TELECOMMUNICATIONS ENGINEERING

Impact of Security Threats on IoT Telecommunication Network Performance

Onyenwoke Afam Henry, Promise Elechi, Shadrach Kukuchuku

Department of Electrical/Electronic Engineering, Faculty of Engineering, Rivers State University, Port Harcourt, Nigeria

Published November 2026

Abstract

The integration of Internet of Things (IoT) devices within telecommunication networks has led to the emergence of many security vulnerabilities affecting network performance, reliability, and information integrity. In this regard, this paper provides a comprehensive analysis and evaluation of the effect of cyber threats and cybersecurity solutions for IoT-based telecommunication networks as well as providing an efficient solution. The impact assessment carried out indicates that attacks such as DDoS and MITM attacks significantly impair the network's efficiency since they result in reduced network throughput of 50 Mbps, increased latency to 300 ms, up to 30% packet loss, and energy consumption of up to 80 J. Current approaches used to enhance security include firewalls and encryption algorithms like AES, with the latter achieving a detection accuracy of 98%, but at the expense of high energy consumption of 10 J, while the former achieves 90% detection rate at minimum overhead, but with high latency. An innovative feedforward neural network-based intrusion detection system (FFNN-IDS) was developed with impressive results of a detection accuracy of 99%, low latency of 18 ms, and zero false-positive rates compared to traditional security mechanisms. Post-implementation of the proposed solution resulted in significant improvement in performance, whereby throughput increased from 60 to 85 Mbps, decreased latency from 220 to 150 ms, and reduced packet loss from 25% to 10%, thus enhancing network stability, efficiency, and performance. There was also a decrease in the incidence of cyber threats, such as unauthorized access reduced to 5% from 50% daily, DDoS attacks were reduced to 20% from 80%, whereas the frequency of network downtime was greatly reduced from 120 minutes per day to 20 minutes per day. The efficiency of the proposed solution is further evidenced by the significant increase in data integrity from 65% to 95% despite increased energy consumption of 90 J. Overall, it was observed that the proposed approach performed efficiently despite increased processing overhead as the scale increases from 5% to 80% as the number of devices increases from 100 to 50,000.

Keywords: security threat; IoT; Telecommunication network; performance; integrity; vulnerability

1 Introduction

The influence of security threat on IoT networks has brought significant changes in performance and reliability in data transmission. Recent advances in telecommunication technology have made it possible to transmit data between continents, hence fostering innovations in industries like health care, finance, and industry. One of the remarkable breakthroughs in telecommunication technologies involves Internet of Things (IoT) applications, which extend the functionalities of telecommunication networks beyond human-to-human communication by connecting billions of smart devices (Adeoye et al., 2024a). However, apart from making the network more efficient and reliable, integration of IoT devices into telecommunication networks has brought significant security challenges. Telecommunication IoT networks involve the connection of billions of IoT devices in order to facilitate seamless data exchange and communication. These devices include wearable gadgets, smart sensors, actuat-

ors, and industrial devices connected through communication channels, including Wi-Fi, Bluetooth, 4G/5G communication networks, and Low-power WAN (LP-WAN). These networks have made telecommunication networks extremely versatile and highly functional in recent years, hence accelerating the process of digital transformation (Adeoye et al., 2024a). However, the increase in connectivity through IoT networks comes with numerous cyber threats which can easily impair the efficiency, reliability, and performance of such telecommunication networks.

The threat of distributed denial of service (DDoS) is yet another security challenge in IoT networks, with the Mirai attack being one of the worst cases of such cyberattacks experienced in telecommunication networks. DDoS attacks usually involve the use of botnets, which are created by infecting multiple devices with malicious software (Alaba et al., 2017). Hackers can easily infiltrate millions of IoT devices and turn them into botnets, which could later be controlled to disrupt communication networks. Hence, it has become imperative to implement strong security mechanisms to guard against this security risk.

The impact of cybersecurity on IoT is wide-ranging and cuts across issues of national security, financial gains, and even industrial operations and efficiency. A good security mechanism for IoT would enable us to achieve safer and reliable telecommunication networks in future years. Security will pave the way for sustainable development of the IoT in telecommunication.

2 Materials and methods

2.1 Materials

This section describes the materials used in the study and the methodology employed to meet its objectives. Specifically, the present paper examines the effect of security mechanisms on IoT network performance using simulation-based analysis using MATLAB and Simulink software, Microsoft Excel, published research articles and a computer system (Core i7, 16 GB RAM).

2.2 Simulation blocks

The Simulink model in use is composed of two stages: pre-security implementation stage and post-security implementation stage. In the first stage, a Bernoulli Binary Block generates random binary data packets representing IoT traffic in an IoT network, an AWGN (Additive White Gaussian Noise) Block introduces channel noise to simulate realistic channel interference, a Splitter Block duplicates the signals in order to simultaneously compare the secured and unsecured network performances, and a Scope Block monitors the behavior of the signals in the network.

In the post-security implementation stage, a Random Number Block represents the encrypted IoT data packets in the IoT network. A MATLAB Function Block, in which a new security algorithm (such as Feedforward Neural Network based Intrusion Detection System) is implemented. There are additional security mechanisms like firewall and access control implemented using the MATLAB Function Block. A Combiner Block is added to merge the secured and unsecured network performances in order to conduct comparison of their efficiencies. Another MATLAB Function Block is used to represent the supplementary security mechanisms, another AWGN Block to simulate real noise interference in the secured IoT network, and finally a Scope Block to visualize the improvements made by security measures (Figure 1).

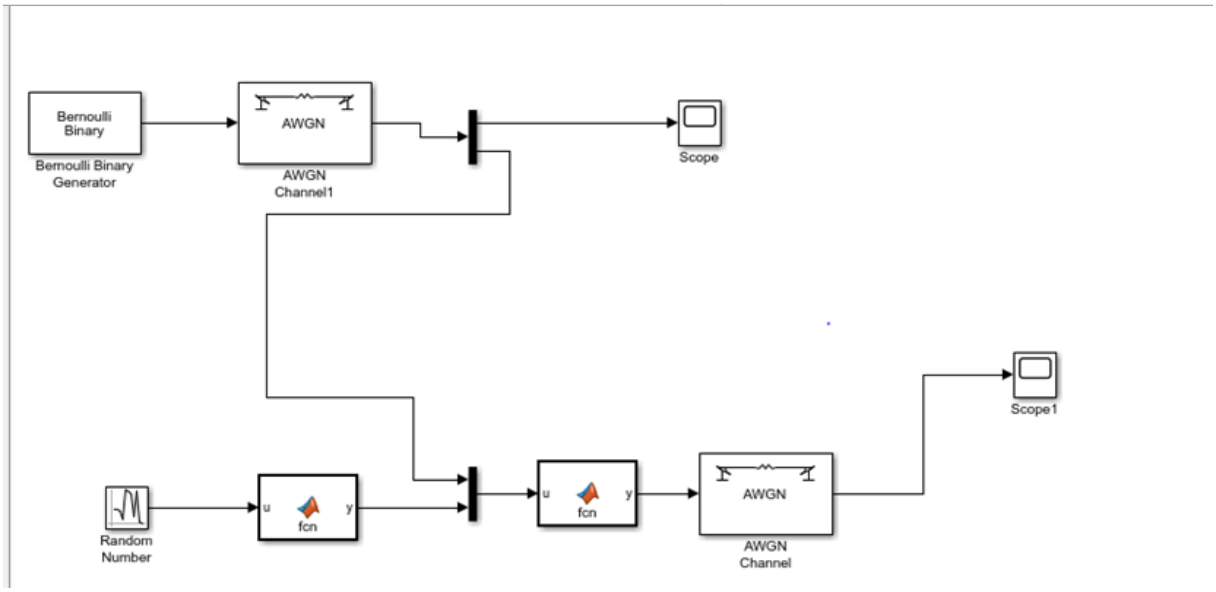


Figure 1. MATLAB Simulink model showing the pre- and post-security implementation stages for the IoT network simulation.

Essentially, the Simulink model in Figure 1 represents an IoT telecommunication network initially unprotected against any kinds of threats or attacks and then secured using various measures. In other words, the model simulates both the state before security mechanisms are applied and the state after applying those security measures. It comprises six functional blocks, the role of each of which will be explained below.

Block 1: Bernoulli Binary Block. As mentioned above, this model uses the Bernoulli Binary Block to produce binary data, which is the most common representation of data packets sent by IoT devices within the Internet of Things framework. This process occurs in the beginning of simulation. Essentially, this block is responsible for generating random streams of ones and zeros that symbolize network traffic (sent from smart sensors, cameras, household appliances etc.). This randomness represents the reality of IoT traffic since different IoT devices may be transmitting data packets of different types to varying degrees of success.

Block 2: AWGN Block (Additive White Gaussian Noise) – Pre-Security. After the binary data packets are generated by the Bernoulli Block, it is the turn of the AWGN Block. This functional block introduces noise into the IoT network, which simulates realistic conditions of data packet transmission (because in reality such interference inevitably occurs as a result of different kinds of disturbances such as distance between the sender and the recipient, interference from electromagnetic waves, etc.). If not for the AWGN block, the simulation would run in an unrealistic situation in which there is absolutely no signal interference.

Block 3: Splitter Block. The Splitter Block creates two paths out of the input signal – one representing an unprotected baseline and the other leading to a network under security. Such arrangement is essential to enable side-by-side comparison of secured and unsecured network states (meaning that both the signal and its performance characteristics must be absolutely equal in both paths).

Block 4: Scope Block – Pre-Security. This block acts as a kind of monitor for viewing signal performance characteristics under unprotected conditions (meaning in the absence of security mechanisms). Thus, it continuously records throughput degradation, latency and packet loss under threat. In practical terms, this corresponds to observing the network while under cyber-attack.

Block 5: Random Number Block. This Block represents the traffic that has undergone encryption and is therefore protected from cyberattacks. In comparison with the Bernoulli Block, whose main task is to generate data packets, this one is supposed to simulate what happens after the data has passed through security filters. In other words, it generates packets that are randomized and hence more difficult to decipher and hack.

Block 6: Combiner Block. The Combiner Block plays an important role in comparing secured and unsecured network performances, as it merges output data obtained through simulation of security mechanisms with unprotected baseline performance.

To sum up, reading the Simulink diagram from left to right reveals the whole simulation process: generation of data packets, introduction of noise into the signal, creation of two parallel lines. On one side of these lines, the traffic flow is unsecured; on the other side, there are encryption, FFNN-IDS, firewall security and additional noise introduced. Then the outputs of these two simulations are brought together by the Combiner Block, and finally they are compared using the last Scope Block. Every block in this process performs a unique task.

2.3 Analysing the impact of security threats on IoT network performance

This part of the study sought to establish the impact of various types of cyber threats (DDoS, malware, unauthorized access, Man-in-the-Middle attacks) on the performance of an IoT-based telecommunication network.

Role of the MATLAB Simulink Diagram: For completing the objective, the pre-security stage of the Simulink model was primarily used. The Bernoulli Binary Block generates IoT data packets randomly simulating IoT traffic, the AWGN Block introduces realistic interference into the signal (as discussed in the previous section). Afterward, the Splitter Block creates two parallel lines with an unprotected network on one side and a network under simulated cyber-attacks on the other side. Lastly, the Scope Block continuously records and monitors the packet loss, latency, and throughput, capturing their change caused by the presence of security threats.

Data Collection and Analysis: In this phase, simulations involving different types of security threats were separately conducted for four threat categories: DDoS attacks, Malware, Unauthorized Access and Man-in-the-Middle (MITM) attacks. For each scenario, the values of the four key performance indicators (packet loss (%), latency (ms), throughput (Mbps) and energy consumption (J)) were recorded. The results are presented as bar charts to allow a quantitative comparison of the threat categories.

2.4 Evaluating the efficiency of existing security solutions in IoT networks

This part of the study evaluated the efficiency of existing security mechanisms (AES encryption, firewall, Intrusion Detection System and blockchain security) in protecting an IoT-based network and preserving its performance at an optimal level.

Role of the MATLAB Simulink Diagram: To evaluate the effectiveness of existing security solutions, each of them was implemented using the MATLAB Function Block in the post-security stage of the Simulink Model, as illustrated in Figure 1. Specifically, each of these measures was separately applied under DDoS and Man-in-the-Middle attacks in order to assess their impact on signal performance. The results were recorded using the Scope Block.

Data Collection and Analysis: Performance data (including detection accuracy (%), latency (ms), power consumption (J) and data overhead (%)) obtained during simulation runs with four security solutions was recorded and compared using bar charts. Besides, the data was used to train the Feedforward Neural Network (FFNN) which was used to develop a new security technique.

2.5 Key performance metrics for security evaluation

Security measures implemented within IoT-based networks impact their performance. The performance indicators used in this study are described below.

2.5.1 Throughput

This metric measures the rate at which the data transfer occurs within the IoT network. It is usually measured in bits per second (bps), kilobits per second (kbps), megabits per second (mbps) or gigabits per second (gbps). The throughput is given by Equation (1) (Adeoye et al., 2024a):

$$T = \frac{D}{t} \tag{1}$$

where T is the throughput (Mbps), D is the total data transmitted (MB) and t is the transmission time (s).

Relevance to security in IoT networks:

- Without security: An IoT network may be exposed to cyber threats such as DoS attacks or jamming that significantly reduce throughput through frequent retransmissions.
- With security: Security mechanisms such as encryption, authentication and firewalls are able to ensure higher network throughput and protect it from attacks. However, certain security measures may have a negative impact on IoT network throughput due to additional computations.

Ideal Scenario: An IoT network should demonstrate optimal throughput while securing and validating the transferred data.

2.5.2 Packet loss ratio (PLR)

This term refers to the proportion of the packets sent that are not received in a network. Packet loss is calculated using Equation (2) (Ajala et al., 2024a):

$$\text{PLR} = \frac{P_{\text{Sent}} - P_{\text{Received}}}{P_{\text{Received}}} \tag{2}$$

where PLR is the packet loss ratio, P_{Sent} is the total number of packets sent and P_{Received} is the total number of packets received.

Relevance to security in IoT networks:

- Without security: The network may be exposed to packet dropping attacks (also called blackhole attacks), jamming, or flooding that may result in high packet loss.
- With security: Various security measures such as IDS, packet authentication and access control are effective in preventing packet loss. However, overly restrictive security measures can sometimes block the legitimate packets.

2.5.3 Latency

Latency is another important factor affecting performance efficiency in IoT networks. It refers to the time delay between the transmission and reception of the packet. It is measured in milliseconds (ms) (Kim et al., 2023) and is calculated using Equation (3):

$$L = T_{\text{Arrived}} - T_{\text{Sent}} \tag{3}$$

where T_{Sent} is the time when the packet was sent and T_{Arrived} is the time when the packet was received.

Relevance to security in IoT networks:

- Without security: IoT network has low latency because no additional time is spent on encrypting and decrypting the data. Nevertheless, it is vulnerable to various attacks which can negatively affect network performance.
- With security: Security measures, such as encryption, authentication and firewall filtering result in processing delays, increasing latency. They are needed in order to ensure secure data transfer.

Ideal Scenario: Security measures should be used in order to protect the network while introducing minimal computational overhead.

2.5.4 Energy consumption

IoT network energy consumption is another important metric. It refers to the total amount of power spent for IoT data transfer and security (Kim et al., 2023), and is calculated using Equation (4):

$$E = Pt \tag{4}$$

where E is the energy consumed (J), P is the power consumed (W) and t is the time taken for data transmission.

Relevance to security in IoT networks:

- Without security: IoT network consumes little power since encryption, authentication, data integrity check does not take place. However, it is exposed to potential attacks leading to the depletion of its power sources.
- With security: Security measures such as encryption (AES, RSA), authentication protocols, IDS etc., require additional processing that takes up additional energy. IoT network becomes more secure and protects itself from such attacks as DoS, man-in-the-middle attacks and others.
- Ideal Scenario: Security measures in IoT should protect IoT devices from various attacks and ensure minimal energy consumption.

2.5.5 Computational overhead

Computational overhead is an indicator reflecting additional processing and computational time introduced into the IoT network as a result of applying various security mechanisms. It is calculated using Equation (5) (Lai et al., 2024):

$$\text{CO} = \frac{T_s - T_u}{T_u} \times 100 \tag{5}$$

where CO is the computational overhead (%), T_s is the processing time with security and T_u is the processing time without security.

Relevance to security in IoT networks:

- Without security: IoT network works in optimal conditions and does not introduce any computational overhead as it does not need to carry out security processing.
- With security: Modern security measures, such as public-key cryptography (RSA, ECC), machine learning-based anomaly detection and blockchain security involve complex operations that require high processing power.

Ideal Scenario: Optimal Security Solution involves minimal computational overhead

2.5.6 *Security efficiency*

Security efficiency reflects the extent to which security measures positively impact IoT network performance and security while introducing minimal overhead. It is calculated using Equation (6) (Lai et al., 2024):

$$\mathrm{SE} = \frac{T_s - T_{\mathrm{ua}}}{\mathrm{CO}} \tag{6}$$

where SE is the security efficiency, T_{ua} is the throughput when the network is under attack, T_{s} is the throughput after applying security and CO is the computational overhead (%).

Relevance to security in IoT networks:

- Without security: The network is fully operational and operates efficiently. However, it is extremely vulnerable to cyber-attacks.
- With security: Effective and robust security measures can ensure protection, but at the cost of network performance, which is adversely affected by security measures.
- Balancing security and efficiency: The aim of security enhancement is finding the optimal balance between them.

Ideal scenario: a highly efficient security system should:

- detect and prevent all cyber-attacks effectively;
- minimise network latency and packet loss;
- provide high throughput; and
- minimise computational overhead.

3 Results and discussion

3.1 Impact of security threats on network performance

Figures 2–5 show the effect of the four threat categories on throughput, latency, packet loss and energy consumption, respectively.

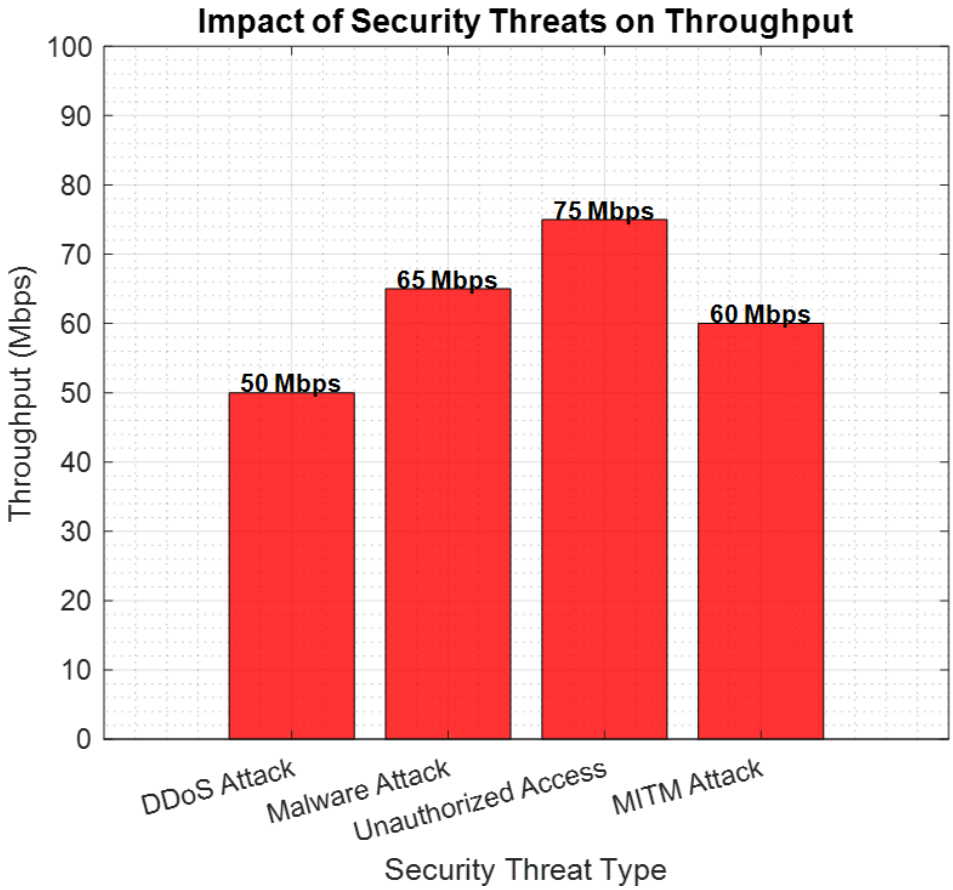


Figure 2. Effect of security threats on network throughput in an IoT-based telecommunication environment.

Figure 2 displays a graph that illustrates how four types of cyber threats, namely, DDoS, malware attacks, unauthorized access, and Man in the middle attacks (MITM) reduce network throughput in IoT-based telecommunication environment. The results show the negative effect of all types of security threats. The DDoS attack causes the worst impact because it reduces the throughput to 50 Mbps. As mentioned above, DDoS attack involves the flooding of network with huge amount of traffic. It means that the network is filled with useless packets that displace useful ones. Next, the MITM attack reduces network capacity to 60 Mbps as it is associated with the rerouting and traffic interception. The malware attack and unauthorized access reduce network capacity to 65 Mbps and 75 Mbps correspondingly. The figure helps to prove that cyber threats negatively influence network performance. Specifically, the data obtained in relation to network throughput illustrate how dangerous threats are for IoT network. Thus, this illustrates the negative effect of cybersecurity issues and demonstrates its significance.

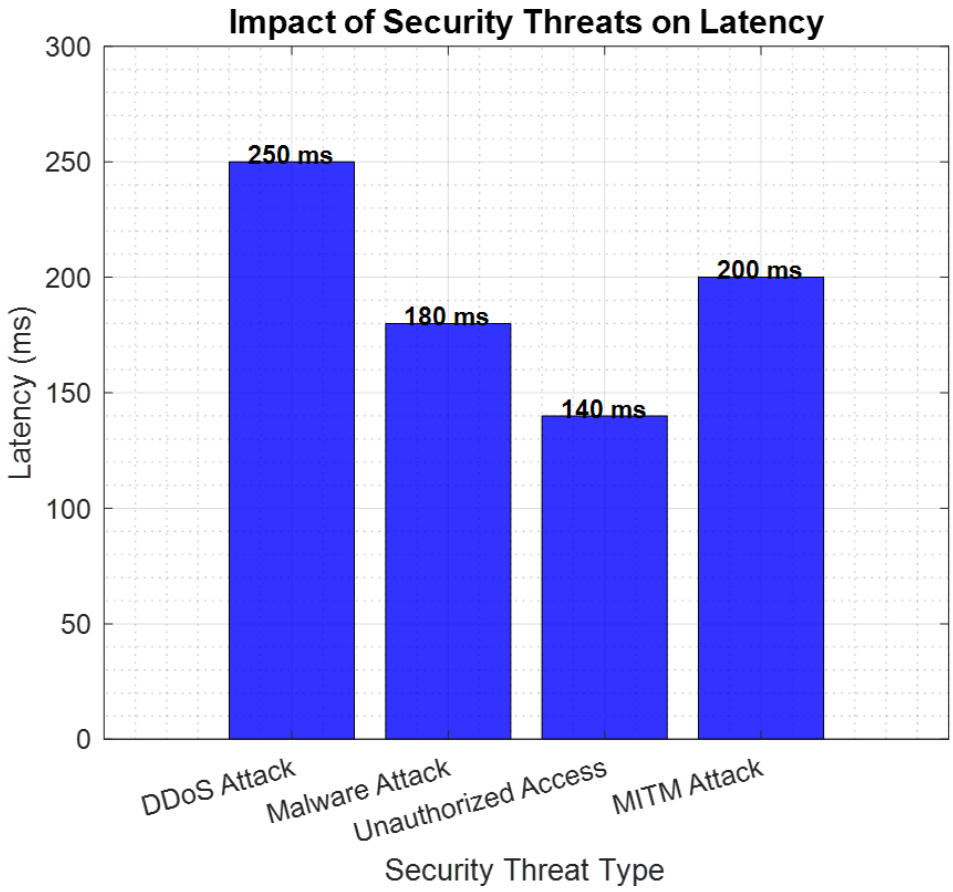


Figure 3. Effect of security threats on network latency in an IoT-based telecommunication environment.

Figure 3 presents graphs that demonstrate the latency introduced by different kinds of cyber threats, measured in milliseconds. According to the results, all four types of threats cause a considerable increase of end-to-end delay that is unacceptable for the normal functioning of network. DDoS attack produces the highest value (250 ms), which means that in the conditions of attack, network cannot function properly. As it can be seen in the chart, MITM attack causes 200 ms latency, which corresponds to additional processing during traffic interception and retransmission. The malware attack and unauthorized access produce 180 ms and 140 ms latencies correspondingly.

Figure 3 shows that cybersecurity issues influence important parameters of network functioning. The latency values demonstrate the fact that threats not only decrease the volume of delivered traffic, but also influence its real-time characteristics. The 250 ms latency in the conditions of DDoS attack is a good confirmation of it.

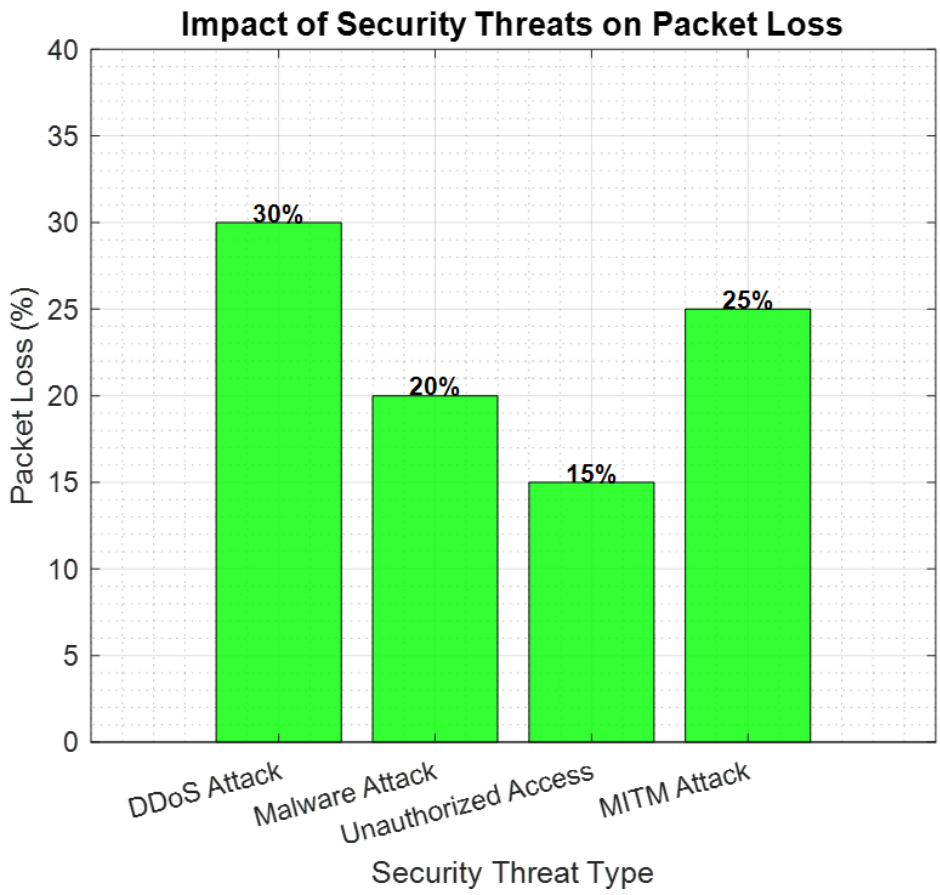


Figure 4. Effect of security threats on network packet loss in an IoT-based telecommunication environment.

Figure 4 illustrates the packet loss percentage related to different types of threats. As shown in Figure 4, the most critical threat in terms of packet loss is DDoS attack because it leads to 30% loss of packets. In relation to MITM attack, packet loss equals to 25%, which is associated with the interception and further destruction of packets. The packet loss in the case of malware attacks and unauthorized access is 20% and 15% correspondingly.

The information provided in Figure 4 plays a crucial role. Packet loss demonstrates the fact that cyber threats can negatively influence data integrity. As shown above, about one-third of packets can be lost in the conditions of DDoS attack.

Figure 4 provides perhaps the most operationally significant evidence of threat impact. Packet loss directly degrades data integrity, triggers retransmission cycles that compound congestion, and undermines the reliability of IoT communication. The 30% packet loss under DDoS conditions means that in a practical deployment, nearly a third of sensor readings, command signals, or telemetry data would be lost entirely. This figure therefore not only quantifies a performance metric but illustrates a real-world consequence of leaving IoT networks unprotected, reinforcing the core motivation of this study.

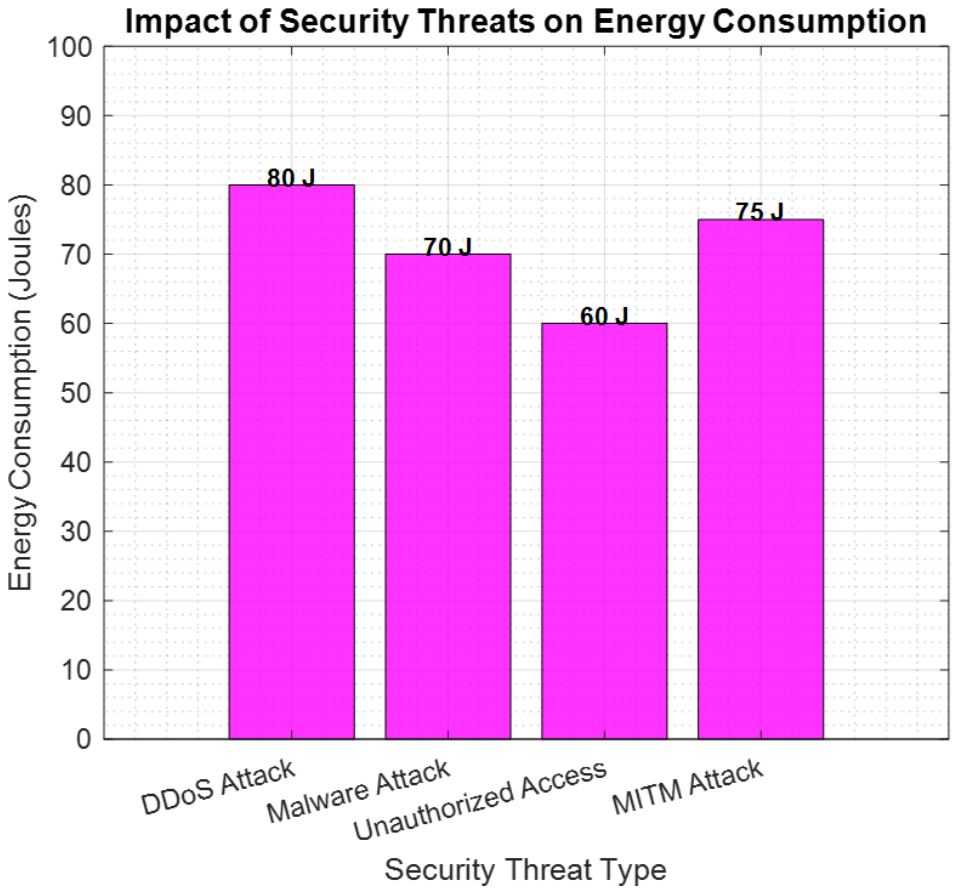


Figure 5. Effect of security threats on device energy consumption in an IoT-based telecommunication environment.

Figure 5 shows that all four types of cyber threats lead to the increase of energy consumption. Thus, in the conditions of DDoS attack, device energy consumption grows to 80 J because they spend much time retransmitting packets, as well as performing additional processing to handle large volumes of traffic. In relation to MITM attack, energy consumption of device rises to 75 J. Moreover, the energy consumption of devices is 70 J and 60 J in the cases of malware attacks and unauthorized access correspondingly.

Figure 5 is important as it illustrates one more dimension of influence of cyberattacks on IoT network. As stated above, energy consumption influences the working life of batteries. This information is therefore essential for assessing threat impact.

Table 1 summarises the impact of the four threat categories on the four performance indicators.

Table 1. Impact of security threats on IoT network performance.

Security threat	Throughput (Mbps)	Latency (ms)	Packet loss (%)	Energy consumption (J)
DDoS attack	50	250	30	80
Malware attack	65	180	20	70
Unauthorized access	75	140	15	60
MITM attack	60	200	25	75

Table 1 represents how the mentioned cybersecurity threats negatively influence IoT network's main performance indicators. In the conditions of a DDoS attack, throughput drops to 50 Mbps, whereas the latency increases up to 250 ms and packet loss is 30%. Also, energy consumption is 80 J. MITM attack also results in a significant degradation of network performance (60 Mbps throughput, 300 ms latency, 25% packet loss, and 75 J energy consumption). Such degradation of performance clearly confirms the importance of effective security mechanisms.

3.2 Performance before and after security enhancement

Figure 6 and Table 2 compare the network performance before and after the security enhancement.

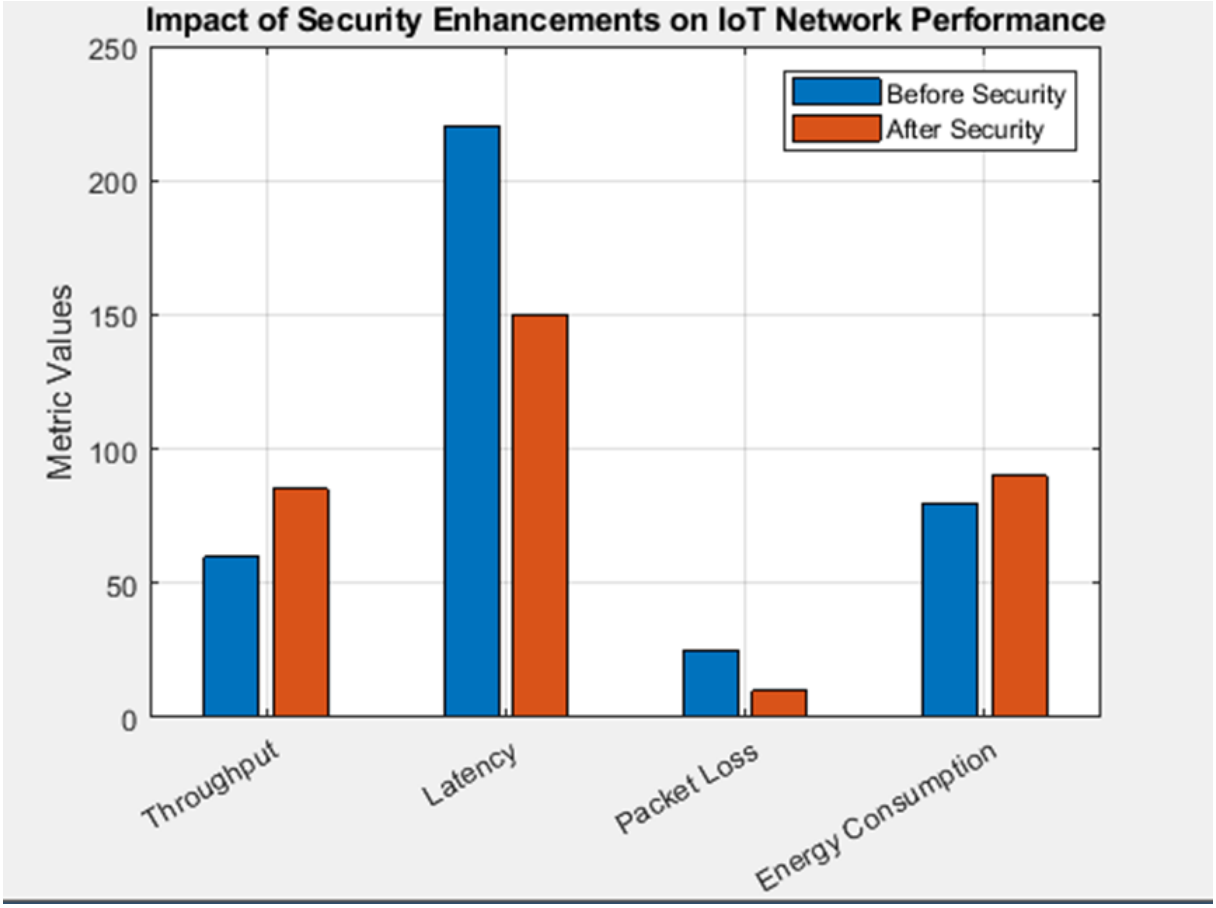


Figure 6. Impact of security enhancement on IoT network performance.

As shown in Figure 6, when the security mechanism is implemented in the IoT network and it positively influences the performance of the system. In particular, network throughput has been increased from 60 Mbps to 85 Mbps. As for latency, it has decreased to 150 ms. Furthermore, the packet loss rate has fallen from 25% to 10%, which means that the implementation of a security measure leads to increased integrity of data transmission. The energy consumption, however, has increased from 80 J to 90 J.

Table 2. Performance before and after security enhancement.

Performance metric	Before security	After security
Throughput (Mbps)	60	85
Latency (ms)	220	150

Performance metric	Before security	After security
Packet loss (%)	25	10
Energy consumption (J)	80	90

As can be seen in Table 2, after applying security measure to IoT network, network throughput increased by 25% and became 85 Mbps. Moreover, network latency dropped from 220 ms to 150 ms. As for packet loss, it became 10%, which means that packet loss became half as high. Although the energy consumption increased to 90 J, the positive influence of security enhancement outweighed this disadvantage.

It should be noted that, first of all, energy consumption increases due to the necessity to implement encryption and conduct intelligent intrusion detection. Second, it depends on the kind of enhancement implemented in a network. For instance, the implementation of AES encryption and an AI-based IDS leads to the high energy usage. Third, the reduction of unnecessary transmission through optimization of intrusion detection also saves energy. For instance, the implementation of a firewall reduces packet retransmissions.

3.3 Effectiveness of security enhancement in reducing cyber threats

Figure 7 summarises the effect of the security enhancement on threat occurrence, data integrity, unauthorized access attempts and network downtime.

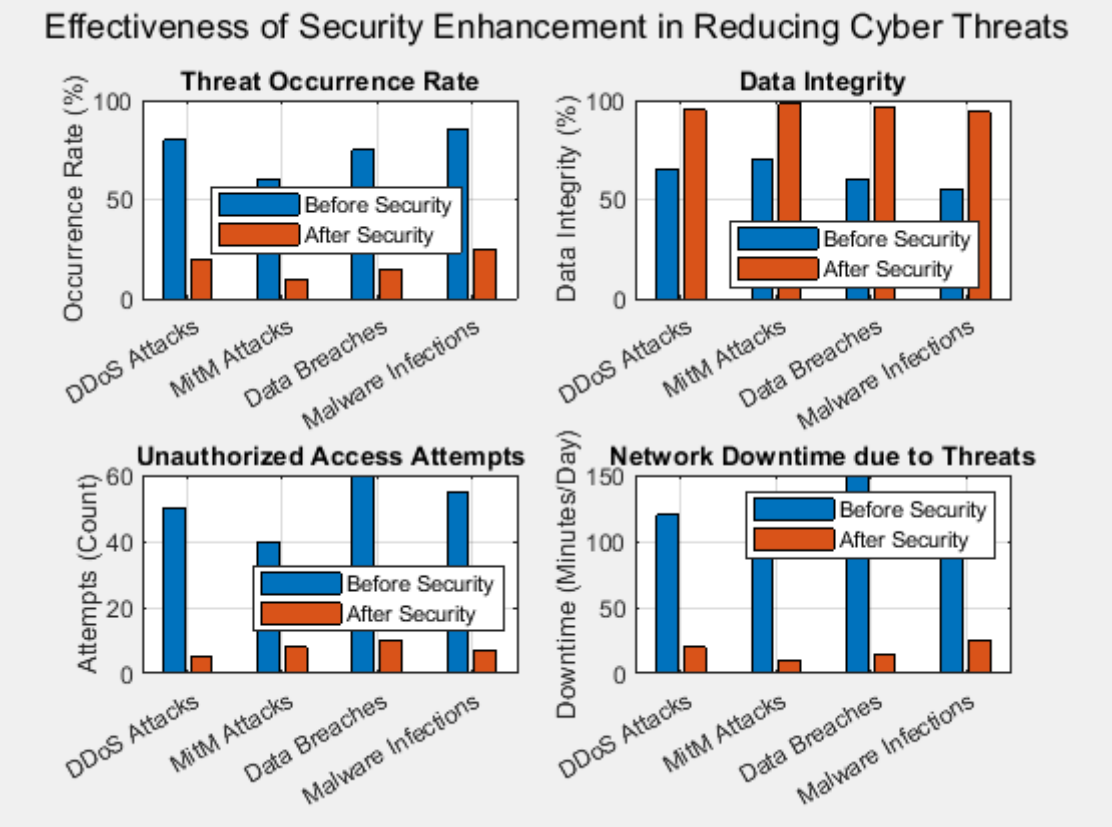


Figure 7. Effectiveness of security enhancement in reducing cyber threats.

Figure 7 shows the effect of security enhancement in terms of cyber threat occurrence, data integrity, unauthorized access, and network downtime. In relation to DDoS attacks, security enhancement

reduces occurrence rate to 20% and improves data integrity to 95%. Also, unauthorized access becomes rare, occurring only five times in a day and network downtime becomes much shorter (from 120 min to 20 min). As for MITM attacks, occurrence rate becomes 10% and data integrity equals to 98%. Moreover, unauthorized access occurs rarely only eight times a day. The average network downtime is 10 minutes. In turn, data breach becomes extremely rare, happening only 15 times per day, and its data integrity increases to 96%. As far as unauthorized access is concerned, its occurrence becomes rare 10 per day. Network downtime becomes 15 minutes. Finally, in the case of Malware infection, occurrence drops to 25% and data integrity becomes 94%. Unauthorized access occurs seven times a day and network downtime equals to 25 minutes.

4 Conclusion

The research was aimed at enhancing the security of IoT based telecommunication networks by investigating the problem through a systematic and objective-oriented approach, which provided valuable information and insight into a specific problem that was necessary for understanding how the performance of IoT based telecommunication networks can be boosted with the help of intelligent security mechanisms.

The study helped determine how cyber threats affect network performance. The results revealed that the throughput capacity can be limited to 50 Mbps, and the latency can reach 250ms when experiencing DDoS attacks. In addition, up to 30% of packets may be lost and the total energy consumption can rise to 80J. Similarly, MITM attacks proved to be dangerous as they increase latency to 250 ms, packet loss to 30% and energy consumption up to 80J. Thus, not only does network performance become noticeably impaired, but also the possibility to ignore these threats is rather unprofessional and irrational. In summary, this research demonstrates that IoT telecommunication networks are vulnerable to multiple cyber threats that impair their performance and reliability. However, security enhancement using FFNN-IDS is possible due to its capabilities in efficient threat detection, as well as reasonable computational costs that can be easily managed.

References

[1] Adeoye OB, Addy WA, Ajayi-Nifise AO, Odeyemi O, Okoye CC, Ofodile OC (2024a). Leveraging AI and data analytics for enhancing financial inclusion in developing economies. *Finance & Accounting Research Journal*, 6(3), 288–303.

[2] Adeoye OB, Addy WA, Odeyemi O, Okoye CC, Ofodile OC, Oyewole AT, Ololade YJ (2024b). FinTech, taxation, and regulatory compliance: Navigating the new financial landscape. *Finance & Accounting Research Journal*, 6(3), 320–330.

[3] Adeoye OB, Okoye CC, Ofodile OC, Odeyemi O, Addy WA, Ajayi-Nifise AO (2024c). Integrating artificial intelligence in personalized insurance products: A pathway to enhanced customer engagement. *International Journal of Management & Entrepreneurship Research*, 6(3), 502–511.

[4] Ajala OA, Arinze CA, Ofodile OC, Okoye CC, Daraojimba AI (2024a). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods.

[5] Ajala OA, Arinze CA, Ofodile OC, Okoye CC, Daraojimba OD (2024b). Reviewing advancements in privacy-enhancing technologies for big data analytics in an era of increased surveillance. *World Journal of Advanced Engineering Technology and Sciences*, 11(1), 294–300.

[6] Alaba FA, Othman M, Hashem IAT, Alotaibi F (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

[7] Almohaimeed M, Albalwy F (2024). Enhancing IoT network security using feature selection for intrusion detection systems. *Applied Sciences*, 14(24), 11966. https://doi.org/10.3390/app142411966

[8] Alrefaei A, Ilyas M (2024). Using machine learning multiclass classification technique to detect IoT attacks in real time. *Sensors*, 24(14), 4516. https://doi.org/10.3390/s24144516

[9] Amoo OO, Atadoga A, Osasona F, Abrahams TO, Ayinla BS, Farayola OA (2024a). GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*, 11(1), 1338–1347.

[10] Amoo OO, Osasona F, Atadoga A, Ayinla BS, Farayola OA, Abrahams TO (2024b). Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Science and Research Archive*, 11(1), 1304–1310.

[11] Anajemba JH, Tang Y, Iwendi C, Ohwoekevwo A, Srivastava G, Jo O (2020). Realizing efficient security and privacy in IoT networks. *Sensors*, 20(9), 2609. https://doi.org/10.3390/s20092609

[12] Atadoga A, Osasona F, Amoo OO, Farayola OA, Ayinla BS, Abrahams TO (2024). The role of IT in enhancing supply chain resilience: A global review. *International Journal of Management & Entrepreneurship Research*, 6(2), 336–351.

[13] Atzori L, Iera A, Morabito G (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

[14] Barbosa GNN, Andreoni M, Mattos DMF (2024). Optimizing feature selection in intrusion detection systems: Pareto dominance set approaches with mutual information and linear correlation. *Ad Hoc Networks*, 159, 103485.

[15] Bella K, Guezzaz A, Benkirane S, Azrour M, Fouad Y, Benyeogor MS, Innab N (2024). An efficient intrusion detection system for IoT security using CNN decision forest. *PeerJ Computer Science*, 10, e2290.

[16] Bharadiya JP (2023). The role of machine learning in transforming business intelligence. *International Journal of Computational Artificial Intelligence*, 4, 16–24.

[17] Farayola OA (2024). Revolutionizing banking security: Integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Accounting Research Journal*, 6(4), 501–514.

[18] Funchal GS, Pedrosa T, de la Prieta F, Leitão P (2024). Edge multi-agent intrusion detection system architecture for IoT devices with cloud continuum. In *Proceedings of the* 2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS) (pp. 1–6). St. Louis, MO, USA.

[19] Kim S, Jung C, Jang R, Mohaisen D, Nyang D (2023). A robust counting sketch for data plane intrusion detection. In *Proceedings of the Network and Distributed System Security Symposium (pp*. 1–15). Internet Society.

[20] Koirala A, Bista R, Ferreira JC (2023). Enhancing IoT device security through network attack data analysis using machine learning algorithms. *Future Internet*, 15(6), 210. https://doi.org/10.3390/fi15060210

[21] Lai T, Farid F, Bello A, Sabrina F (2024). Ensemble learning-based anomaly detection for IoT cybersecurity via Bayesian hyperparameter sensitivity analysis. *Cybersecurity*, 7, 44.

[22] Musthafa MB, Huda S, Kodera Y, Ali MA, Araki S, Mwaura J, Nogami Y (2024). Optimizing IoT intrusion detection using balanced class distribution, feature selection, and ensemble machine learning techniques. *Sensors*, 24(13), 4293. https://doi.org/10.3390/s24134293

[23] Nguyen V-T, Navas RE, Doyen G (2024). Lightweight security for IoT systems leveraging moving target defense and intrusion detection. In *Proceedings of the NOMS* 2024-2024 IEEE Network Operations and Management Symposium (pp. 1–6). Seoul, Republic of Korea.

[24] Otokwala U, Petrovski A, Kalutarage H (2024). Optimized common features selection and deep-autoencoder (OCFSDA) for lightweight intrusion detection in Internet of Things. *International Journal of Information Security*, 23, 2559–2581.

[25] Piyush P, Gill NS, Gulia P, Rao DD, Mandiga Y, Pareek PK (2024). Systematic analysis of threats, machine learning solutions, and challenges for securing IoT environment. *Journal of Cybersecurity and Information Management*, 14(3), 367–382.

[26] Roopak M, Parkinson S, Tian GY, Ran Y, Khan S, Chandrasekaran B (2024). An unsupervised approach for the detection of zero-day distributed denial of service attacks in Internet of Things networks. *IET Networks*, 13, 513–527.

[27] Sharmila B, Nagapadma R (2023). Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. *Cybersecurity*, 6, 41.

[28] Sinha M (2024). SynFloWatch: A detection system against TCP-SYN based DDoS attacks using entropy in hybrid SDN. In *Proceedings of the* 25th International Conference on Distributed Computing and Networking (pp. 200–210). ACM.

[29] Vimal V, Muruganantham R, Prabha R, Arularasan AN, Nandal P, Chanthirasekaran K, Ranabothu GR (2022). Enhance Software-Defined Network security with IoT for strengthening the encryption of information access control. *Computational Intelligence and Neuroscience*, 2022, 1–10. https://doi.org/10.1155/2022/4437507

[30] Yang K, Wang J, Li M (2024). An improved intrusion detection method for IIoT using attention mechanisms, BiGRU, and Inception-CNN. *Scientific Reports*, 14, 19339.

[31] Zhu J, Liu X (2024). An integrated intrusion detection framework based on subspace clustering and ensemble learning. *Computers & Electrical Engineering*, 115, 109113.