithms. Next, it defines the open research challenges and recommendations based on the literature review.

Title: Lightweight cryptography for the internet of things.
Author: M. Katagi and S. Moriai.
Year: 2024
Description:
This paper surveys Lightweight Cryptographic solutions for Internet of Things (IoT). This survey covers comprehensively a flow of security measures from Lightweight Cryptographic solutions to comparison among different types of block ciphers. It also includes comparison between Hardware vs Software solutions and different recent approaches of the most trusted and researched block cipher, Advanced Encryption Standard (AES) in terms of architecture, Mix-Column/S-box modify strategy and attacks for IoT security. According to the study, lightweight AES has proved to be a good security solution for constrained IoT devices.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13380

Title: A new lightweight cryptographic algorithm for enhancing data security in cloud computing
Author: S. Fugkeaw, L. Wirz, and L. Hak,
Year: 2024
Description:
Data has been pivotal to all facets of human life in the last decades. In recent years, the massive growth of data as a result of the development of various applications. This data needs to be secured and stored in secure sites. Cloud computing is the technology can be used to store those massive amounts of data. The rapid development of this technology makes it more critical. Therefore, it has become urgent to secure data from attackers to preserve its integrity, confidentiality, protection, privacy and procedures required for handling it. This paper proposed a New Lightweight Cryptographic Algorithm for Enhancing Data Security that can be used to secure applications on cloud computing. The algorithm is a 16 bytes (128-bit) block cipher and wants 16 bytes (128-bit) key to encrypt the data. It is inspired by feistal and substitution permutation architectural methods to improve the complexity of the encryption. The algorithm achieves Shannon's theory of diffusion and confusion by the involvement of logical operations, such as (XOR, XNOR, shifting, swapping). It also features flexibility in the length of the secret key and the number of turns. The experimental results of the proposed algorithm presented a strong security level and an apparent enhancement in measures of cipher execution time and security forces compared to the cryptographic systems widely used in cloud computing.

IV. PROPOSED SYSTEM

- 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.

V. PROPOSED SYSTEM ADVANTAGES

- OTP ensures one-time secure access — changes every time.
- RSA protects the OTP and eliminates insecure key sharing.
- High security in both key exchange and data encryption

ALGORITHM
Asymmetric Encryption (RSA), Dynamic One-Time Password (OTP) Generation
The proposed algorithm for the secure data sharing system integrates asymmetric encryption using RSA with dynamic One-Time Password (OTP) generation to enhance the security of data transmission and access. The algorithm is designed to provide strong protection against unauthorized access, interception, and replay attacks by combining multi-factor authentication and encryption techniques. The process begins with a setup phase, where the intended receiver generates an RSA key pair consisting of a public key and a private key. The public key is shared with the data owner or sender, while the private key is securely stored by the receiver and never disclosed to any third party. This asymmetric key pair ensures that any data encrypted using the public key can only be decrypted by the corresponding private key, thereby establishing a secure communication channel between the sender and the receiver. Once the keys are generated and exchanged, the system proceeds to the data sharing phase. In this phase, whenever the data owner intends to share sensitive data with a user, the system dynamically generates a unique One-Time Password (OTP) for that particular transaction. The OTP acts as a temporary session key and ensures that every data sharing operation uses a different encryption parameter, thereby eliminating the risk of key reuse. The generated OTP is first used to encrypt the original data using a symmetric encryption mechanism, ensuring fast and efficient processing of the data. After encrypting the data, the OTP itself is further protected by encrypting it using the receiver's RSA public key. This two-layer encryption mechanism guarantees that even if the encrypted data and OTP are intercepted during transmission, the attacker cannot decrypt the OTP without possessing the private key of the legitimate receiver. Both the encrypted data and the RSA-encrypted OTP are then transmitted through the network to the authorized user. In the data access phase, the receiver initiates the decryption process by first decrypting the OTP using their private RSA key. Since the private key is known only to the receiver, this step ensures that only the legitimate user can retrieve the OTP. After successfully obtaining the

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

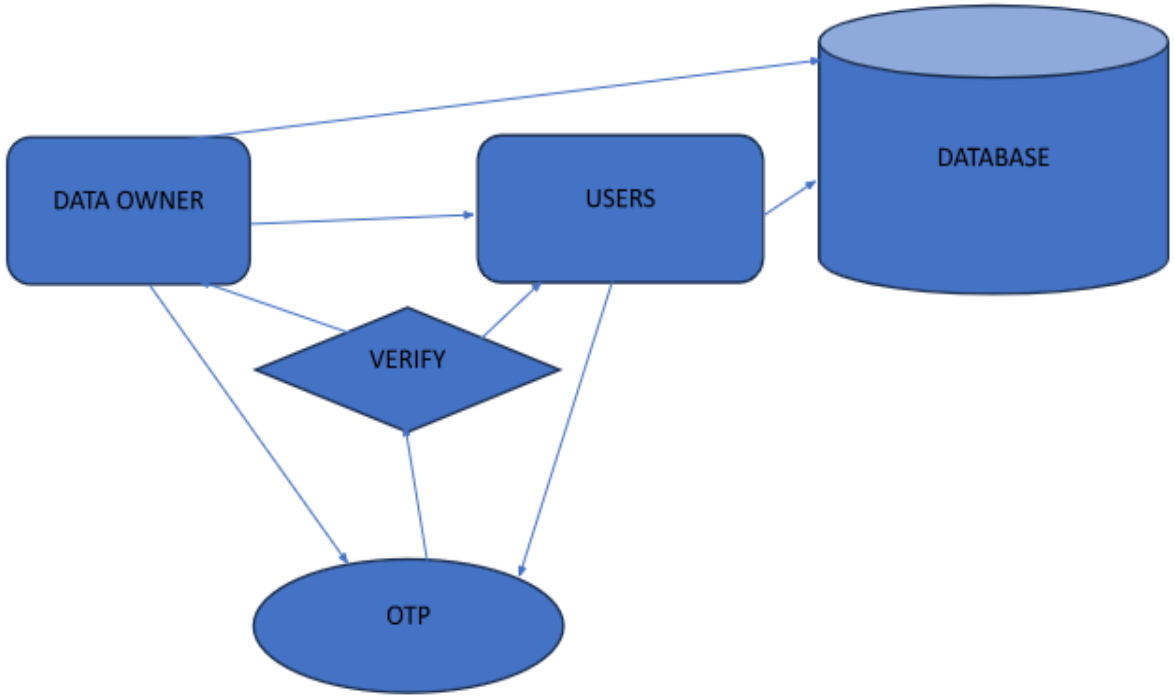
International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13380

OTP, the receiver uses it as the symmetric key to decrypt the encrypted data and recover the original information. This multi-stage process significantly strengthens the confidentiality and integrity of the transmitted data. Additionally, the dynamic nature of the OTP ensures that each communication session uses a new key, preventing replay attacks and unauthorized reuse of credentials. By combining RSA-based secure key exchange with time-based OTP authentication, the proposed algorithm provides a robust, lightweight, and scalable security solution suitable for environments such as cloud systems and Internet of Things (IoT) networks where secure data transmission and user authentication are critical. The algorithm not only protects data confidentiality but also improves trust, reliability, and resistance against common cyber threats such as man-in-the-middle attacks, brute-force attempts, and unauthorized data access.

VI. 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.

VII. CONCLUSION

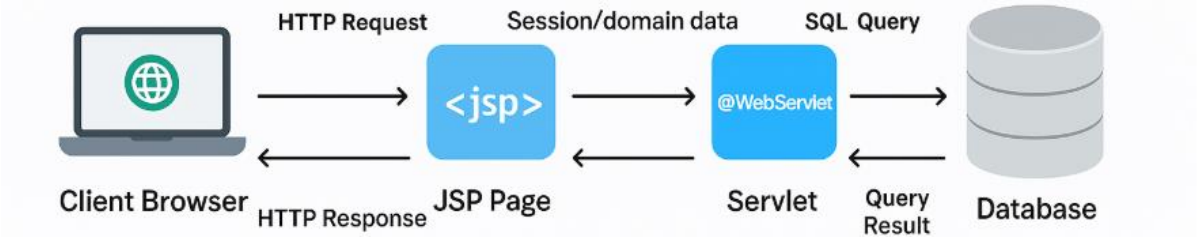
Java offers several features that make it well-suited for interacting with databases. One of its key strengths is the Java Database Connectivity (JDBC) API, which provides a standard interface for connecting to relational databases. JDBC enables Java applications to execute SQL queries, update data, and manage database connections, allowing developers to work with databases in a consistent and platform-independent way. Java also supports Object-Relational Mapping (ORM) frameworks like Hibernate, which simplify the interaction between Java objects and relational database tables, reducing the need for boilerplate SQL code. Additionally, Java's portability and scalability make it ideal for large-scale enterprise applications that need to interact with databases, whether running on a local server or in the cloud. Its strong exception handling, multi-threading capabilities, and robust security features also ensure reliable, efficient, and secure database management. Overall, Java's rich set of libraries and frameworks, along with its ability to seamlessly integrate with databases, makes it a powerful choice for developing database-driven applications.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13380



REFERENCES

[1]. H. Suo, J. Wan, C. Zou and J. Liu. Security in the internet of things: a review. In Proceedings of the International conference on computer science and electronics engineering, IEEE, 3: 648–651, 2012.

[2]. A. M. MohamadAl-Aboosi, S. Kamil, S. N. H. Sheikh Abdullah and K. A. Zainol Ariffin. Lightweight Cryptography for Resource Constraint Devices: Challenges and Recommendation. In Proceedings of the 3rd International Cyber Resilience Conference(CRC), IEEE, 1–6, 2021.

[3]. S. Misra, M. Maheswaran, S. Hashmi. Security challenges and approaches in internet of things. Cham: Springer International Publishing, 2017.

[4]. I. K. Dutta, B. Ghosh and M. Bayoumi. Lightweight cryptography for internet of insecure things: A survey. In Proceedings of the 9th Annual Computing and Communication Workshop and Conference(CCWC), IEEE, 0475–0481, 2019.

[5]. P. Shah, M. Arora and K. Adhvaryu. Lightweight Cryptography Algorithms in IoT-A Study. In Proceedings of the Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(ISMAC), IEEE, 332–336, 2020.

[6]. 96 V.N.H.Kollipara et al.

[7]. S. A. Kumar, T. Vealey and H. Srivastava. Security in internet of things: Challenges, solutions and future directions. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), IEEE, 5772–5781, 2016.

[8]. N. A. Gunathilake, A. Al-Dubai and W. J. Buchana. Recent Advances and Trends in Lightweight Cryptography for IoT Security. In Proceedings of the 16th International Conference on Network and Service Management(CNSM), IEEE, 1–5, 2020.

[9]. M. Katagi and S. Moriai. "Lightweight cryptography for the internet of things." Sony Corporation, 7–10, 2008.

[10]. T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann and L. Uhsadel. A survey of lightweight-cryptography implementations. IEEE Design & Test of Computers, 24(6):522—533, 2007.

[11]. D. M'Raihi, David, S. Machani, M. Pei, and J. Rydell. Totp: Time-based one-time password algorithm, Internet Engineering Task Force, RFC: 6238, 2011.

[12]. M'Raihi, David, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen. Hotp: An hmac-based one-time password algorithm. In The Internet Society, Network Working Group. RFC4226, 2005.

[13]. M. L. T. Uymatiao and W. E. S. Yu. Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore. In Proceedings of the 4th IEEEInternational Conference on Information Science and Technology, IEEE, 225–229, 2014.

[14]. D. Kumar, A. Agrawal and P. Goyal. Efficiently improving the security of OTP. In Proceedings of the International Conference on Advances in Computer Engineering and Applications, IEEE, 912–915, 2015.

[15]. V. L. Shivraj, M. A. Rajan, M. Singh and P. Bala Muralidhar. One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In Proceedings of the 5th National Symposium on Information Technology: Towards New Smart World, IEEE, 1–6, 2015.

[16]. K. S. Roy and H. K. Kalita. A survey on authentication schemes in IoT. In Proceedings of the International Conference on Information Technology(ICIT), IEEE, 202–207, 2017.

[17]. M. Abd Zaid, Mustafa, and S. Hassan. Lightweight RSA Algorithm Using Three Prime Numbers. Journal of Engineering and Applied Sciences, 14(5): 9032–9035, 2019.

[18]. J. Sahu, V. Singh, V. Sahu, and A. Chopra. An enhanced version of RSA to increase the security. Journal of Network Communication and Emerging Technologies, 7(4), 1–4, 2017.

[19]. T. K. Goyal and V. Sahula. Lightweight security algorithm for low power IoT devices. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, 1725–1729, 2016.

[20]. V.G. Kumar Kiran, S.J. Mascarenhas, S. Kumar, J. Pais Viven Rakesh. Design and implementation of Tiny encryption algorithm. International Journal of Engineering Research and Applications, 5(6): 94–97, 2015.

DOI: 10.17148/IARJSET.2026.13380

[21]. R. Beaulieu, D. Shors, J. Smith, S. Treat man-Clark, B. Weeks, and L. Wingers. SIMON and SPECK: Block Ciphers for the Internet of Things. NIST Lightweight Cryptography Workshop., 1–15, 2015.

[22]. M. Usman, I. Ahmed, M.I. Aslam, S. Khan, and U.A. Shah. SIT: a lightweight encryption algorithm for secure internet of things. International Journal of Advanced Computer Science and Applications, 8(1): 1–10, 2017.

[23]. F. Thabit, S. Alhomdy, A. H. Al-Ahdal and S. Jagtap. A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1):91–99, 2021.

[24]. C. A. Lara-Nino, A. Diaz-Perez and M. Morales-Sandoval. Elliptic Curve Lightweight Cryptography: A Survey. IEEE Access, 6: 7251472550, 2018.

[25]. S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu & N. Kumar. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. The Journal of Supercomputing, 74(12), 64286453, 2018.

[26]. A. Karati, S. H. Islam & M. Karuppiah. Provably secure and lightweight certificateless signature scheme for IIoT environments. IEEE Transactions on Industrial Informatics, 14(8), 3701–3711, 2018.

