

Mitigating IoT Network Penetration using the Internet Protocol Security Algorithm through Artificial Intelligence Edge

MUSTAFA K. ATI
Misan Governorate,
IRAQ

Abstract: - The global Internet of Everything is rapidly spreading, connecting every aspect from smart houses to household machinery. These devices exposed significant security threats due to hacker attacks, including stolen data and infection. Older security solutions are insufficient to prevent contemporary attacks. IoT is secure with artificial intelligence. Artificial intelligence (AI) detects hazards, analyzes risks, and responds automatically. This article explores modern technology in IoT security, its relationship with blockchain, and its problems and improvements in the security and reliability of IoT devices in the digital era. This study offers substantial insights into the establishment of reliable and secure IoT systems through a proposed algorithm called the Internet Protocol Security (IPsec) algorithm, which works using this technology and a modern communication protocol that is characterized by speed, accuracy, and security in transmitting information, with the protocol being encrypted in the Encapsulating Security Payload (ESP) method and the possibility of developing this algorithm to counter any attack, and with various modern methods using advanced communication devices.

Key-Words: - Intelligent Computing (IC), Cyber Risks, Artificial Intelligence Edge, Internet of thing (IoT), IoT Protection, Risk Evaluation.

Received: March 13, 2026. Revised: May 15, 2026. Accepted: June 11, 2026. Published: October 23, 2026.

1 Introduction

The Global Internet of Things (IoT) has experienced significant expansion in recent years, revolutionizing multiple sectors, including healthcare, logistics, industry, and smart technologies, [1]. A collection of connected gadgets collects, exchanges, and analyses data to automate, improve efficiency, and make better decisions.

The widespread use of Internet of Things (IoT) equipment has led to security flaws, making it a prime target for fraudsters, [2]. Integrating AI techniques into IoT systems is a possible solution to handle security concerns and protect the ecosystem. Combining AI and IoT technology enhances their respective strengths, [3].

Modern techniques like machine learning (ML), deep learning (DL), and natural language processing (NLP) let IoT systems evaluate large volumes of data, get insights, and make accurate choices. These strategies let IoT systems adapt to changing surroundings, detect anomalies, and execute security measures against intrusions. AI can improve cyberattack monitoring, secure communication, and data privacy, resulting in a more reliable IoT infrastructure, [4]. AI techniques like machine learning (ML), deep learning (DL), and natural language processing (NLP) let IoT systems evaluate large volumes of data, get insights, and

make informed decisions. These strategies let IoT systems adapt to changing surroundings, detect issues, and automate security measures against intrusions. AI can improve cyber-attack identification, secure communication, and data privacy, resulting in a more secure IoT infrastructure, [5].

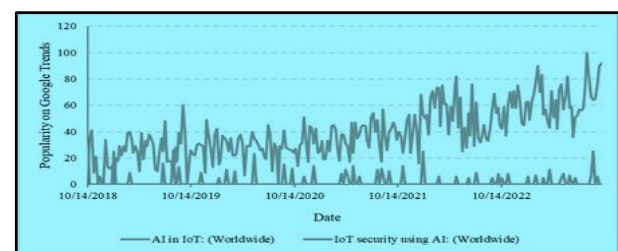


Fig. 1: The level of scientific research for using AI in IoT.

Source: [6]

In Figure 1, the graph illustrates the global research trends in the use of AI with IoT devices. The highest value indicates a standard level of AI utilization in IoT, while the lowest value reflects the application of data security technology involving AI, [6].

Understanding these challenges is essential for developing effective privacy solutions that mitigate risks and protect IoT implementations. AI

approaches play a significant role in enhancing IoT security. Therefore, it is necessary to explore the use of AI in addressing IoT security concerns, [7], [8], [9].

While IoT settings grow, security solutions must address significant difficulties, notably scalability and agility. Traditional, sometimes centralized, security systems are insufficiently nimble to handle the volume and velocity of data created by new IoT networks, [10]. This monolithic strategy results in long delays, excessive energy usage, and an unwillingness to respond effectively to emergent threats. Even combining multiple communication technologies, including 5G, LoRa, and Zigbee, adds a layer of intricacy to controlling security, since linked devices demonstrate vast variety in processing capability and communication requirements, [11].

2 Assault Situations and Risk Strategies

Hybrid attacks couple various threat sources, such as spoofing and DoS, in which a hostile actor impersonates genuine devices before generating large volumes of traffic to destabilize the network. These attacks are especially difficult because of their dynamic nature and ability to use a few weaknesses at once.

Integrating blockchain with AI features shown Figure 2. Block chain enables traceability and data integrity, while AI algorithms detect and classify unusual actions, [12]. In a simulated mixed strike scenario, edge nodes recognized faked devices using anomalies in blockchain transaction records while also isolating high-traffic sources associated with the DoS component of the attack. By integrating these two skills, the system mitigated the attack's effect on networking efficiency. Foundation against a variety of dangers, including illegal access and spoofing. This hybrid technique guarantees a balance between robust security and computational efficiency by fusing the advantages of both technologies. By creating an overwhelming amount of malicious traffic, denial-of-service (DoS) attacks seek to overload network resources like bandwidth or processing power. These attacks usually target devices with limited resources and take advantage of lax communication standards in IoT networks.

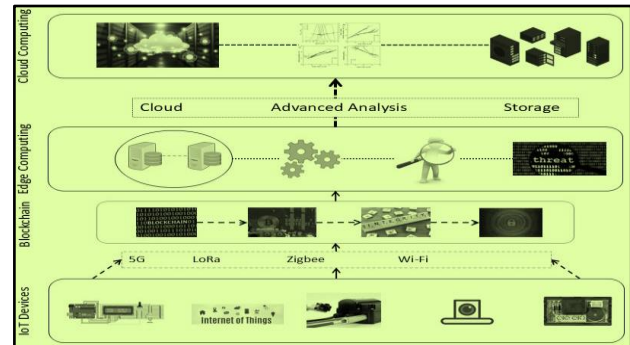


Fig. 2: The level of scientific research for using AI in IoT.

Source: [12]

3 Issues of Confidentiality and Morality

The key security guidelines and strategies for protecting IoT systems are listed in Table 1. It divides these strategies into three main categories: safe software development, defense-in-depth architectures, and secure data management, [13]. To strengthen IoT deployments against a variety of attack vectors, defense-in-depth architectures place an emphasis on layered security mechanisms, reliable safety systems, and secure hardware design. Private coding, over-the-air update systems, and thorough security testing are all part of secure software development techniques, which lower vulnerabilities and increase the resilience of IoT software. To ensure the safety, integrity, and quality of IoT data, secure data management comprises data classification, access controls, safe saving, and life cycle management. Each strategy contributes to deep IoT security strategies by providing unique critical measures and advantages, [14].

Organizations can enhance the security, integrity, and privacy of IoT data by implementing secure data management policies. By utilizing information categorization and access control systems, data is restricted to authorized entities only. Additionally, secure storage and processing procedures protect information both at rest and during processing. Measures for data lifecycle management help mitigate the risks of hacking. All of these principles contribute to establishing a safe and legally compliant framework for handling information related to IoT devices. This framework

enables enterprises to derive value from IoT data while maintaining data safety and confidentiality. Consequently, the raw data remains confidential during processing without being disclosed, [15], [16].

3.1 Ensuring the Security of IoT Networks

Networks play a crucial role when devices connect to AI edge computing systems, as edge nodes process and act on data locally. This local processing necessitates secure connections to protect systems from threats such as surveillance, hacking, spoofing, and other types of attacks. To safeguard data in transit, various communication modes and security frameworks are employed, which authenticate devices and prevent unauthorized access. Below are the most widely used methods and an explanation of how they function, [17], [18], [19]:

3.1.1 Transport Layer Security (TLS)

Handset statuses , such as sleep cycle relation and Detachment and the material of base stations , such as engine speeds change considerably. Furthermore, the number of IoT networks can change vigorously. Where TLS is used for TCP-based protocols (e.g., HTTPS, MQTT over TLS) and DTLS for UDP-based protocols (e.g., CoAP over DTLS), it works:

- A. Establishes encrypted connections between devices and edge servers.
- B. Uses X.509 certificates or pre-shared keys for mutual authentication.
- C. Protects against eavesdropping , message tampering, and replay attacks, MQTT-TLS encrypts messages between IoT sensors and edge brokers so attackers can't read or tamper with data, [20].

3.1.2 Built-in Security Extensions with MQTT

The input text appears to have some clarity issues and may benefit from better structure. Here's a revised version:

MQTT is a lightweight publish/subscribe protocol for IoT messaging. It operates as follows:

- A. It includes TLS encryption for confidentiality.
- B. It uses username/password authentication and optional client certificates.
- C. It supports Access Control Lists (ACLs) to restrict who can publish or subscribe to topics.

For example, a thermostat can securely publish sensor data to an AI edge platform using MQTT over TLS, [21].

3.1.3 Constrained Application Protocol over DTLS / OSCORE

Where it's used: Designed for resource-constrained IoT devices, often used in sensor networks and smart city infrastructure, it works:

- A. Similar to HTTP but optimized for minimal bandwidth.
- B. DTLS adds secure transport
- C. Object Security for Constrained Restful Environments (OSCORE) adds end-to-end object encryption, protecting messages even across intermediaries.

A battery-powered sensor sends encrypted CoAP messages to an AI edge gateway, [22].

3.1.4 Hypertext Transfer Protocol Secure (HTTP) Over (TLS)

The input contains some awkward phrasing and lacks clarity in certain areas. Here's a revised version for improved readability and coherence:

IoT devices that have sufficient resources utilize web-based APIs to connect with edge and cloud services as follows:

- A. They implement standard web security protocols.
- B. They encrypt traffic through processes such as the TLS handshake, symmetric keys, and encrypted communication.
- C. This approach protects against man-in-the-middle (MITM) attacks and data interception. For example, a connected camera streams securely to an AI edge analytics server using HTTPS.

This revision maintains the original meaning while enhancing clarity and flow, [23].

3.1.5 Internet Protocol Security (IPsec)

The text is clear and has a consistent tone. However, slight improvements can be made for better readability and coherence. Here's a revised version: Used for network-level protection between IoT sub-networks and edge infrastructure, particularly in industrial IoT and enterprise deployments, it functions as follows:

- A. Operates at the IP layer.
- B. Utilizes ESP (Encapsulating Security Payload) for encryption and integrity.
- C. Enforces site-to-site VPN tunnels for secure routing.

3.1.6 LoRaWAN Security (AES Encryption)

Where it's used for long-range, low-power IoT (e.g., agriculture, utilities), it works:

- A. Advanced Encryption Standard-128 encryption at:
 1. Network level: authenticity of devices.
 2. Application level: payload confidentiality.
- B. Uses unique session keys per device; long-range low-power networks often link back to AI edge for analysis.

3.1.7 Network Access Control

Where used for enterprise Wi-Fi and Ethernet connections of IoT gateways, it works:

- A. Uses EAP (Extensible Authentication Protocol) to authenticate devices before they join a network
- B. Ensures only authorized endpoints communicate with edge resources, [24].

3.1.8 Secure Boot and Firmware Integrity (Supporting Protocols)

Where it's used on IoT devices and edge nodes, it works:

- A. Cryptographically verifies firmware before booting.
- B. Ensures only trusted software runs.
- C. Protocols include UEFI Secure Boot and signed updates. While not strictly a “communication protocol,” it prevents compromised devices from joining networks.

3.1.9 Zero Trust and Device Identity Frameworks

Where used protocols are Oath 2.0 / JWT and DTMI / DRS (Device Identity Standards).

It works:

- A. Treat every device as untrusted until authenticated.
- B. Use tokens, certificates, and continuous verification.
- C. Limits lateral movement even after connection.

4 How These Protocols Protect IoT

By making a simple comparison between the types of protection for IoT networks linked to AI edge, Table 1 shows each type, its purpose, and how it is done. Through our research, we confirm that the IPsec protocol is concerned with protecting network layers, which are usually the target of attacks during penetration, [25].

Table 1. Summary how these Protocols Protect IoT

Protocol Type	Protects	How
TLS/DTLS	Data in transit	Encryption + authentication
MQTT	Messaging	Secure channel + ACLs
CoAP over DTLS/OSCORE	Lightweight comms	Encrypted transport + object security
HTTPS	API/web comms	Standard SSL/TLS protection
IPsec	Network layer	Encrypted IP packets
LoRaWAN	LPWAN traffic	AES encryption
802.1X	Network access	Authentication before connection
Secure Boot	Device trust	Ensures firmware integrity
OAuth/JWT / Zero Trust	Identity & access	Token-based authentication

Source: [25]

5 Security Diagram for the AI-Edged Internet of Things

The communication stages between the IoT devices and (AI edge) devices are divided into the (cloud layer), (local edge server), (AI edge), and (IoT devices layer). Each stage addresses threats that could disrupt the communication system of the IoT devices or lead to the theft of their information through network security breaches shown in Figure 3.

In this study, we propose encrypting the communication protocol (IPsec) that connects the IoT and cloud devices using AI edge. This makes the communications system more secure, stable, and difficult for attackers to penetrate, [26].

The algorithm we've been discussing uses a special protocol called IPsec. It kicks in before any traffic is allowed to pass through. This protocol links up devices on the IoT network when everything seems safe. To keep things secure and reliable, it uses a method called encapsulating

security payload, or ESP for short. This method encrypts data and makes sure devices stay connected. It does all this using the AI edge method, which doesn't rely on the main cloud system. If the network detects a threat before data is sent, it happens during a specific part of the process. IPsec protocol, this algorithm performs the following:

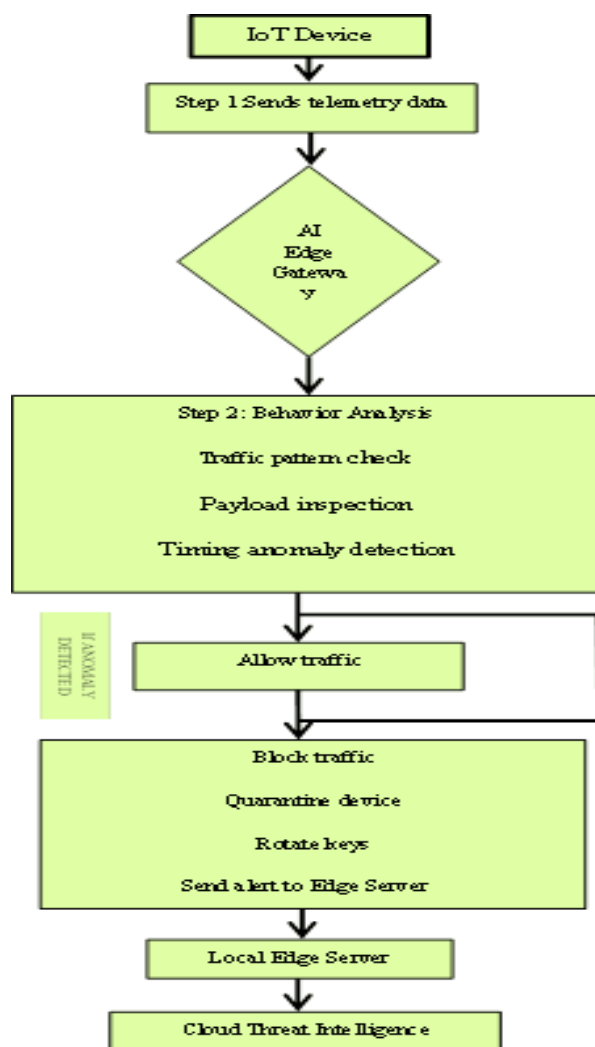


Fig. 3: The proposed IPsec algorithm for network security IoT by using the AI edge.

Source: created by the author

The algorithm we've been discussing uses a special protocol called IPsec. It kicks in before any traffic is allowed to pass through. This protocol links up devices on the IoT network when everything seems safe. To keep things secure and reliable, it uses a method called encapsulated security payload, or ESP for short. This method

encrypts data and makes sure devices stay connected. It does all this using the AI edge method, which doesn't rely on the main cloud system.

1. Isolate device.
2. Reconfigure network path.
3. Rotate cryptographic keys.
4. Deploy patched firmware.
5. Update AI model.

6 A Simulation-Based Quantitative Evaluation of an IPsec Algorithm

A Simulation-Based Quantitative Evaluation of an IPsec Algorithm is often accomplished by comparing critical performance and security parameters in controlled environments (for example, normal traffic against attack situations). Here's how such an evaluation is often structured and what outcomes reflect effectiveness, [27].

6.1 Initialization of the Simulation

Researchers frequently employ instruments such as:

- A. Network simulators, such as OMNeT++ and NS
- B. Actual traffic models (multimedia traffic, TCP/UDP flows).
- C. Attack scenarios (man-in-the-middle, replay, and denial of service).

Protocols. assessed:

- A. Authentication Header, or AH.
- B. Encapsulating Security Payload, or ESP.

6.2 Important Quantitative Measures

A. Latency

Meaning: The duration of a packet's journey from its source to its destination.

Calculating:

$$\text{Latency} = \frac{\sum(\text{arrival time} - \text{send time})}{\text{total packets}} \quad (1)$$

Typical Results:

IPsec causes significant delays owing to:

1. Encryption/decryption.
2. Authentication processing.

Example outcome:

1. Without IPsec: ~10 ms.
2. With IPsec: ~15–25 ms.

An indicator of effectiveness:

A reasonable rise (low overhead in relation to security gain).

B. Productivity (Throughput)

Meaning: The quantity of data that is successfully supplied every second.

Measurement:

$$\text{Throughput} = \frac{\text{total received bits}}{\text{simulation time}} \quad (2)$$

Typical Results: Slight reduction due to overhead:

1. Without IPsec: ~100 Mbps.

2. With IPsec: ~85–95 Mbps.

Effectiveness indicator:

High throughput retention (>80–90%).

C. Integrity

Meaning: Ability to detect unauthorized data modification, measurement:

1. Packet integrity check success rate

2. Hash verification accuracy (e.g., HMAC), Typical

Results:

1. Integrity detection rate

2. ~99.9%–100% for tampered packets.

Effectiveness indicator: Near-perfect detection of altered packets.

D. Resistance to Attacks

1. Replay Attack

IPsec uses sequence numbers, anti-replay window

Detection rate: ~100%

2. Man-in-the-Middle (MITM)

Encryption (ESP) prevents data exposure, Attack success rate: near 0%

3. Denial of Service (DoS)

Some degradation occurs, but: Legitimate packet acceptance remains high

Example:

A. Without protection: network collapse.

B. With IPsec: ~70–85% service maintained.

E. Injection of Packets

1. Unauthorized packets rejected via authentication

2. Detection rate: ~99%, Effectiveness indicator:

High attack detection/prevention rate, Graceful degradation under stress.

F. Simulation results typically prove that an IP security algorithm is effective when:

1. Integrity is nearly perfect (~100%)

2. Attack success rate is near zero

3. Delay increase is minimal and acceptable (Figure 4), it contained the results of the impact IP sec algorithm on delay by using the AI edge, These

results were obtained through simulation using MATLAB programming.

4. Throughput remains high (>80–90%), shown Figure 5, it contained the results of the impact IPsec algorithm on throughput by using the AI edge, We observe a significant improvement in the performance of the Internet of Things IoT communication network using AI edge, as shown by the plotted lines in Figure 4 and Figure 5). These results were obtained through simulation using MATLAB programming.

This demonstrates a balanced trade-off between security and performance, which is the key goal of IPsec, [28], [29], [30].

F. Total Assessment Synopsis, Table 2. Explained the deference between using IP sec and without using IP sec.

Table 2. Displays the results of the impact performance on IoT networks with IP sec and without IP sec.

Measured	Without IPsec	With IPsec	Analysis
Latency	low	↑ moderate	acceptable overhead
Throughput	high	slight↓	efficient
Integrity	low	very high	strong protection
attack resistance	weak	strong	secure

Source: created by the author

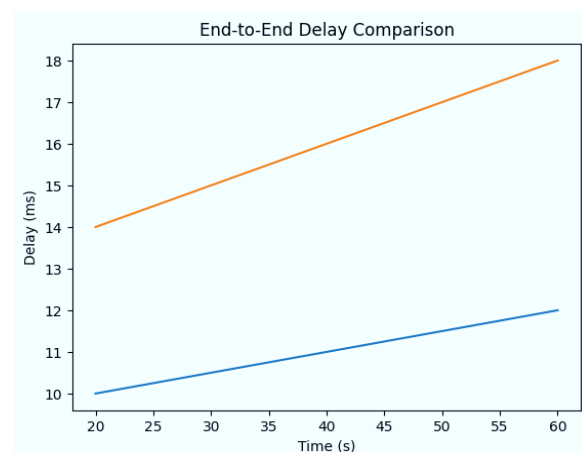


Fig. 4: Displays the results of the impact of the IPsec algorithm on delay by using the AI edge

Source: created by the author

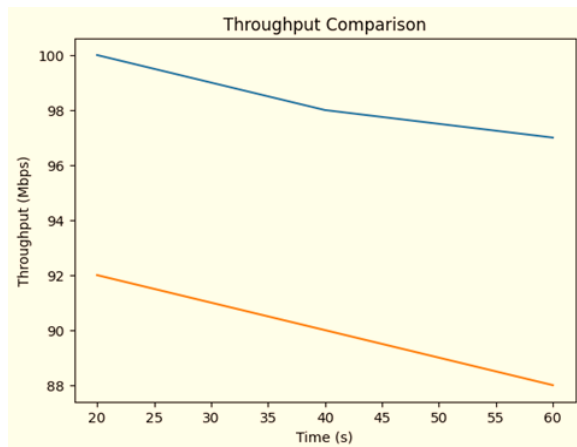


Fig. 5: Displays the results of The impact IPsec algorithm on throughput by using the AI edge
Source: created by the author

7 Conclusion

Network security has become crucial, especially with the increasing number of network devices. Such protection is essential for enhancing security accuracy and preventing attacks on networks serving vital sectors such as industry, agriculture, healthcare, the military, smart cities, smart roads and bridges, and smart buildings, shown Table 3 (Appendix). below. This research presents a specialized algorithm for IoT network security shown in Figure 3. It utilizes AI edge with a protocol that operates with high confidentiality, speed, and accuracy. The proposed name is the Internet Protocol Security (IPsec) algorithm. It encrypts the protocol using a modern encryption method called Encapsulating Security Payload (ESP), which operates within the network layer. While cryptographic processing causes a substantial increase in end-to-end delay (30-50%), performance reduction is negligible (less than 12%). Integrity verification is nearly 100% accurate, ensuring reliable identification of altered packets. Furthermore, the system is highly resilient to replay, MITM, and DoS assaults, with strike success rates nearing zero and considerable improvements in packet delivery during attacks. These results demonstrate the IPsec method's performance and confidence in safeguarding network communications.

Future research should focus on improving IPsec capability by lowering security overhead using lightweight methods and hardware

acceleration techniques. Furthermore, adaptive security techniques that dynamically modify encryption parameters based on network conditions are a promising development. The use of artificial intelligence for proactive threat identification can strengthen resilience against complex attacks. Furthermore, the use of IPsec in new settings such as IoT, 5G, and cloud computing warrants additional exploration. Enhanced attack modeling, energy efficiency considerations, and real-world deployment studies are all necessary to assure IPsec's scalability and robustness in modern network infrastructures.

Declaration of Generative AI and AI-assisted Technologies in the Writing Process

During the preparation of this work, the author(s) utilized artificial intelligence (AI) technologies solely for the purpose of linguistic refinement and grammatical correction. Following the application of these tools, the author(s) comprehensively reviewed, verified, and edited the resulting text. The author(s) maintain full accountability and responsibility for the accuracy, integrity, and final content of the publication.

References:

- [1] Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W. S. (2024). *Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. Transactions on Emerging Telecommunications Technologies*, 35(4), e4329, <https://doi.org/10.1002/ett.4329>.
- [2] Liu, Y., Zhang, J., & Zhan, J. (2021). *Privacy protection for fog computing and the internet of things data based on blockchain. Cluster Computing*, 24(2), 1331-1345, <https://doi.org/10.1007/s10586-020-03190-3>.
- [3] Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Bakar, K. A. A., Al-Dmour, N. A., Said, R. A., ... & Alomoush, W. (2023). *Machine learning-based intrusion detection approaches for secured internet of things. The effect of information technology on business and marketing intelligence systems*, 2013-2036, https://doi.org/10.1007/978-3-031-12382-5_110.
- [4] Khosrojerdi, F., Akhigbe, O., Gagnon, S., Ramirez, A., & Richards, G. (2022).

- Integrating artificial intelligence and analytics in smart grids: a systematic literature review*. International Journal of Energy Sector Management, 16(2), 318-338, <https://doi.org/10.1108/IJESM-06-2020-0011>.
- [5] Chui, K. T., Gupta, B. B., Liu, J., Arya, V., Nedjah, N., Almomani, A., & Chaurasia, P. (2023). *A survey of internet of things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions*. Information, 14(7), 388, <https://doi.org/10.3390/info14070388>.
- [6] Wang, X., Du, H., Feng, L., Zhou, F., & Li, W. (2025). *Effective throughput maximization for noma-enabled urlhc transmission in industrial iot systems: A generative AI-based approach*. IEEE Internet of Things Journal, 12(10), 13327-13339, <http://doi.org/10.1109/JIOT.2025.3533570>.
- [7] Sedjelmaci, H. (2021). *Cooperative attacks detection based on artificial intelligence system for 5G networks*. Computers & Electrical Engineering, 91, 107045, DOI: 10.1016/j.compeleceng.2021.107045.
- [8] Nithyavani, G., & Raja, G. N. (2025). *A comprehensive survey on security and privacy challenges in internet of medical things applications: Deep learning and machine learning solutions, obstacles, and future directions*. IEEE Access, <http://doi.org/10.1109/ACCESS.2025.3588489>.
- [9] Alabdulatif, A., Thilakarathne, N. N., & Aashiq, M. (2024). *Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System*. Computers, Materials & Continua, 80(3). DOI: 10.32604/cmc.2024.054610.
- [10] Whig, P., Madavarapu, J. B., Yathiraju, N., & Thatikonda, R. (2024). *IoT healthcare's advanced decision support through computational intelligence*. In *Evolution of Machine Learning and Internet of Things Applications in Biomedical Engineering* (pp. 41-53). CRC Press, DOI: 10.1201/9781003476207-3.
- [11] Soy, H., Fatih Ateş, T., & Osman Özkan, A. (2025). *Feasibility of LoRa-based Infrastructure-to-Vehicle (I2V) communication for road weather information systems*. International Journal of Communication Systems, 38(4), e6002, <https://doi.org/10.1002/dac.6002>.
- [12] Joshan, A. (2026). *Towards a Human-Centric Industry 5.0 Enabled by the Convergence of Artificial Intelligence, Internet of Things, and Blockchain*. Journal of Data Analytics and Intelligent Decision-making, 1(4), 32-49, DOI: 10.22091/jdaid.2026.14749.1025.
- [13] Elsagheer Mohamed, S. A., & AlShalfan, K. A. (2021). *Intelligent traffic management system based on the internet of vehicles (IoV)*. Journal of advanced transportation, 2021(1), 4037533, <https://doi.org/10.1155/2021/4037533>.
- [14] Cholke, A., Mandhare, V. V., & Vikhe, P. S. (2024, October). *A Review of Security and Information Control in Blockchain-Integrated IoT Applications*. In 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1-6). IEEE, DOI: 10.1109/ICBDS61829.2024.10837192.
- [15] Imankulova, B., Alpar, S., & Amanzholova, S. (2022). *Data security, modeling and visualization of data from IoT devices*. Scientific Journal of Astana IT University, DOI: 10.37943/ACWT2121.
- [16] Song, Y., Feng, Y., Li, Y., Kong, R., & Xiao, S. (2026). *Evolutionary patterns and future trends of China's hydrogen energy industry policy*. Energy Reports, 15, 108966, <https://doi.org/10.1016/j.egy.2025.108966>.
- [17] Abdalzaher, M. S., Krichen, M., Shaaban, M., & Fouda, M. M. (2025). *Quality-focused Internet of Things data management: A survey, perspectives, open issues, and challenges*. IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2025.3613669.
- [18] Oliveira, N., Praça, I., Maia, E., & Sousa, O. (2021). *Intelligent cyber attack detection and classification for network-based intrusion detection systems*. Applied Sciences, 11(4), 1674, <https://doi.org/10.3390/app11041674>.
- [19] Wilhelm, T. (2025). *Professional penetration testing: Creating and learning in a hacking lab*. Elsevier, DOI: 10.1016/C2012-0-00443-7.
- [20] Albalawi, N., Alamrani, N., Aloufi, R., Albalawi, M., Aljaedi, A., & Alharbi, A. R. (2023). *The Reality of Internet Infrastructure and Services Defacement: A Second Look at Characterizing Web-Based Vulnerabilities*.

- Electronics*,12(12),2664,
<https://doi.org/10.3390/electronics12122664>.
- [21] Eriksson, A., & Mirza, R. (2025). *Investigating the Technical and Organizational Challenges of Implementing IIoT in Automotive Manufacturing: A case study of Scania*, master's thesis published via the KTH Royal Institute of Technology's digital archive, DiVA.
- [22] Ahmad, G. I., Singla, J., & Giri, K. J. (2021). *Security and Privacy of E-health Data*. In *Multimedia security: algorithm development, analysis and applications* (pp. 199-214). Singapore: Springer Singapore, https://doi.org/10.1007/978-981-15-8711-5_10.
- [23] Torre, D., Chennamaneni, A., & Rodriguez, A. (2023). *Privacy-preservation techniques for IoT devices: A systematic mapping study*. IEEE Access,11,16323-16345, DOI: 10.1109/ACCESS.2023.10044661.
- [24] Marimuthu, D., Rao, G. R. K., Mehbodniya, A., Mohanasundaram, D., Sundaram, C. K., Maria, A. B., & Mani, D. (2023). *Mathematically modified adaptive neuro-fuzzy inference system for an intelligent cyber security system*. SN Computer Science, 4(5), 453, <https://doi.org/10.1007/s42979-023-01822-0>.
- [25] Ati, M. K., Abbas, R. A., & Khazaal, H. F. (2022, May). *Grants and hurdles machine to machine Communication at Scale*. In 2022 5th International Conference on Engineering Technology and its Applications (IICETA) (pp. 243-247). IEEE, ieeexplore.ieee.org.
- [26] Schwenk, J. (2022). *Transport Layer Security. In Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications* (pp. 201-242). Cham: Springer International Publishing.
- [27] Thamer, K. A., Ahmed, S. R., Almarshadany, M. T. M., Abdulqader, S. G., Abduladheem, W., & Algburi, S. (2024, May). *Secure data transmission in iot networks using machine learning-based encryption techniques*. In *Proceedings of the Cognitive Models and Artificial Intelligence Conference* (pp. 285-291), <https://doi.org/10.1145/3660853.3660929>.
- [28] Boboyeva, Z., Sokhibov, R., Yuldashev, I., & Ma'murov, A. (2023). *A Survey on Internet of things architectures*. In *E3S Web of Conferences* (Vol. 402, p. 03053).EDP Sciences, DOI: 10.1051/e3sconf/202340203053.
- [29] Ati, M. K., Abbas, R. A., & Khazaal, H. F. (2022, May). *Grants and hurdles machine to machine Communication at Scale*. In 2022 5th International Conference on Engineering Technology and its Applications (IICETA) (pp. 243-247). IEEE..
- [30] Baliyar Singh, R. K., Dash, J. K., & Reddy, K. H. K. (2026). *The role of Edge-AI in edge enabled IoT systems: A comprehensive performance analysis*. Peer-to-Peer Networking and Applications,19(1),35, DOI: 10.1007/s12083-025-02182-7.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The author in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

https://creativecommons.org/licenses/by/4.0/deed.en_US

APPENDIX

Table 3. Displays the results of Methods and strategies for integrity

Assurance Methods & Structures	Important Steps	Advantages	References
Multi-layered safeguards	1. Triple-layered safeguards. 2. All-encompassing safety systems. 3. Encrypted equipment creation and execution.	1.Increased security from multiple points of attack. 2.A total method for safety of the IoT. 3.A solid basis for protection of devices.	[13], [14], [15], [16]
Private designing software	1. Use safe programming habits. 2. Implement private equipment and an upgrade procedures. 3. Security testing and vulnerability evaluation approaches for Internet of Things (IoT) systems.	1.Lower danger to create risks. 2.Patching security weaknesses in a timely manner. 3. Enhanced software reliability. 4.proactively identifying and resolving threats.	[17], [18], [19], [20]
Protection of information	1.Methods for classifying data and controlling access. 2.Provide appropriate archive and processing of data mechanisms for IoT applications. 3. Information evolution administration issues for IoT systems.	1. Managed and approved permission to use IoT data. 2. Ensuring privacy of information and integrity. 3. Security of information during storage and processing. 4. Keeping up with confidential information regulations. 5.Reduced the danger of hacking of data.	[21], [22], [23], [24]
Solving for all challenges to receive the signals with high speed and security	1. Jamming devices pose a great challenge to communication devices by continuously sending random signals to the channels, which leads to preventing communication between users. 2. Complexity is a big challenge for receivers because it decrypts all messages.	To avoid interference with devices operating within the IoT network system, create a secure and fast protocol to connect the AI edge with these network systems.	[25] ,[29], [30]

Source: created by the author