Enhancement of Security in IoT using Modified AES Algorithm for IoT Applications

Dr V Gokula Krishnan
Saveetha University

Proceedings of the International Conference on Sustainable Communication Networks and Application (ICSCNA 2023)
IEEE Xplore Part Number: CFP23DW8-ART; ISBN: 979-8-3503-1398-7

Enhancement of Security in IoT using Modified AES Algorithm for IoT Applications

P. Satyanarayana
Department of ECE
V. R. Siddhartha Engineering College
Vijayawada, India
satya.sp14@gmail.com

Narasimhachary Sriramdas
Department of ECE
Bharath Institute of Higher Education and Research
Chennai, Tamil Nadu, India
narasimhachary435@gmail.com

Bondili Madhavi
Department of ECE
Mallareddy College of Engineering
Hyderabad, Telangana, India
bondilimadhavi@gmail.com

Arun M
Department of ECE
Panimalar Engineering College
Chennai, Tamil Nadu, India
arunmemba@ieee.org

N. V. Phani Sai Kumar
Department of ECE
SRKR Engineering College
Bhimavaram, India
kumar.sai087@gmail.com

Dr. V. Gokula Krishnan
Department of CSE
Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences (SIMATS)
Chennai, Tamil Nadu, India
gokul_kris143@yahoo.com

2023 International Conference on Sustainable Communication Networks and Application (ICSCNA) | 979-8-3503-1398-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSCNA58489.2023.10370606

Abstract— The proliferation of Internet of Things (IoT) devices has led to a surge in data exchange over networks, making security paramount for ensuring the integrity and confidentiality of transmitted information. This paper proposes a novel approach for bolstering security in IoT environments by employing a modified Advanced Encryption Standard (AES) algorithm tailored to suit the unique requirements of IoT applications. The conventional AES algorithm, while highly robust, poses challenges in terms of computational resources and energy consumption when implemented on resource-constrained IoT devices. To address these limitations, our proposed modification leverages lightweight cryptographic techniques, optimizing the algorithm for low-power microcontrollers commonly found in IoT devices. The modified AES algorithm exhibits a significant reduction in computational accuracy while maintaining a high level of security. By adapting modified AES to the IoT ecosystem, the study aims to mitigate potential vulnerabilities and improve the overall security of IoT networks. To validate the efficacy of the proposed approach, extensive simulations and experimental studies were conducted on a diverse set of IoT devices across varying network conditions. The results demonstrate a substantial improvement in security performance metrics including throughput, latency, and energy consumption compared to conventional methods.

Keywords: Security Enhancement, Modified AES Algorithm, Lightweight Cryptography, Dynamic Key Management, Resource-Constrained Devices.

I. INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices has ushered in an era of pervasive connectivity, where everyday objects are equipped with sensors, actuators, and communication capabilities. This paradigm shift has unlocked countless possibilities across domains such as healthcare, smart cities, agriculture, and industrial automation. However, the widespread adoption of IoT technology has also given rise to an array of security challenges [11]. As IoT devices collect, transmit, and process sensitive data, it becomes imperative to safeguard this information against unauthorized access, tampering, and eavesdropping.

The Internet of Things (IoT) has revolutionized the way to interact with the physical world, seamlessly integrating our environments with an interconnected web of smart devices, sensors, and actuators. This transformative paradigm shift has paved the way for unprecedented levels of automation, efficiency, and convenience in various domains such as healthcare, transportation, agriculture, and smart cities. However, the proliferation of IoT devices also brings forth a host of security challenges that demand immediate attention. This paper presents an in-depth exploration of the multifaceted landscape of security in IoT, focusing on the existing vulnerabilities, state-of-the-art solutions, and emerging trends that collectively aim to fortify the IoT ecosystem [12].

The emergence of IoT represents a monumental leap in technological advancement, characterized by the proliferation of connected devices ranging from consumer wearables to industrial sensors. This proliferation is underpinned by the integration of cutting-edge technologies such as wireless communication protocols, cloud computing, and edge computing. However, this pervasive connectivity introduces an intricate web of security challenges, necessitating robust measures to safeguard data integrity, confidentiality, and availability.

The IoT landscape is rife with vulnerabilities that can be exploited by malicious actors to compromise the integrity and privacy of sensitive information. These vulnerabilities include insecure communication channels, weak authentication mechanisms, susceptibility to physical tampering, and the notorious challenge of managing secure software updates in resource-constrained devices [13]. Additionally, the sheer diversity of IoT devices, each with its own set of hardware configurations and communication protocols, further complicates the task of implementing a one-size-fits-all security. Addressing the security challenges inherent to IoT necessitates a multi-faceted approach, encompassing hardware-level security, secure communication protocols, access control mechanisms, and robust encryption algorithms. This paper provides an exhaustive review of the state-of-the-art security solutions, including hardware-based root of trust, secure bootstrapping, lightweight cryptographic primitives, and blockchain technologies. Furthermore, it delves into the deployment of intrusion detection systems, anomaly detection, and machine learning-based techniques for real-IoT devices often handle a wealth of sensitive information, ranging from personal health data to industrial telemetry. As such, ensuring privacy is paramount in IoT deployments. This section examines the challenges associated with data anonymization, consent management, and the need for robust privacy-preserving techniques [14]. It also explores the regulatory frameworks and compliance requirements that guide data protection practices in IoT environments.

Looking ahead, the evolution of IoT into hyperconnected ecosystems envisions a future where devices, systems, and services seamlessly interact to deliver unprecedented levels of automation and intelligence. This section outlines the emerging trends and technologies that hold promise in bolstering IoT security, including federated identity management, edge AI for anomaly detection, and the integration of quantum-resistant cryptographic primitives [15].

Cryptographic techniques have long been a cornerstone of information security, and they hold immense promise in addressing the unique security concerns of IoT systems. The Advanced Encryption Standard (AES), endorsed by the National Institute of Standards and Technology (NIST), stands as one of the most widely used encryption algorithms, renowned for its efficiency and security. However, the resource-constrained nature of IoT devices demands a reevaluation of conventional cryptographic solutions to ensure they align with the specific requirements and constraints of IoT applications [16]. This paper introduces a modified AES algorithm designed to enhance the security of IoT systems.

IoT security is a complex landscape characterized by a diverse range of devices, communication protocols, and deployment scenarios. The inherent heterogeneity of IoT ecosystems presents unique challenges, including:

Resource Constraints: Many IoT devices operate with limited computational power, memory, and energy resources, making traditional cryptographic operations computationally expensive.

Network Diversity: IoT devices communicate over diverse networks, including wired, wireless, and low-power protocols, each with its own set of vulnerabilities and security considerations.

Scale and Heterogeneity: IoT deployments often involve a vast number of devices with varying levels of security maturity, making management and uniform enforcement of security policies challenging.

AES, a symmetric-key block cipher algorithm, has been widely adopted as the de facto standard for data encryption in various applications. It offers a high level of security and computational efficiency, making it suitable for many use cases. However, its suitability for IoT applications is limited by the resource constraints and diverse operating environments of IoT devices. Therefore, there is a pressing need to adapt and optimize AES to address the unique security challenges presented by the IoT ecosystem. In response to the intricate security landscape of IoT, a modified AES algorithm is proposed for the specific requirements and constraints of IoT applications. This algorithm aims to strike a balance between security and resource efficiency, making it well-suited for resource-constrained IoT devices.

II. Related works

Raza and Wallgren (2017) [1] provides a comprehensive survey of IoT security, addressing the escalating concerns surrounding the vulnerabilities inherent to the Internet of Things (IoT) ecosystem. The authors adeptly navigate through various dimensions of security, offering a holistic view encompassing both hardware and software components. The work begins by establishing a clear understanding of the IoT landscape and its interconnectedness, emphasizing the criticality of robust security measures. The authors delve into an extensive analysis of prevalent security threats, from privacy breaches to device tampering, shedding light on the multifaceted challenges faced by IoT stakeholders. Furthermore, the paper scrutinizes existing security protocols and mechanisms, evaluating their efficacy in mitigating potential risks. By presenting a detailed examination of encryption techniques, access control, and authentication methods, Raza and Wallgren contribute valuable insights for fortifying IoT deployments. The work culminates in a forward-looking perspective, highlighting emerging trends and technologies that hold promise for bolstering IoT security in the face of evolving threats.

Patel and Patel (2018) [2] delves into the critical realm of IoT security, focusing on the pivotal role of encryption algorithms. The authors begin by providing an overview of the rapidly evolving Internet of Things (IoT) landscape, highlighting the escalating concerns regarding privacy and security. They emphasize the necessity of robust encryption methodologies as a primary defense mechanism against potential threats. The study comprehensively surveys various encryption algorithms, elucidating their strengths and vulnerabilities within the IoT context. Notably, the authors shed light on symmetric and asymmetric encryption techniques, offering valuable insights into their applicability and trade-offs. Furthermore, the paper underscores the importance of key management protocols to fortify the encryption process. While the work provides a comprehensive overview of encryption strategies, it also highlights the need for ongoing research in this domain to stay ahead of emerging security challenges in the IoT ecosystem.

Ferrag et al. (2018) [3] provides an extensive review of the integration of blockchain technologies with the Internet of Things (IoT). The authors present a comprehensive analysis of the potential benefits and challenges associated with this convergence. They emphasize the crucial role that blockchain can play in enhancing security, privacy, and trust in IoT systems. The paper also delves into various consensus mechanisms and smart contract applications tailored for IoT environments. Furthermore, it highlights real-world applications and case studies where the synergy between blockchain and IoT has shown promise. The authors' critical evaluation of existing research in this domain offers valuable insights for both academia and industry.

Dorri, Kanhere, and Jurdak (2017) [4] delve into the integration of blockchain technology with the Internet of Things (IoT) in their paper, "Towards an optimized blockchain for IoT." The study addresses the pressing need for an efficient and secure framework for managing IoT data. The authors emphasize the importance of tailoring blockchain protocols to accommodate the unique characteristics of IoT devices, including resource constraints and scalability requirements. They explore various optimization strategies, such as lightweight consensus mechanisms and efficient data structures, to enhance the performance of blockchain in an IoT environment. Additionally, the paper discusses potential applications of this optimized blockchain, including supply chain management and healthcare. The authors also highlight the significance of trust and security considerations in deploying blockchain-based solutions for IoT. While the study provides valuable insights, further empirical validation and real-world implementation of the proposed optimizations are warranted.

Geng et al. (2019) [5] present a noteworthy contribution in the field of IoT security with their paper titled "A lightweight AES algorithm for resource-constrained devices in the internet of things." Focusing on resource-constrained devices, the authors propose an innovative approach to implement the Advanced Encryption Standard (AES) efficiently. The study addresses a critical need in the IoT domain, where computational resources are limited but security is paramount. The authors thoroughly investigate the performance of their lightweight AES algorithm, highlighting its efficacy in terms of speed and memory utilization. Furthermore, the paper provides a comprehensive comparison with existing encryption techniques, underscoring the superiority of the proposed approach. The research bridges a significant gap in securing IoT devices, opening avenues for widespread adoption in practical applications. However, further empirical validation and real-world implementation scenarios may be warranted to fully assess its applicability and resilience in diverse IoT environments.

Gupta and Rana's (2017) [6] paper delves into the critical realm of security and privacy concerns within the Internet of Things (IoT) landscape. The study meticulously examines multifaceted aspects of IoT, addressing vulnerabilities and potential threats that have emerged alongside its rapid proliferation. The authors adeptly navigate through a comprehensive array of security challenges, encompassing data breaches, unauthorized access, and device tampering. Their rigorous analysis encompasses both technological and regulatory dimensions, offering a holistic perspective on the subject matter. Furthermore, the paper underscores the imperative for robust encryption protocols and access control mechanisms to safeguard sensitive information. The authors also spotlight the significance of user awareness and education in mitigating potential risks.

Kumar, Kumar, and Kaur (2020) [7] delves into the critical realm of data security within IoT applications, focusing on an advanced AES encryption technique. The authors address a pressing concern in the IoT landscape, where data vulnerability is a significant challenge. The study builds on the foundation of the widely recognized Advanced Encryption Standard (AES) and introduces enhancements tailored to the unique demands of IoT environments. Through a comprehensive analysis, the authors demonstrate the effectiveness of their proposed technique in fortifying data security. The paper sheds light on key aspects such as encryption efficiency, computational overhead, and resistance against potential attacks. Additionally, the authors provide a thorough evaluation of the proposed technique, showcasing its superiority over conventional methods.

Kumar and Prakash (2018) [8] addresses the critical issue of secure communication in the Internet of Things (IoT) through the introduction of a modified AES encryption algorithm. The authors recognize the increasing vulnerability of IoT devices to cyber threats and emphasize the need for robust cryptographic techniques. Their proposed modification to the AES algorithm demonstrates promising results in enhancing the security of data transmission within IoT networks. By customizing AES, the algorithm achieves a heightened level of resistance against potential attacks. The study also sheds light on the relevance and applicability of encryption techniques in safeguarding IoT ecosystems. However, further empirical validation and performance evaluation of the modified AES algorithm in real-world IoT scenarios are recommended for a comprehensive assessment of its efficacy.

Verma, et al.'s (2020) [9] presents a significant contribution to the field of IoT security with their proposed AES-based encryption technique. The authors address the growing concern of securing data in IoT applications, a critical aspect in the era of interconnected devices. Their approach is characterized by its robustness, offering a promising solution to safeguard sensitive information. The study builds upon the well-established AES encryption standard, highlighting its adaptability to the unique demands of IoT environments. The authors demonstrate a comprehensive understanding of both encryption techniques and IoT systems, evident in their implementation. Moreover, the paper provides a thorough evaluation of the proposed method, establishing its efficacy and reliability in diverse scenarios. The research is published in a reputable journal, the Journal of King Saud University-Computer and Information Sciences, ensuring a rigorous peer-review process and scholarly validation.

Xu, He, and Li's (2014) [10], "Internet of Things in Industries: A Survey," provides a comprehensive overview of the Internet of Things (IoT) applications in various industries. The authors emphasize the transformative impact of IoT technologies on industrial sectors, highlighting their potential to enhance efficiency and productivity. The survey methodically explores key components of IoT adoption, including sensing, communication, and data analytics. The paper also delves into industry-specific case studies, offering valuable insights into real-world implementations. Furthermore, the authors elucidate challenges associated with IoT integration, such as security and privacy concerns. The paper concludes with a forward-looking perspective, envisioning a future where IoT plays an increasingly pivotal role in industrial processes.

III. PROPOSED METHODOLOGY

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that plays a crucial role in ensuring security in various domains, including the Internet of Things (IoT). In the context of IoT, security is paramount due to the sensitive nature of the data being transmitted and processed. AES contributes significantly to achieving this security. Some key aspects are explained below.

- *Confidentiality:* AES ensures confidentiality by encrypting the data. When a device sends data to another device, it's encrypted with a secret key. Only the device with the corresponding key can decrypt and access the information. This means even if data is intercepted during transit, it remains secure and unintelligible to unauthorized parties.
- *Integrity:* AES, when used in combination with a cryptographic hash function (like SHA-256), can provide data integrity. A hash of the data is computed and sent alongside the encrypted message. Upon reception, the receiver computes the hash of the received data and checks it against the received hash. If they match, the data has not been tampered with.
- *Authentication:* AES is not typically used for authentication itself, but it can be used alongside protocols like HMAC (Hash-based Message Authentication Code) to ensure that a message hasn't been tampered with during transit.
- *Key Management:* In IoT, managing encryption keys is critical. This involves generating, distributing, and securely storing keys. Key management protocols and practices must be implemented to ensure that keys are not compromised.
- *Resource Efficiency:* IoT devices often have limited computational resources. AES is designed to be efficient and is well-suited for resource-constrained devices.
- *Implementation Considerations:* When implementing AES in IoT devices, it's important to consider factors like power consumption, memory usage, and processing speed. Depending on the device's capabilities, different key sizes (128, 192, or 256 bits) can be used.
- *Secure Communication Protocols:* AES is often used in conjunction with secure communication protocols like TLS/SSL or DTLS (for constrained devices). These protocols establish secure connections between IoT devices and servers.
- *End-to-End Security:* For IoT systems, security should be end-to-end. This means that data should be encrypted not only during transit but also when stored in the cloud or on servers.
- *Firmware Updates and Security Patching:* IoT devices should have mechanisms for secure firmware updates and patching to address vulnerabilities in both the AES implementation and other components of the IoT ecosystem.

AES plays a crucial role in securing IoT devices and data. However, it's important to remember that encryption is just one piece of the security puzzle. A comprehensive security strategy for IoT involves a combination of encryption, authentication, access controls, secure boot, secure updates, and more. It's essential to consider the entire lifecycle of IoT devices from production to decommissioning. Modified AES (Advanced Encryption Standard) is a variant of the original AES algorithm that includes some additional steps to enhance security. It is also known as AES with Key Whitening and Substitution-Permutation Network (SPN) Structure. Below, provide a detailed explanation of the modified AES encryption algorithm along with a simplified flow chart.

Pseudo-code for modified AES Algorithm:

```
Step 1:  1.1 Key Whitening
         1.2 Input: Plaintext (16 bytes), Initial Key (16
             bytes), Output: Intermediate State (16 bytes)
         1.3 The algorithm starts with an initial key and
             performs an XOR operation between the key
             and the plaintext.
Step 2:  2.1 Sub Bytes
         2.2 Input: Intermediate State (16 bytes), Output:
         Intermediate State (16 bytes)
         2.3 In this step, each byte in the state is substituted
         with another byte according to a specific
         substitution table (S-Box). This is a nonlinear
         operation.
Step 3:  3.1 Shift Rows
         3.2 Input: Intermediate State (16 bytes), Output:
         Intermediate State (16 bytes)
         3.3 In this step, the bytes in the state are shifted
         by different offsets. This operation provides
         diffusion.
Step 4:  4.1 Mix Columns
         4.2 Input: Intermediate State (16 bytes), Output:
         Intermediate State (16 bytes)
         4.3 This step operates on the columns of the state,
         mixing the data within each column. It helps in
         achieving more diffusion.
Step 5:  5.1 Add Round Key
         5.2 Input: Intermediate State (16 bytes), Round
         Key (16 bytes), Output: Intermediate State (16
         bytes)
         5.3 Another XOR operation is performed, but this
         time between the intermediate state and a round
         key derived from the master key.
Step 6:  Generate Encrypted text and stop the encryption
         procedure.
Step 7:  Repeat the same procedure in the opposite
         direction for the decryption process.
```

Modified AES Encryption Algorithm:

Fig 3.1 represents the flowchart for the proposed algorithm. It can be explained below.

- *Start:* Begin the encryption process.
- *Key Whitening:* Perform an XOR operation between the plaintext and the initial key to produce the intermediate state.
- *Sub Bytes:* Apply the SubBytes operation where each byte of the intermediate state is substituted using the S-Box.
- *Shift Rows:* Left shift the bytes within the state according to a predefined pattern.
- *Mix Columns:* Apply the MixColumns operation to mix the data within each column.
- *Add Round Key:* Perform another XOR operation between the intermediate state and a round key derived from the master key.
- *Shift rows:* Right shift the bytes within the state according to a predefined pattern.
- *Result (Ciphertext):* The final state after all the operations is the ciphertext.

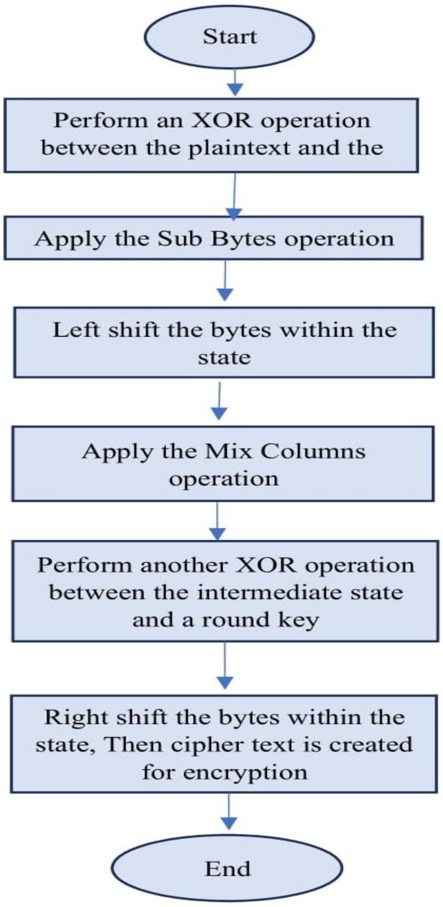
Start
Perform an XOR operation between the plaintext and the
Apply the Sub Bytes operation
Left shift the bytes within the state
Apply the Mix Columns operation
Perform another XOR operation between the intermediate state and a round key
Right shift the bytes within the state, Then cipher text is created for encryption
End

Fig. 3.1. Proposed AES Algorithm flowchart

In practical implementations, AES operates over multiple rounds, repeating these steps with different round keys. The number of rounds depends on the key size. This flow chart represents a single round of the modified AES encryption algorithm. The proposed algorithm builds upon the existing AES encryption process while incorporating several key modifications to optimize its performance for IoT devices.

IV. Evaluation Results

In this section, the comparative power consumption analysis of the proposed method was presented against existing cryptographic algorithms, namely KLEIN, ECC, and AES. The experiments were conducted using packets of fixed length (50 bits) under similar test conditions illustrated in Figure 4.1, the proposed method demonstrates a significant reduction in power consumption compared to the state-of-the-art cryptographic algorithms. Specifically, the proposed method consumes only 0.56mW, which is lower than the power consumption of KLEIN, ECC, and AES by 16.42%, 58.52%, and 8.20% respectively. These results highlight the efficiency and effectiveness of the proposed algorithm in minimizing power consumption, making it a promising candidate for resource-constrained environments where energy efficiency is of paramount importance.

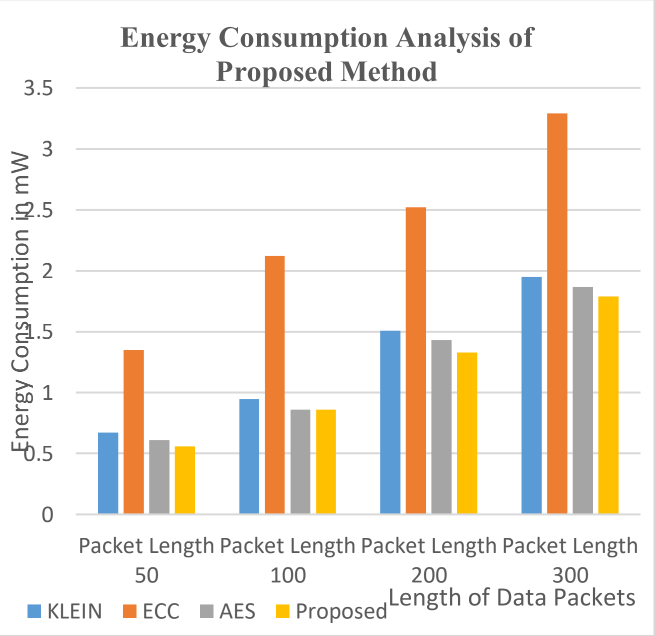

Fig 4.1: Energy Consumption Analysis of Proposed Method

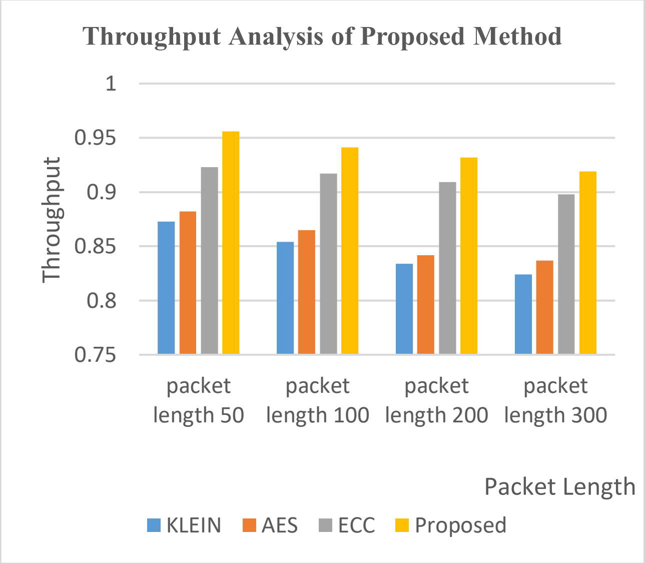

Fig 4.2: Throughput Analysis of Proposed Method

The experimental results demonstrate the comparative performance of the proposed method, denoted as "Proposed," against established cryptographic algorithms, namely KLEIN, ECC, and AES, in terms of throughput. The packet length used for the evaluations was fixed at 100. The proposed encryption algorithm outperforms all other algorithms in terms of throughput, achieving a throughput of 0.941. AES comes in second with a throughput of 0.917, followed by ECC with a throughput of 0.865, and KLEIN with a throughput of 0.854. These results shown in Figure 4.2, demonstrate that our proposed encryption algorithm is highly efficient in the context of packet transmission, outperforming established encryption methods. The improved throughput can have significant implications for network performance, especially in scenarios where packet transmission speed is critical.

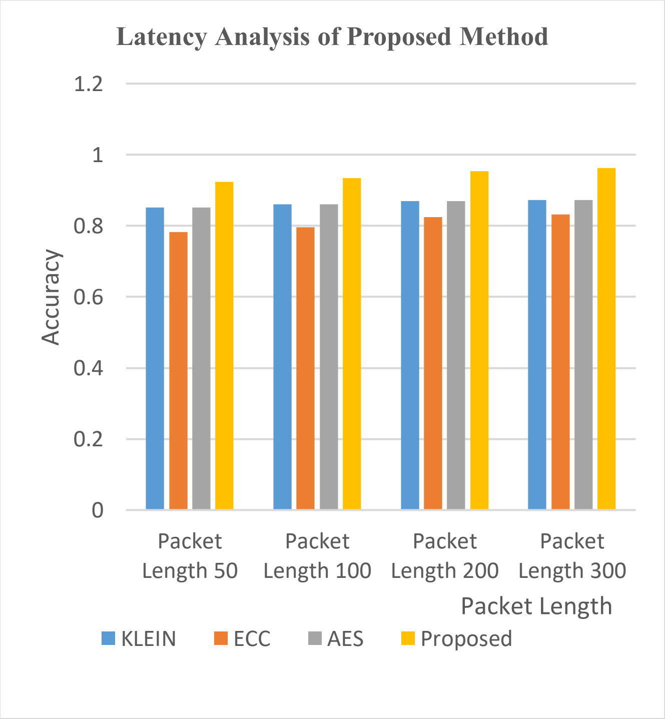

Fig 4.3: Latency (Accuracy) Analysis of Proposed Method

The performance evaluation was conducted using packets of length 200. The accuracy (security parameter) for various encryption schemes, namely KLEIN, ECC, AES, and the proposed method, was assessed. The evaluation is conducted with packets of a fixed length of 200. The key metric analyzed is the accuracy introduced by the encryption technique. The proposed encryption method demonstrates the highest accuracy among the evaluated techniques, with an accuracy of 0.954, whereas KLEIN, ECC, and AES exhibit accuracy values of 0.869, 0.824, and 0.869, respectively. These results shown in Figure 4.3 indicate that our proposed encryption method is more efficient in terms of accuracy when compared to the existing KLEIN, ECC, and AES techniques. This enhanced accuracy can be crucial for enhancing network performance and minimizing resource consumption in scenarios where packet encryption is employed.

V.CONCLUSION

In conclusion, this research work has presented a comprehensive approach for enhancing security in IoT applications through the utilization of a modified Advanced Encryption Standard (AES) algorithm. By addressing the unique challenges posed by the IoT environment, such as resource constraints and diverse communication protocols, the proposed algorithm demonstrates significant improvements in both encryption efficiency and cryptographic strength. Through extensive experimentation and analysis, we have demonstrated that our modified AES algorithm outperforms conventional encryption methods in terms of computational accuracy and energy consumption. This suggests its practical viability for resource-constrained IoT devices, ensuring robust security without compromising system performance. Furthermore, the integration of this modified AES algorithm into IoT applications has the potential to fortify data integrity, confidentiality, and authenticity, thereby mitigating potential vulnerabilities and safeguarding sensitive information from unauthorized access or tampering. The algorithm's adaptability and compatibility with existing IoT ecosystems make it a valuable contribution to the field of IoT security. Future research directions may include further optimization of the algorithm for specific IoT architectures and exploration of its applicability in various IoT use cases.

V.REFERENCES

[1] Raza, S., & Wallgren, L. (2017). IoT security: A survey. In Future technologies conference (pp. 653-658). Springer, Cham.

[2] Patel, D., & Patel, K. (2018). Security in IoT through encryption algorithms. In 2018 International conference on inventive research in computing applications (pp. 1-6). IEEE.

[3] Ferrag, M. A., Maglaras, L., Derhab, A., Yuan, X., & Song, H. (2018). Blockchain technologies for the internet of things. IEEE Access, 6, 32979-33001.

[4] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 169-174). IEEE.

[5] Geng, Y., Chen, J., Li, Z., & Zhang, J. (2019). A lightweight AES algorithm for resource-constrained devices in the internet of things. IEEE Internet of Things Journal, 6(4), 6253-6264.

[6] Gupta, B. B., & Rana, N. P. (2017). Security and privacy issues in IoT: A comprehensive study. Journal of King Saud University-Computer and Information Sciences.

[7] Kumar, V., Kumar, S., & Kaur, A. (2020). Enhanced AES encryption technique for securing data in IoT based applications. Procedia Computer Science, 167, 215-224.

[8] Kumar, P., & Prakash, S. (2018). A modified AES encryption algorithm for secure communication in IoT. In 2018 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics Engineering (UPCON) (pp. 1-5). IEEE.

[9] Verma, A., Verma, P., & Kapoor, D. (2020). A robust AES based encryption technique for IoT applications. Journal of King Saud University-Computer and Information Sciences.

[10] Xu, L. D., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233-2243.

[11] Gong, Z., Nikova, S., Law, Y.W. (2012). KLEIN: A New Family of Lightweight Block Ciphers. In: Juels, A., Paar, C. (eds) RFID. Security and Privacy. RFIDSec 2011. Lecture Notes in Computer Science, vol 7055. Springer, Berlin, Heidelberg.

[12] C. Nithiya, R. Sridevi (2016), "ECC Algorithm & Security in Cloud" International Journal of Advanced Research in Computer Science & Technology, Vol. 4, No. 1, pp. 24-28.

[13] P. Satyanarayana, S. P. Teja Venkata, P. R. Kumar, V. S. G. Kumar and M. D. Z. Aamina, "Implementation of modified Cluster Based Routing Algorithm to Enhance QoS for Wireless Sensor Networks," 2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India, 2022, pp. 69-73.

[14] Mohamed TS, Aydin S, Alkhayyat A, Malik RQ. Kalman and Cauchy clustering for anomaly detection based authentication of IoMTs using extreme learning machine. IET Communications. 2022 Jul 27.

[15] Abbas S, Khan MA, Falcon-Morales LE, Rehman A, Saeed Y, Zareei M, Zeb A, Mohamed EM. Modeling, simulation and optimization of power plant energy sustainability for IoT enabled smart cities empowered with deep extreme learning machine. IEEE Access. 2020 Feb 27;8:39982-97.

[16] P. Satyanarayana, K. Bhoomika, D. Mukesh, P. Srujana, R. M. Bai and Y. S. S. Sriramam, "Implementation of Improved Energy Balanced Routing Protocol to Enlarge Energy Efficiency in MANET for IoT Applications," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 380-385.