ISSN: 2633-4828 Vol. 5 No. S4 (July-Aug 2023)

International Journal of Applied Engineering & Technology

SECURING IOT NETWORKS WITH DUPLEX COMMUNICATION

Sadiya Begum [1], Dr. Mukesh Tiwari [2]

[1] Research Scholar, Department of Electronics and Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences (SSSUTMS), Sehore, Madhya Pradesh, India

[2] Research Guide, Department of Electronics and Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences (SSSUTMS), Sehore, Madhya Pradesh, India

Abstract

Security has emerged as a critical concern across various sectors, prompting the adoption of robust communication protocols like AESCQTTP (Advanced Encryption Standard Constrained Queuing Telemetry Transport Protocol) in IoT devices. This protocol ensures the confidentiality, integrity, and authenticity of transmitted data by leveraging AES encryption and optimized queuing mechanisms. The Integrated AESCQTTP framework offers a comprehensive solution to the challenges posed by resource-constrained IoT environments, securing data transmission from sensing to application layers. Through algorithmic implementation and duplex operation, AESCQTTP facilitates bidirectional communication between IoT devices and servers, ensuring secure data transfer. Our results demonstrate the protocol's efficiency in maintaining stable throughput and enhancing security integrity across networks of varying sizes, outperforming existing protocols like COAP and AES. AESCQTTP represents a significant advancement in securing IoT ecosystems, enabling organizations to embrace connectivity without compromising data protection.

Keywords: *AESCQTTP, AES encryption, COAP, IoT.*

INTRODUCTION

The concept of IoT pertains to the network comprising linked devices and the technology enabling interaction among devices, both with the cloud and amongst each other. A customary IoT System operates by continuously gathering and sharing data instantly. This system encompasses three essential constituents:

- Smart Devices
- IoT Applications
- A Graphical User Interface

Illustrations include Connected Cars, Smart Homes, and similar instances. IoT Devices encompass a broad range of internet-connected devices such as Smart TVs, Smart Watches, and Alexa devices.

The vast majority of RFID tags and wireless sensors, which are examples of widely dispersed Internet of Things devices, are located in public spaces. That makes it harder to manage and makes these gadgets more susceptible to physical attacks. The existence of an unattended environment for IoT devices has made data integrity an issue [4]. When all systems are up and running, the majority of devices operate independently. Data manipulation occurs more sooner than in a supervised wired network since almost little maintenance is necessary. The devices and the gateway communicate with one another over a wireless manner. For this reason, data secrecy is jeopardized. Eavesdropping is one example of a serious problem that can develop in wireless networks. Ensuring the privacy of transmitted data is not an easy task because most Internet of Things (IoT) devices are resource-constrained low-end devices. There is a risk of data leakage when Internet of Things (IoT) networks are linked to the internet for the purpose of monitoring and interacting with the physical environment [5]. By establishing connections between physical things and data stored online, the information might potentially be accessible to a wide range of online entities. The secure access protocol allows for two routes of communication between mobile devices and gateways. The IP-based backbone receives data transmitted by the gateway, which in turn receives it from the mobile devices.

Data transmission to service platforms will be facilitated by the IP-based backbone. In order to ensure that mobile devices and gateways can communicate securely in both directions, the Diffie-Hellman algorithm is used [6].

APPLICATIONS OF IOT

View some of the practical Internet of Things (IoT) uses that have improved our lives. For those interested in writing a thesis on the Internet of Things (IoT), this subtopic of applications is a good place to start (Internet of Things). In the future, this field will continue to reveal additional surprises. See how the Internet of Things is being used in the actual world.

- **Smart Homes –** Internet of Things smart homes are currently all the rage. There is a lot of interest in this feature. In an effort to improve the quality of their lives, they are considering having their houses upgraded to smart homes. Who among us wouldn't desire a house that can sense the temperature and turn the heat or lights on and off automatically? Time, money, and energy savings are the three main goals of smart home products. Just like cellphones, smart houses will soon be ubiquitous.
- **Wearable gadgets –** The market for wearable internet of things devices is booming. With the help of built-in sensors and software, these wearable IoT devices may gather important user data, which, when processed, can provide vital insights. The primary functions of these devices are related to health, exercise, and entertainment. The primary benefit of these devices is their compact size, exceptional efficiency, and minimal power consumption.
- **Connected Cars –** For the convenience of its passengers, these autonomous vehicles can operate and maintain themselves with the help of sensors and internet connectivity. A number of well-known companies are aiming to revolutionize vehicle systems in this way.
- **Industries –** The topic of the industrial internet is now trending. With the use of sensors, software, and analytics, it hopes to equip companies to produce smarter, more sophisticated machinery. Among the many benefits, quality assurance, environmental friendliness, product tracking, and the capacity to share data in real time stand out.
- **Smart Cities –** The Internet of Things (IoT) has expanded its uses beyond smart homes to smart cities. What exactly does a "smart city" consist of? Enlightened monitoring of the environment, smart surveillance, automated transportation management, energy distribution, and water storage. People who live in cities often encounter issues like traffic, pollution, and more, but the Internet of Things (IoT) promises to fix all of them.
- **Agriculture –** An ever-increasing human population means a greater need for food. When it comes to agriculture, the Internet of Things often leads to the development of specific methods that boost food production. In addition, farmers can gain valuable knowledge on soil conditions, moisture needs, and more.
- **Energy –** Global interest in the smart grid concept is growing. It measures customer electricity use and tries to enhance electricity efficiency.
- **Healthcare** – Individual health records will soon be able to be gathered by smart healthcare systems. Its goal is to help people live longer, healthier lives.

What sets full duplex apart from other technologies?

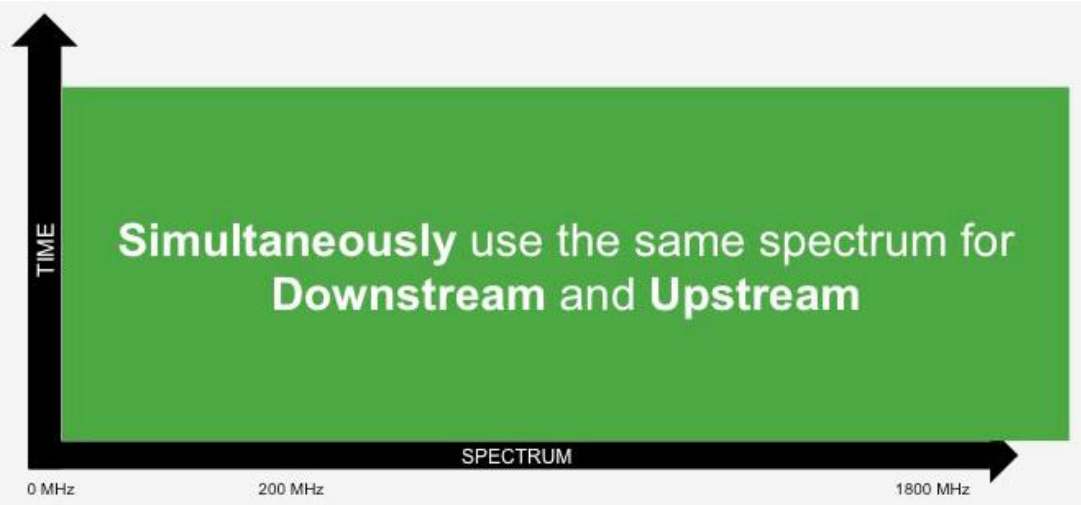

Figure 1: *Full Duplex DOCSIS*

A Full Duplex DOCSIS 3.1 network, which is now DOCSIS 4.0 technology, offers a solid basis for the next generation of HFC distribution, which is one of its appealing qualities. Through careful planning and study, we have determined that the current DOCSIS 3.1 Physical and MAC layer protocols are more than capable of supporting this new symmetric service. An incremental improvement of DOCSIS 3.1 technology, the DOCSIS 3.1 Full Duplex network that is now a component of DOCSIS 4.0 technology will allow for the continued use of older DOCSIS networks while also being compatible with newer ones.

RESEARCH METHODOLOGY

Security has taken the spotlight in strategic applications across diverse sectors such as defense, automotive, healthcare, education, and more. The need to safeguard transmitted data has become paramount, prompting the implementation of secure communication protocols like AESCQTTP (Advanced Encryption Standard Constrained Queuing Telemetry Transport Protocol) for IoT devices.

In today's interconnected world, where information flows incessantly between devices, ensuring the confidentiality, integrity, and authenticity of data is crucial. AESCQTTP steps in as a robust solution, leveraging the Advanced Encryption Standard to encrypt data effectively. By integrating constrained queuing mechanisms, it optimizes resource usage while maintaining security standards, making it suitable for the resource-constrained environments often found in IoT devices.

This protocol not only secures data transmission but also addresses the challenges posed by the limitations of IoT devices, such as restricted processing power and memory. Through its efficient queuing system, AESCQTTP manages data flow intelligently, mitigating the risk of data loss or compromise.

In essence, AESCQTTP represents a significant advancement in ensuring the security of IoT ecosystems, providing a reliable framework for transmitting sensitive information across various applications. Its adoption underscores the growing recognition of security as a critical component of modern technology, empowering organizations to embrace the benefits of connectivity without sacrificing data protection.

In IoT devices, data is gathered by either sensing or observing the designated area of interest. This collected information is then transmitted to a server in the form of packets, which essentially means that the data is divided into various segments for transmission. These packets travel through the network, forming multiple nodes, and are queued in the QTTP (Quantum Transport Protocol) before reaching the server. Once received, the data is accumulated at the application layer, where it can be further utilized.

The novelty of the proposed Integrated AESCQTTP framework lies in its approach to secure and efficient data transmission within the IoT ecosystem. AES (Advanced Encryption Standard) ensures that the data is encrypted before transmission, enhancing security and protecting sensitive information from unauthorized access. The integration of AES with QTTP optimizes the data transfer process, enabling smoother communication between IoT devices and the server.

This framework addresses the critical concerns of data security and transmission efficiency in IoT environments, offering a comprehensive solution for managing and utilizing data effectively. By combining encryption with a robust transport protocol, the Integrated AESCQTTP framework provides a reliable foundation for IoT applications, ensuring the integrity and confidentiality of data throughout its journey from sensing to application. Figure 1 illustrates the framework's architecture, highlighting the interconnectedness of nodes, encryption keys, and data transmission, emphasizing the importance of encryption in safeguarding sensitive information.

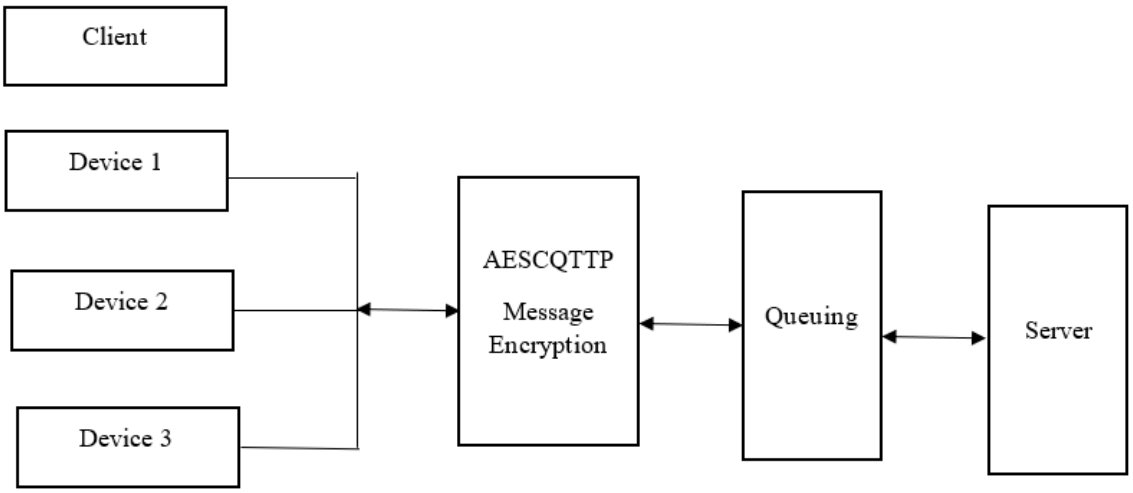

Figure 1. Proposed Framework

In this framework, an IoT device is deployed to gather data from its surrounding environment. Once the data is collected, the IoT device sends it out. At this point, the framework comes into play. Upon reception of the data from the IoT device, a predefined bit size is chosen for encryption keys. These keys are specifically tailored for AESCQTTP encryption.

After determining the appropriate key size, encryption keys are generated to secure the data. Once encrypted, the data is then directed to a queuing system for further processing. This queuing system serves as an intermediate step before the encrypted data reaches the final destination: the server.

By encrypting the data before transmission, this framework ensures the security and integrity of the information gathered by the IoT device. It establishes a structured process to safeguard sensitive data while facilitating its seamless transfer to the server for analysis or storage.

Algorithm

Let D represent the data collected by the IoT device, K be the set of predefined encryption key sizes, E_k denote the encryption function with key k, and De represent the encrypted data.

Initialization:

- $K=\{k_1,k_2,...,k_n\}$ (Set of predefined encryption key sizes).
- Server S and Client C.

Data Collection:

- D = Data collected by the IoT device.
- Transmit (D) = Transmit data to the server.

Data Reception and Encryption:

- k_i = Selection of encryption key size from *K*.
- k_i = Pre-defined Bit Sizes [*i*].
- k_i = Select Key Size(*K*).
- $E_{ki}(D)=D_e$ (Encrypt the data using key k_i).

Authentication and Transmission:

- Utilize FIFO algorithm for authentication.
- Master Encryption=$E_{ki}(M)$ (Encrypt message *M* with key k_i).
- Transmit (Master Encryption) Transmit (Master Encryption).

Decryption and Response:

- $D_r=E_{ki}^{-1}(D_e)$ (Decrypt received data D_e using key k_i).
- Response=Process(D_r).

Response Encryption and Transmission:

- Encrypted Response=E_{ki}(Response).
- Transmit (Encrypted Response).

Decryption and Processing:

- Decrypted Response=E_{ki}^{-1}(Encrypted Response).
- Process (Decrypted Response).

Repeat:

- Repeat steps 2-7 for continuous bidirectional communication between the client and server.

The AESCQTTP concept enables secure bidirectional communication between the host and IoT devices by employing a duplex mode. It operates on a server-client model where the server acts as the master to encrypt messages in real-time, utilizing a FIFO algorithm for authentication. This authentication mechanism ensures secure data transmission, with the IoT node serving as an intelligent gateway, facilitating requests and responses between client and server domains. Overall, AESCQTTP enhances data security within the IoT ecosystem, protecting sensitive information from unauthorized access.

RESULT AND DISCUSSION

According to the provided data, the AESCQTTP throughput shows an intriguing trend within IoT networks. Initially, with 2 nodes, the throughput stands at approximately $2.6x10^3$ Kbps. As the network expands to include 4 nodes, a modest increase to about $2.62x10^3$ Kbps is observed. Interestingly, this trend continues as the network further scales, reaching approximately $2.63x10^3$ Kbps for both 6 and 8 nodes.

This progression suggests a relatively stable throughput performance despite the increase in the number of nodes. Such consistency can be indicative of efficient network management or effective utilization of resources within the

IoT infrastructure. Additionally, it underscores the network's capability to accommodate higher node counts without significant degradation in throughput, which is crucial for sustaining reliable data transmission and communication in IoT environments.

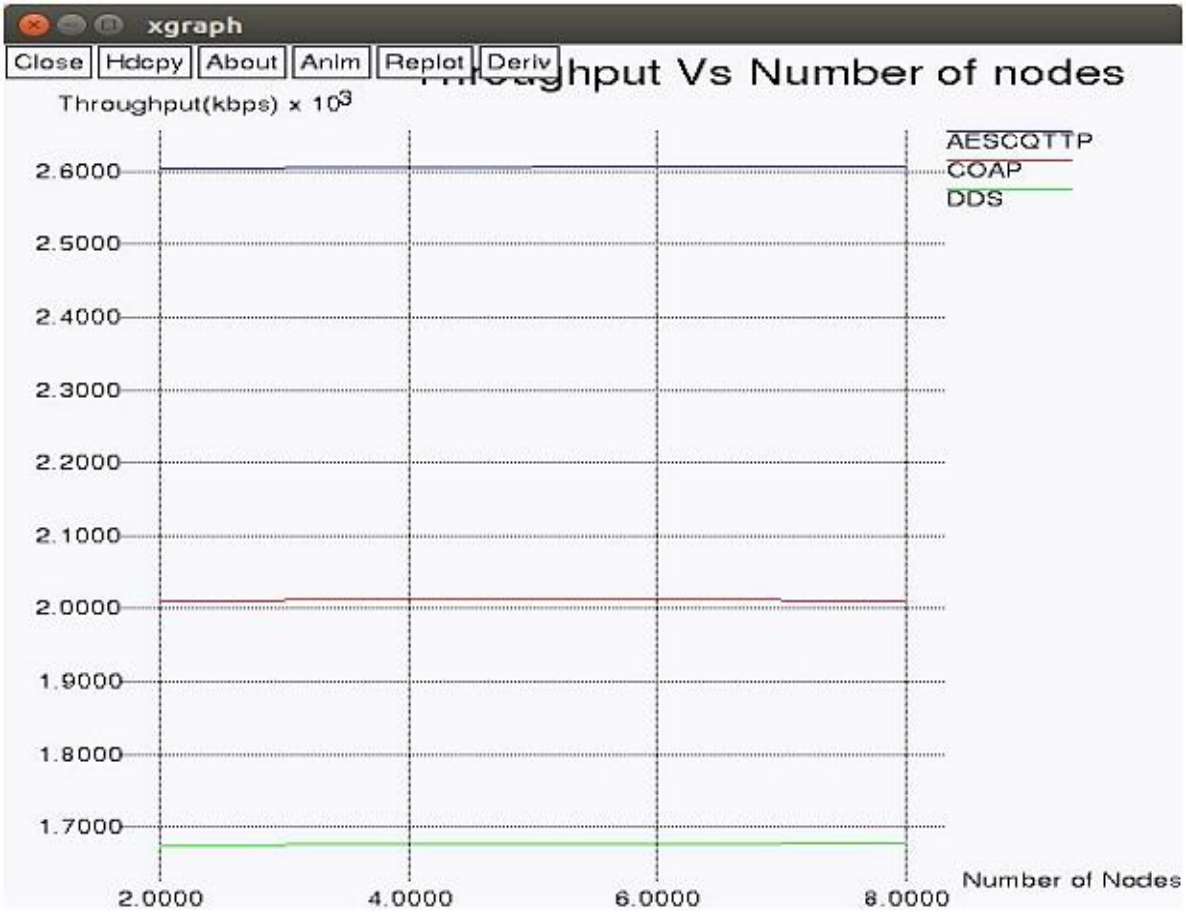

Figure 2. Node Scaling Effects on AESCQTTP Throughput in IoT Networks

The Advanced Encryption Standard for IoT Communication with Quantum Trusted Third Party (AESCQTTP) protocol's security has been tested in an IoT setting with networks of different sizes. The results demonstrate a significant enhancement in security compared to existing protocols, as shown in Figure 3.

Initially, with only two nodes in the IoT network, AESCQTTP achieves a commendable security level of 95%. As the network expands to four nodes, the security further improves to 95.8%, indicating the scalability and robustness of the protocol.

As the network continues to grow, with six and eight nodes, the security levels rise to 96.25% and 97.60%, respectively. This demonstrates the protocol's effectiveness in maintaining security integrity even as network complexity increases.

Comparative analysis, as shown in Figure 4, with established protocols such as COAP (Constrained Application Protocol) and AES (Advanced Encryption Standard), reveals the clear superiority of AESCQTTP. While COAP and AES offer security levels of 94.3% and 94.20%, respectively, AESCQTTP achieves an impressive security rating of 97.47%. This significant margin underscores the advancements brought forth by AESCQTTP in securing IoT communications.

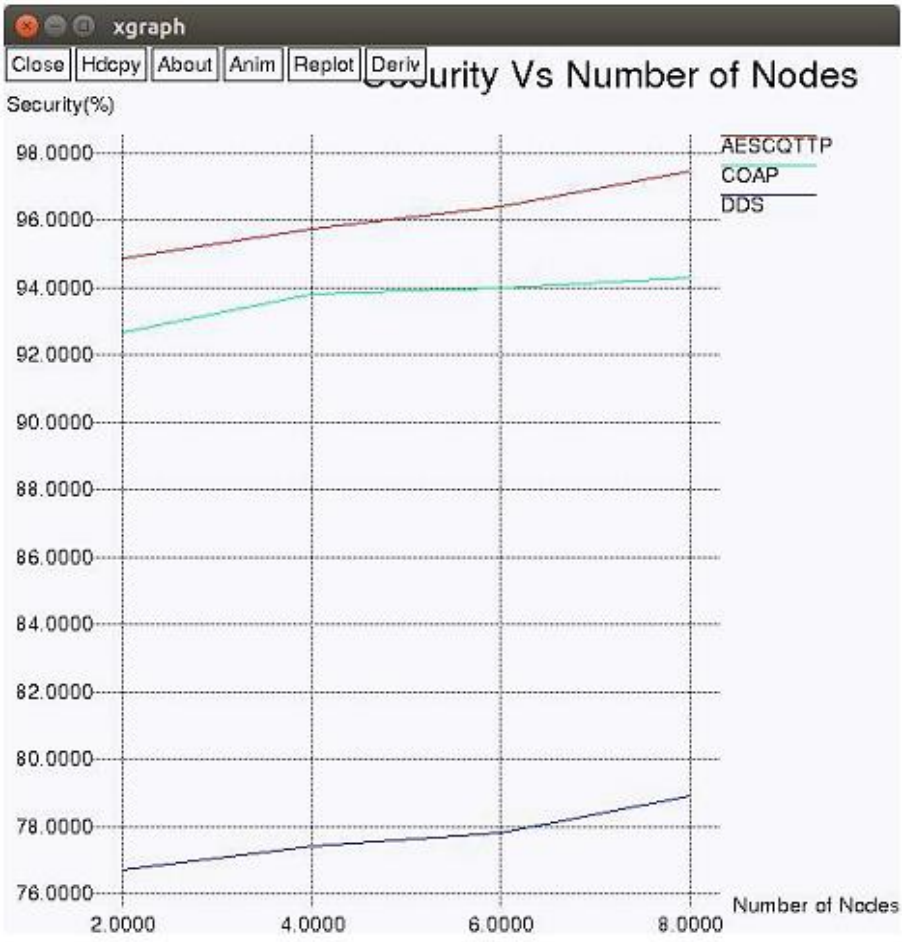

Figure 3. Enhancing IoT Security: AESCQTTP Protocol Evaluation across Node Networks

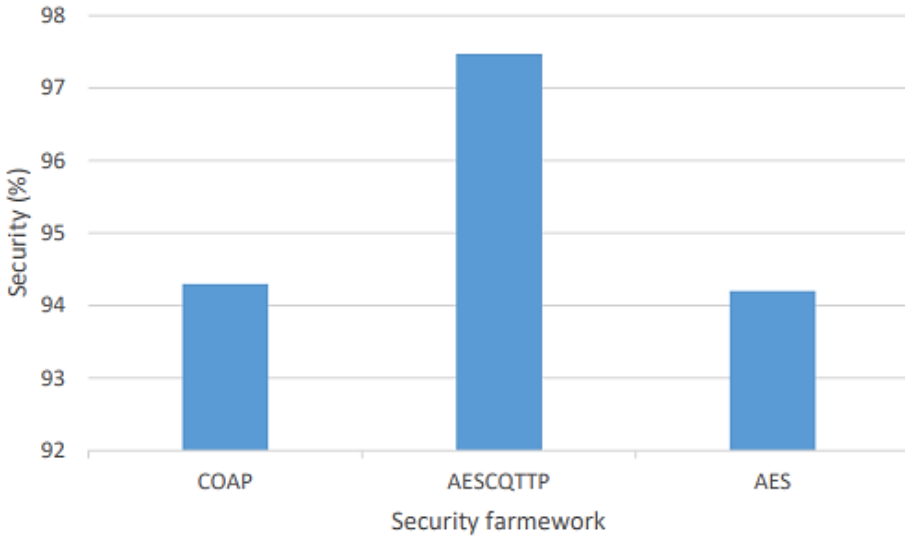

Figure 4. Security for COAP, AES, AESCQTTP

CONCLUSION

The Integrated AESCQTTP Framework presents a novel approach to secure and efficient data transmission in IoT environments. By integrating AES encryption with optimized queuing mechanisms, the framework addresses the critical challenges of data security and transmission efficiency, offering a reliable foundation for IoT applications. Through algorithmic implementation and duplex operation, AESCQTTP enables bidirectional communication, enhancing security integrity across networks of different sizes. Comparative analysis demonstrates the protocol's superiority over existing protocols, highlighting its effectiveness in securing IoT communications. Overall, AESCQTTP represents a significant advancement in ensuring the confidentiality, integrity, and authenticity of data in IoT ecosystems, paving the way for secure and interconnected applications across diverse sectors.

REFERENCES

[1] Pedro Miguel Sánchez Sánchez, et al (2024), "Adversarial attacks and defenses on ML- and hardware-based IoT device fingerprinting and identification," Future Generation Computer Systems, Volume 152, 2024, Pages 30-42, ISSN 0167-739X, https://doi.org/10.1016/j.future.2023.10.011.

[2] Parjanay Sharma, et al (2021), "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," Ad Hoc Networks, Volume 123, 2021, 102685, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2021.102685.

[3] Abhishek Gupta, et al (2019), "RETRACTED: Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: A survey," Journal of Network and Computer Applications, Volume 132, 2019, Pages 118-148, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2019.01.012.

[4] Fadi Al-Turjman, et al (2020), "UAVs assessment in software-defined IoT networks: An overview," Computer Communications, Volume 150, 2020, Pages 519-536, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2019.12.004.

[5] Khizar Hameed, et al (2022), "A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues," Journal of Industrial Information Integration, Volume 26, 2022, 100312, ISSN 2452-414X, https://doi.org/10.1016/j.jii.2021.100312.

[6] Weiping Ding, et al (2024), "DeepSecDrive: An explainable deep learning framework for real-time detection of cyberattack in in-vehicle networks," Information Sciences, Volume 658, 2024, 120057, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2023.120057.

[7] Sara Aboukadri, et al (2024), "Machine learning in identity and access management systems: Survey and deep dive," Computers & Security, Volume 139, 2024, 103729, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.103729.

[8] A.G. Sreedevi, et al (2022), "Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review," Information Processing & Management, Volume 59, Issue 2, 2022, 102888, ISSN 0306-4573, https://doi.org/10.1016/j.ipm.2022.102888.

[9] Mohammed Banafaa, et al (2023), "6G Mobile Communication Technology: Requirements, Targets, Applications, Challenges, Advantages, and Opportunities," Alexandria Engineering Journal, Volume 64, 2023, Pages 245-274, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2022.08.017.

[10] Pietro Boccadoro, et al (2021), "An extensive survey on the Internet of Drones," Ad Hoc Networks, Volume 122, 2021, 102600, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2021.102600.

[11] Sarina Aminizadeh, et al (2024), "Opportunities and challenges of artificial intelligence and distributed systems to improve the quality of healthcare service," Artificial Intelligence in Medicine, Volume 149, 2024, 102779, ISSN 0933-3657, https://doi.org/10.1016/j.artmed.2024.102779.

[12] Pedro Miguel Sánchez Sánchez, et al (2024), "Single-board device individual authentication based on hardware performance and autoencoder transformer models," Computers & Security, Volume 137, 2024, 103596, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103596.

[13] Chunyan Li, Jiaji Wang, et al (2024), "A review of IoT applications in healthcare,

[14] Neurocomputing," Volume 565, 2024, 127017, ISSN 0925-2312, https://doi.org/10.1016/j.neucom.2023.127017.

[15] Yassine Himeur, et al (2024), "Edge AI for Internet of Energy: Challenges and perspectives," Internet of Things, Volume 25, 2024, 101035, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.101035.

[16] Mohammad Hosein Panahi Rizi, et al (2022), "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," Internet of Things, Volume 20, 2022, 100584, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.100584.

[17] Hamed Alqahtani, et al (2024), "Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems," Engineering Applications of Artificial Intelligence, Volume 129, 2024, 107667, ISSN 0952-1976, https://doi.org/10.1016/j.engappai.2023.107667.

[18] Ruiyun Yu, et al (2023), "Blockchain-based solutions for mobile crowdsensing: A comprehensive survey," Computer Science Review, Volume 50, 2023, 100589, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2023.100589.

[19] Rakesh Kumar, et al (2019), "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," Computer Science Review, Volume 33, 2019, Pages 1-48, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2019.05.002.

[20] Tawseef Ayoub Shaikh, et al (2023), "Machine intelligence and medical cyber-physical system architectures for smart healthcare: Taxonomy, challenges, opportunities, and possible solutions," Artificial Intelligence in Medicine, Volume 146, 2023, 102692, ISSN 0933-3657, https://doi.org/10.1016/j.artmed.2023.102692.

[21] Abderahman Rejeb, et al (2024), "Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions," Internet of Things and Cyber-Physical Systems, Volume 4, 2024, Pages 1-18, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2023.06.003.

[22] Hadi Habibzadeh, et al (2018), "Sensing, communication and security planes: A new challenge for a smart city system design," Computer Networks, Volume 144, 2018, Pages 163-200, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2018.08.001.

[23] Antonio Petrosino, et al (2023), "Light Fidelity for Internet of Things: A survey," Optical Switching and Networking, Volume 48, 2023, 100732, ISSN 1573-4277, https://doi.org/10.1016/j.osn.2023.100732.

[24] Prabhakar Krishnan, et al (2024), "eSIM and blockchain integrated secure zero-touch provisioning for autonomous cellular-IoTs in 5G networks," Computer Communications, Volume 216, 2024, Pages 324-345, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2023.12.023.

[25] Keyvan Ramezanpour, et al (2023), "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," Computer Networks, Volume 221, 2023, 109515, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2022.109515.

[26] Chen Wang, et al (2023), "Network approaches in blockchain-based systems: Applications, challenges, and future directions," Computer Communications, Volume 212, 2023, Pages 141-150, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2023.09.018.