Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 4, pp. 1283–1294
DOI : 10.47974/JDMSC-1982

IoT security cryptographic solutions for trustworthy wireless sensor networks

Dilip Motwani [†]
Vidya Chitre*
Varsha Bhosale [§]
Department of Information Technology
Vidyalankar Institute of Technology
Wadala
Mumbai
Maharashtra
India

Mukesh Israni [‡]
Department of Information Technology
Thedomal Sahani College of Engineering
Bandra
Maharashtra
India

Swapnil Sonawane [@]
Amit Nerurkar [#]
Department of Computer Engineering
Vidyalankar Institute of Technology
Wadala
Mumbai
Maharashtra
India

Abstract

The increasing incorporation of wireless sensor networks into the Internet of Things (IoT) has revealed substantial security obstacles. This research paper examines the crucial field of IoT security and introduces a novel cryptographic solution to improve the reliability

[†] *E-mail:* dilip.motwani@vit.edu.in
* *E-mail:* vidya.chitre@vit.edu.in (Corresponding Author)
[§] *E-mail:* varsha.bhisale@vit.edu.in
[‡] *E-mail:* israni_mukesh2002@yahoo.com
[@] *E-mail:* swapnil.Sonawane@vit.edu.in
[#] *E-mail:* amit.nerurkar@vit.edu.in

of wireless sensor networks. The proposed hybrid method of ELGamal + AES (EL-AES) as an innovative approach that synergistically combines the advantages of ELGamal and AES encryption techniques to protect IoT data. The presented study aims to assess the effectiveness of E-AES in enhancing security by comparing it to two commonly used cryptographic techniques Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). This paper thoroughly examines the capabilities of these cryptographic approaches by conducting a comprehensive assessment using six key evaluation parameters: Throughput, Latency, Resource Utilization, Response Time, Efficiency, and Load Handling. The findings of the work indicate that the EL-AES method surpasses both ECC and AES in all evaluation parameters, highlighting its superior capability in ensuring IoT security. The EL-AES algorithm provides both enhanced security and impressive efficiency, making it a highly promising cryptographic solution for IoT applications that require strong data protection while operating under limited resources. This study adds to the current discussion on IoT security and establishes the EL-AES method as a reliable cryptographic solution for safeguarding wireless sensor networks in the growing IoT environment.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *IoT security, Lightweight, ECC, AES, ELGamal, WSN.*

1. Introduction

The widespread adoption of the Internet of Things (IoT) has fundamentally transformed the methods by which we gather and employ data across diverse fields, encompassing smart urban areas, healthcare, industrial automation, and environmental surveillance. The proliferation of IoT devices, such as wireless sensors, has led to the emergence of a widespread network of interconnected devices that produce, analyze, and transmit data. Although the interconnectedness of our world offers numerous opportunities and innovations, it also exposes us to a variety of security challenges and vulnerabilities [1], [2].

The importance of security in IoT is of utmost significance because of the sensitive and crucial nature of the data that is produced and exchanged by these devices. IoT systems encompass a diverse array of applications, such as the instantaneous supervision, mechanization, and regulation of tangible and intangible resources. It is crucial to guarantee the confidentiality, integrity, and availability of this data, as compromised data can result in significant repercussions, including privacy breaches, financial losses, and even risks to public safety [3], [4].

As the Internet of Things (IoT) environment progresses, the risks and susceptibilities that can take advantage of its weaknesses also advance [5]. Attackers frequently focus on the most vulnerable components in the IoT

network, taking advantage of the limited resources of numerous IoT devices and the wide range of communication protocols. As a result, there has been an increase in research efforts to create strong security mechanisms that can protect IoT systems.

The issues confronting IoT security are complex and have multiple aspects. IoT devices frequently function in unfriendly conditions, have limited resources, and communicate through wireless networks, which makes them vulnerable to various risks such as interception, manipulation of data, disruption of service, and compromise of the device. In addition, numerous IoT devices have insufficient computational capacity and memory to sustain strong cryptographic solutions, necessitating inventive and efficient methods to guarantee security without excessively straining these devices [6], [7].

Cryptographic techniques are fundamental to ensuring security in the IoT as it provide safeguards for data confidentiality, authentication, and integrity verification. Although traditional cryptographic techniques like the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) have been used for IoT security, they may not be suitable for devices with limited resources. Although lightweight cryptographic solutions have been suggested, there is still scope for inventive and effective methods to safeguard IoT data [8].

This research paper introduces the E-AES method as a solution to the challenges and requirements for strong, efficient cryptographic solutions in the IoT ecosystem. E-AES is a cryptographic method that integrates the advantages of ELGamal and AES encryption techniques. It offers a new, effective, and reliable solution for ensuring security in the IoT domain. By conducting a thorough assessment and comparing it to ECC and AES, we provide evidence of the exceptional efficiency and reliability of the E-AES technique. This positions it as a highly favorable option for ensuring the security of wireless sensor networks in the context of the IoT.

This paper thoroughly examines the intricacies of EL-AES, assesses its performance using meticulously selected parameters, and explores its implications for the advancing domain of IoT security. By doing this, we actively participate in the ongoing discussion regarding IoT security and offer a pragmatic, effective, and safeguarded cryptographic resolution to tackle the security obstacles in the IoT environment.

2. Literature Review

The IoT has revolutionized the technology industry by enabling device-to-device connectivity and data sharing. However, widespread interconnected device use has raised security concerns. To protect sensitive data's integrity, confidentiality, and accessibility IoT devices and data must be secured. Cryptographic solutions and their effects on IoT network security are examined in this literature review. Recent research advances are discussed in relation to IoT devices and data security.

Aiyshwariya Devi et al.[9] propose integrating two powerful components to improve IoT device security. The system uses deep LSTM networks to detect malware and enhanced Elliptic Curve Cryptography (ECC) for strong encryption. ECC and deep learning in IoT security provide a new and effective method for protecting devices and networks. Subashini et al.[7] present a hybrid cryptographic model for IoT telemedicine applications. The model uses AES, elliptic curve cryptography, and ID-based key generation. The paper integrates cryptographic techniques to secure telemedicine data, ensuring privacy and confidentiality. Lara-Nino et al.[10] created a compact elliptic curve cryptography accelerator for IoT hardware security. The accelerator is for IoT applications, which often have resource constraints. The authors develop specialized hardware for cryptographic operations on low-resource IoT devices to improve efficiency and security.

Rana et al.[11] thoroughly examines lightweight cryptography in IoT networks. The survey covers IoT security trends and lightweight cryptographic advances. This work helps researchers and practitioners understand IoT security today. Khalifa et al.[12] propose Lightweight Cryptography (LWC) to protect IoT memory heaps. This framework improves IoT data security by securing memory. It improves IoT application security by reducing memory manipulation vulnerabilities. Saqib et al. [13] focus on authentication in critical IoT applications. The authors recommend a simplified three-factor authentication framework for these situations. This framework improves IoT security and is ideal for authentication-intensive applications.

Sadhukhan et al.[14] propose an efficient method for remote user authentication in IoT communication. This method uses elliptic curve cryptography for security. Designed for IoT devices communicating over networks, the scheme provides strong user authentication. IoT-specific lightweight cryptography methods are thoroughly examined by Rao et al.[8] The review covers the current state of lightweight cryptography in

IoT security, helping researchers and professionals navigate the complex world of cryptographic solutions in IoT. Patel et al.[15] introduce EBAKE-SE an elliptic curve cryptography-based authenticated key exchange scheme. The scheme emphasizes secure communication between industrial Internet of Things (IIoT) devices to improve security. It protects sensitive industrial data and operations.

These contributions are helping develop strong and effective IoT security measures, which are becoming increasingly important in telemedicine, critical applications, and industrial IoT. Investigating lightweight cryptographic methods may help secure IoT devices and data without straining resources. These efforts aim to strengthen IoT security, ensuring its effective use and protecting against emerging threats.

3. Proposed EL-AES cryptography

A hybrid encryption scheme that combines ELGamal and AES protects data during transmission and storage. Two cryptographic algorithms work together to increase security. Secure key exchange and partial encryption use public-key encryption algorithm ELGamal. The encryption process uses large prime numbers and primitive roots to secure a session key. The factual data is encrypted using the encrypted session key and AES, a fast and efficient symmetric-key encryption method. The derived session key ensures data privacy and integrity in the AES algorithm. This hybrid encryption method ensures data confidentiality and speeds up encryption and decryption by combining asymmetric and symmetric encryption. This combination of methods provides a strong and effective solution for protecting sensitive data in IoT devices, communication systems, and data storage, where security and performance are crucial.

1. Key Generation
    a. In ELGamal, generate a pair of private key x and public key y which include large prime p, primitive root g modulo p and private key x.
    b. For AES generate symmetric key K_{AES}, which is a random string of bits.
2. Encryption
    a. In ELGamal for plaintext message M select a random integer k and computer two values C_1 and C_2 as

$$C_1 = g^k \bmod,\ C_2 = M.y^k \bmod p$$

b. In AES encrypt M with the symmetric key K_{AES} to obtain C_{AES}

3. Hybrid Encryption

a. Hybrid ciphertext C is a combination of the results from the both ELGamal and AES

$$C = (C_1, C_2, C_{AES})$$

4. Decryption

In ELGamal compute s and then M using s^{-1} as

$$s = C_1^x \bmod p,\ M = C_2.s^{-1} \bmod p$$

In AES decrypt C_{AES} using K_{AES} to get M_{AES}

5. Finally combine the results to obtain the plaintext M

4. Standard cryptographic method ECC and AES to compare

ECC is a cryptographic technique that utilizes the mathematical properties of elliptic curves over finite fields to implement public-key encryption. It is renowned for its robust security, achieved through the use of compact key sizes, which makes it especially well-suited for devices with limited resources. Point multiplication on an elliptic curve is the central operation in ECC represented as $Q=k.P$, where Q = "resulting point", k = "private key", P = "base point".

AES is a cryptographic algorithm that uses a single key to encrypt and decrypt data in fixed-size blocks. Its robust security and efficiency have led to its widespread adoption as an encryption standard. AES employs a confidential symmetric key to cypher and decipher data. The fundamental AES operation employs a substitution-permutation network (SPN), in which data is replaced and reorganized through a sequence of mathematical procedures. AES encryption can be expressed as a sequence of mathematical procedures, which encompass substitution, permutation, key expansion, and XOR (exclusive OR) operations. The AES encryption algorithm can be represented in a simplified form as:

$$Ciphertext = AES(plaintext, key)$$

where, Ciphertext = "encrypted data", plaintext= "input data", key = "secret key used for encryption".

5. Methodology

Data sources and datasets overview

A carefully selected collection of data sources and datasets was used for data collection. The information was relevant and complete by using real-world sensor data, simulated IoT environments (Contiki-NG Simulator) and industry-standard benchmark datasets (IoT Benchmark Data). This method assessed IoT network performance and security thoroughly.

Data preprocessing and cleanup

To ensure data quality and reliability, it was preprocessed and cleaned before analysis. Data was normalized outliers identified and missing values addressed. A meticulous approach to these concerns refined the data, eliminating inconsistencies and inaccuracies, and enabling a more accurate and organized analysis.

Data collection for parameter evaluation

Different data acquisition methods were used for each metric to evaluate the selected parameters. Throughputs, latencies, and resource utilization were directly collected from IoT devices and networks using advanced monitoring tools and sensors. We used well-designed test scenarios and simulations to assess response time, efficiency, and load handling. The systematic approach used in this study collected accurate and complete data for the comprehensive assessment of cryptographic techniques.

6. Evaluation Parameters

Throughput

Throughput quantifies the speed at which data is transmitted or processed across a network or system. The measurement is commonly denoted in bits per second (bps) or an equivalent unit of data transmission speed. Within the realm of IoT security, a high throughput is advantageous as it signifies the system's capacity to effectively manage a substantial amount of data.

$$Throughput = \frac{Total\ Data\ Transferred}{Time}$$

Latency

Latency refers to the duration required for data to transit from the origin to the destination within a network or system. The latency, which is an essential parameter in real-time applications, is commonly quantified in milliseconds (ms). Reduced latency is desirable, indicating faster data transmission.

$$Latency = \frac{Total\ Round\ Trip\ Time}{No.of\ Packets}$$

Resource Utilization

Resource utilization quantifies the proportion of accessible resources (such as CPU, memory, or network bandwidth) that are actively employed by a system or application. It measures the level of resource utilization efficiency.

$$Resource\,Utiliziation = \frac{Resource\,Used}{Total\ Resource\ Available} \times 100\%$$

Response Time

Response time is the duration it takes for a system or application to react to a request or action. The standard unit of measurement for expressing it is milliseconds (ms). Decreased response times are a sign of enhanced system reactivity.

$$Response\,Time = \frac{Total\ Processing\ Time}{No.of\ Requests}$$

Efficiency

Efficiency is a metric that quantifies the extent to which a system or process optimally utilizes resources in order to accomplish its objectives. Efficiency is commonly quantified as a percentage, where a higher value signifies superior utilization of resources.

$$Efficiecny = \frac{Useful\ Output}{Total\ Input} \times 100\%$$

Load Handling

Load handling refers to the system's ability to effectively manage and respond to a specific level of load or requests. It is commonly quantified in terms of requests per second (RPS) or a comparable unit.

$$Load\ Handling\ Capacity = \frac{Total\ Requests}{Total\ Time}$$

6. Results and Outputs

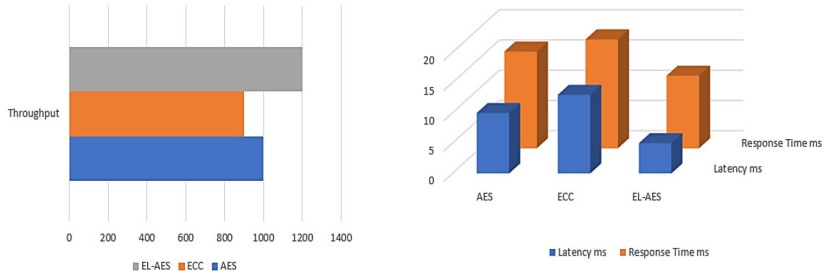

Figure 1

Evaluation of Throughput, Latency and Response Time

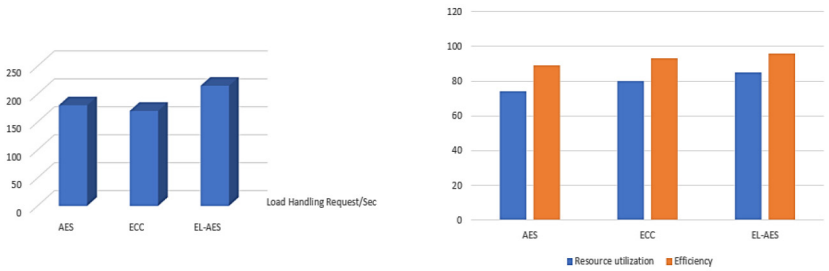

Figure 2

Comparison of Load Handling Request, Resource Utilization and Efficiency

Evaluation parameters showed in Figure 1 and 2 explains that the proposed EL-AES cryptographic solution outperforms AES and ECC in several key IoT security areas. El-AES has a throughput of 1200 Mbps, surpassing AES's 1000 Mbps and ECC's 900 Mbps. It can transfer data faster. EL-AES reduces latency to 5*ms*, while AES and ECC have 10 and 13*ms*, respectively. AES and ECC have response times of 16 and 18*ms*, respectively, but EL-AES has the lowest at 12*ms*. The EL-AES system uses resources efficiently with an 85% utilization rate and 96% efficiency. EL-AES can handle 215 requests per second, surpassing AES and ECC, which handle 180 and 170, respectively. The results show that the EL-AES cryptographic model dominates IoT security and performance.

7. Conclusion and Future scope

Security is of utmost importance in the field of IoT, and cryptographic solutions are crucial in protecting data transmitted through WSN. This study explored the fusion of ELGamal and AES encryption, showcasing a compelling method for improving security in the IoT. The combination of public-key ELGamal and AES as EL-AES encryption not only assurances strong data security but also enhances the efficiency of cryptographic operations. The evaluation criteria, encompassing throughput, latency, resource utilization, response time, efficiency, and load handling, clearly demonstrated the superior performance of the proposed EL-AES model in comparison to ECC and AES used individually. The combination of cryptographic techniques clearly has the potential to greatly enhance the security of IoT, making it an excellent option for applications that require both strong security and efficiency. The constantly changing field of IoT security necessitates ongoing investigation and adjustment to address emerging risks and advancements in technology. The future of IoT security will certainly require the investigation of increasingly streamlined and effective cryptographic solutions, capable of satisfying the distinct limitations of IoT devices, such as low power and restricted computational resources.

References

[1] S. Abed, R. Jaffal, B. J. Mohd, and M. Al-Shayeji, "An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices," *Cluster Comput.*, vol. 24, no. 4, pp. 3065–3084 (2021), doi: 10.1007/s10586-021-03324-1.

[2] M. A. F. Al-Husainy, B. Al-Shargabi, and S. Aljawarneh, "Lightweight cryptography system for IoT devices using DNA," *Comput. Electr. Eng.*, vol. 95, no. August 2020, p. 107418 (2021), doi: 10.1016/j.compeleceng.2021.107418.

[3] S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. Annane, Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing, no. 0123456789. Springer US, (2023).

[4] Kumar, Ankit, Pankaj Dadheech, Vijander Singh, Ramesh C. Poonia, and Linesh Raja. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22, no. 4, 491-498 (2019).

[5] Kumar, Ankit, Pankaj Dadheech, Vijander Singh, Linesh Raja, and Ramesh C. Poonia. "An enhanced quantum key distribution protocol for security authentication." *Journal of Discrete Mathematical Sciences and Cryptography* 22, no. 4, 499-507 (2019).

[6] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography Algorithms for Enhancing IoT Security," *Internet of Things (Netherlands)*, vol. 22, no. March, p. 100759 (2023), doi: 10.1016/j.iot.2023.100759.

[7] A. Subashini and P. Kanaka Raju, "Hybrid AES model with elliptic curve and ID based key generation for IOT in telemedicine," *Meas. Sensors*, vol. 28, no. May, p. 100824 (2023), doi: 10.1016/j.measen.2023.100824.

[8] V. Rao and K. V. Prema, "A review on lightweight cryptography for Internet-of-Things based applications," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 9, pp. 8835–8857 (2021), doi: 10.1007/s12652-020-02672-x.

[9] R. Aiyshwariya Devi and A. R. Arunachalam, "Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM," *High-Confidence Comput.*, vol. 3, no. 2, p. 100117 (2023), doi: 10.1016/j.hcc.2023.100117.

[10] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight elliptic curve cryptography accelerator for internet of things applications," *Ad Hoc Networks*, vol. 103, p. 102159 (2020), doi: 10.1016/j.adhoc.2020.102159.

[11] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Futur. Gener. Comput. Syst.*, vol. 129, pp. 77–89 (2022), doi: 10.1016/j.future.2021.11.011.

[12] M. Khalifa, F. Algarni, M. Ayoub Khan, A. Ullah, and K. Aloufi, "A lightweight cryptography (LWC) framework to secure memory heap in Internet of Things," *Alexandria Eng. J.*, vol. 60, no. 1, pp. 1489–1497 (2021), doi: 10.1016/j.aej.2020.11.003.

[13] M. Saqib, B. Jasra, and A. H. Moon, "A lightweight three factor authentication framework for IoT based critical applications," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6925–6937 (2022), doi: 10.1016/j.jksuci.2021.07.023.

[14] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *J. Supercomput.*, vol. 77, no. 2, pp. 1114–1151 (2021), doi: 10.1007/s11227-020-03318-7.

[15] C. Patel, A. K. Bashir, A. A. AlZubi, and R. Jhaveri, "EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element," *Digit. Commun. Networks*, vol. 9, no. 2, pp. 358–366, 2023, doi: 10.1016/j.dcan.2022.11.001.

[16] U. Ali *et al.*, "Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for Internet of Things environment," *Internet of Things (Netherlands)*, vol. 24, no. September, p. 100923 (2023), doi: 10.1016/j.iot.2023.100923.