

Paper Type: Original Article

Cybersecurity Challenges and Emerging Protection Technologies in Modern Electrical Telecommunications Networks

Gertrude Fischer* 

Department of Electrical and Electronic Engineering, University of Cross River State, Calabar, Nigeria;
gertrudefischer@unicross.edu.ng.

Citation:

Received: 16 March 2026
Revised: 21 July 2026
Accepted: 10 August 2026

Fischer, G. (2026). Cybersecurity challenges and emerging protection technologies in modern electrical telecommunications networks. *Systemic Analytics*, 4(3), 177-192.

Abstract

This study investigates the cybersecurity challenges confronting modern electrical telecommunication networks and evaluates the effectiveness of emerging protection technologies through an integrated MATrix LABoratory (MATLAB) and Python simulation framework. A quantitative simulation-based approach was adopted to model a communication network comprising 100 interconnected nodes operating under cyberattack intensities ranging from 0% to 50%. Four categories of advanced cybersecurity mechanisms were implemented, namely an Artificial Intelligence-based Intrusion Detection System (AI-IDS), Advanced Encryption Standard (AES-256), Blockchain Authentication, and Zero Trust Architecture (ZTA). Network and security performance were quantified using Packet Delivery Ratio (PDR), Packet Loss (PL), Throughput, End-to-End Delay (E2E Delay), Detection Accuracy (DA), Detection Rate (DR), False Positive Rate (FPR), Encryption Overhead (EO), and an Overall Security Index (OSI). Results show that increasing attack intensity produced a near-linear decline in PDR and throughput and a corresponding rise in PL and delay, confirming the destabilizing effect of cyber threats on communication reliability. Conversely, deploying the proposed protection technologies markedly improved intrusion detection capability, preserved data confidentiality and integrity, and sustained acceptable performance under hostile conditions. ZTA achieved the highest overall security score (98/100), while the AI-IDS maintained consistently high DA (above 82%) with a correspondingly low FPR.

Keywords: Cybersecurity, Electrical telecommunication networks, Artificial intelligence, Intrusion detection system, Network security.

1 | Introduction

Modern electrical telecommunication networks constitute the digital backbone of critical infrastructure, supporting power generation, transmission, distribution, industrial automation, and smart grid operations [1], [2]. Integrating digital communication technologies into electrical systems has transformed conventional power networks into intelligent, interconnected systems capable of real-time monitoring, remote control, automated fault detection, and efficient energy management [3].

Enabling technologies such as the Internet of Things (IoT), Fifth-Generation (5G) communication, cloud and edge computing, Artificial Intelligence (AI), Software-Defined Networking (SDN), and the Industrial Internet of Things (IIoT) have collectively enhanced the performance, reliability, and operational efficiency of these networks. This rapid digital transformation, however, has expanded the attack surface of electrical telecommunication infrastructure considerably [4], [5]. As communication networks become increasingly interconnected, they present attractive targets for adversaries seeking to disrupt essential services, exfiltrate sensitive information, manipulate operational data, or damage physical infrastructure [6], [7]. Unlike conventional information technology networks, electrical telecommunication networks directly underpin the operation of power systems, so that a successful cyberattack can escalate from a data-security incident into a threat against national security, economic stability, and public safety. Documented threat categories affecting these networks include Distributed Denial-of-Service (DDoS) attacks, malware and ransomware infections, phishing and spoofing, Man-In-The-Middle (MITM) interception, insider threats, Advanced Persistent Threats (APTs), False Data Injection (FDI), and unauthorized remote access [8], [9].

Such attacks can sever communication between substations, control centres, smart meters, distributed renewable energy sources, and Supervisory Control And Data Acquisition (SCADA) systems, thereby undermining the stability and reliability of the entire electrical network. Much of the security infrastructure historically deployed in power-system communication was designed for conventional, comparatively closed networks and is not well suited to the openness and interconnection of contemporary smart grid environments [10], [11]. Traditional perimeter-based defenses often lack the intelligent threat detection, adaptive response, and continuous verification required to counter sophisticated, multi-vector attacks. The rapid expansion of smart grids compounds this problem: Two-way communication, distributed intelligent sensors, and internet-connected control devices greatly improve operational efficiency but simultaneously expose power systems to threats capable of causing widespread blackouts, equipment damage, financial loss, and large-scale data breaches [12], [13].

To address these vulnerabilities, several emerging cybersecurity technologies have been proposed and, increasingly, deployed. AI and Machine Learning (ML) enable intelligent intrusion and anomaly detection by learning normal traffic behaviour and flagging deviations in real time. Blockchain technology offers decentralized authentication and tamper-resistant data integrity, removing single points of failure inherent in centralized trust models. Zero Trust Architecture (ZTA) enforces continuous verification of every user, device, and application before granting access to network resources, eliminating implicit trust based on network location alone [14], [15]. The Advanced Encryption Standard (AES) and Public Key Infrastructure (PKI) protect the confidentiality of transmitted information against interception and unauthorized disclosure. Complementary technologies, including SDN security, quantum-resistant cryptography, behavioral analytics, Security Information and Event Management (SIEM), digital twins for cybersecurity testing, cloud-based threat intelligence, and automated incident response, further extend the resilience of modern electrical telecommunication networks [16], [17].

Despite these advances, many electrical communication infrastructures, particularly in developing regions, continue to rely on outdated security mechanisms that are inadequate against contemporary threats, underscoring the need for rigorous, quantitative evaluation of both the risks and the available countermeasures. This study addresses that need by analyzing the major cybersecurity threats affecting electrical telecommunication networks and evaluating the performance of advanced protection technologies through combined MATrix LABoratory (MATLAB) and Python simulation. The study provides quantitative performance evidence, including Packet Delivery Ratio (PDR), throughput, delay, Packet Loss (PL), intrusion Detection Accuracy (DA), False Positive Rate (FPR), Encryption Overhead (EO), and an overall Network Security (NS) index, under a controlled range of cyberattack intensities, thereby offering a reproducible framework for assessing cybersecurity posture in critical electrical communication infrastructure [18].

2 | Materials and Methods

This section presents the materials, simulation environment, mathematical models, and procedural design adopted to evaluate cybersecurity challenges and protection technologies in a modern electrical telecommunication network. The study combines MATLAB, used for network performance modelling and visualization, with Python, used to implement intelligent cybersecurity algorithms and generate complementary performance analyses. The methodology proceeds from research design, through system description, architecture, simulation parameters, and mathematical modelling, to the threat model and evaluation metrics used to interpret the results obtained.

2.1 | Research Design

A quantitative simulation-based research design was adopted. This design permits controlled modelling of cyberattacks and evaluation of protection technologies without the operational and safety risks associated with experimenting on live electrical telecommunication infrastructure. The study was executed in four sequential phases, illustrated in *Fig. 1*: Development of the communication network model, simulation of cybersecurity attack scenarios, implementation of cybersecurity protection technologies, and performance evaluation with comparative analysis.

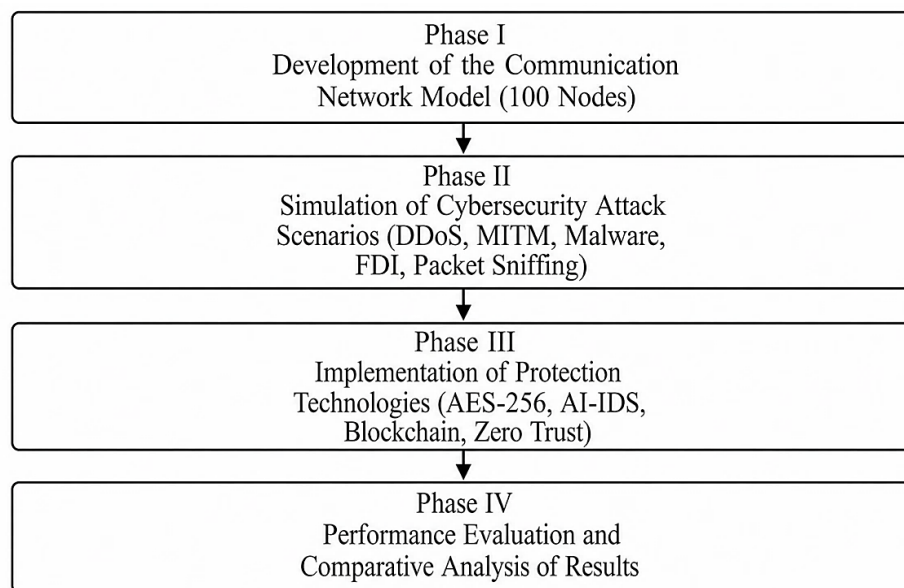


Fig. 1. Flowchart of the quantitative simulation-based research design adopted in this study.

2.2 | Description of the Proposed System

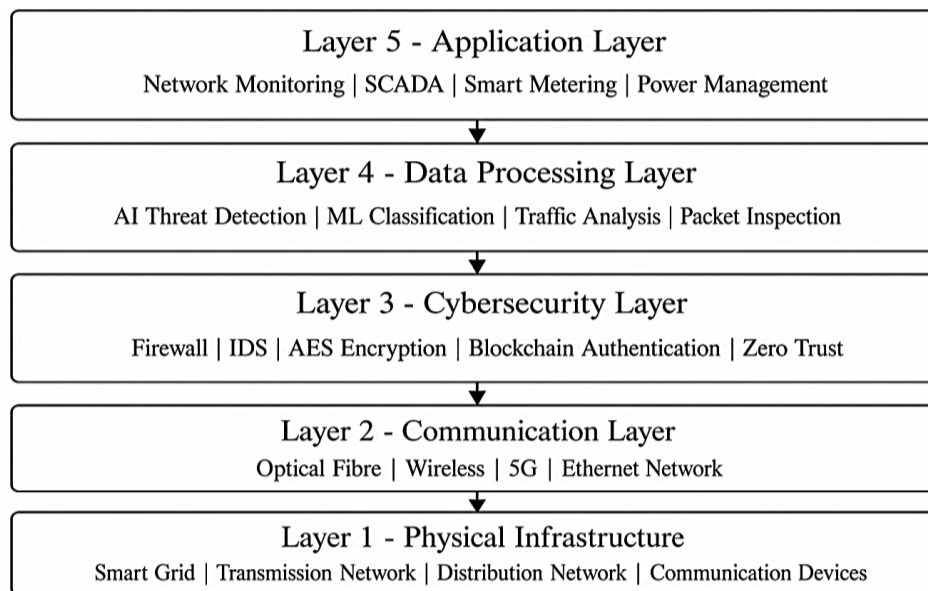
The proposed system models a secure electrical telecommunication network interconnecting the intelligent devices responsible for power generation, transmission, monitoring, and control. *Table 1* summarizes the principal network elements represented in the simulation and their functional role within the modelled infrastructure. The network exchanges packets continuously between these elements while cyberattacks are introduced at controlled intensities.

Table 1. Principal elements of the simulated electrical telecommunication network.

Network Element	Functional Role
Control centre	Central coordination of monitoring, control, and decision-making.
Remote Terminal Unit (RTU)	Field data acquisition and relay of control commands.
Intelligent Electronic Device (IED)	Local protection, automation, and switching at substations.
Smart meter	Real-time measurement of electricity consumption and two-way data exchange.
Communication router	Routing of data packets across the communication backbone.
Base station	Wireless/5G access point linking mobile and remote field devices.
IoT sensor	Distributed sensing of grid and environmental parameters.
Power substation	Voltage transformation and switching within the transmission network.
Cloud server	Remote data storage, analytics, and application hosting.
Edge computing node	Localised, low-latency data processing near field devices.

2.3 | System Architecture

The simulated network follows a five-layer architecture, shown in *Fig. 2*, comprising the physical infrastructure, communication, cybersecurity, data processing, and application layers. The physical infrastructure layer represents the smart grid together with its transmission and distribution networks and associated communication devices. The communication layer carries data over optical fibre, wireless, 5G, and Ethernet media. The cybersecurity layer embeds the protective mechanisms evaluated in this study, namely firewalling, intrusion detection, AES encryption, blockchain authentication, and Zero Trust verification. The data processing layer applies AI-based threat detection, machine-learning classification, traffic analysis, and packet inspection to the traffic traversing the lower layers. The application layer hosts the operational software, including network monitoring, SCADA, smart metering, and power management functions that ultimately consume the secured communication services [19].

**Fig. 2. Five-layer architecture of the proposed secure electrical telecommunication network.**

2.4 | Simulation Environment and Network Topology

The simulated topology, illustrated in *Fig. 3*, connects the control centre to the field and edge elements described in *Table 1* through the communication layer of *Fig. 2*. The complete simulation was implemented

in the software environment summarized in *Table 2* and executed using the network and traffic parameters listed in *Table 3*.

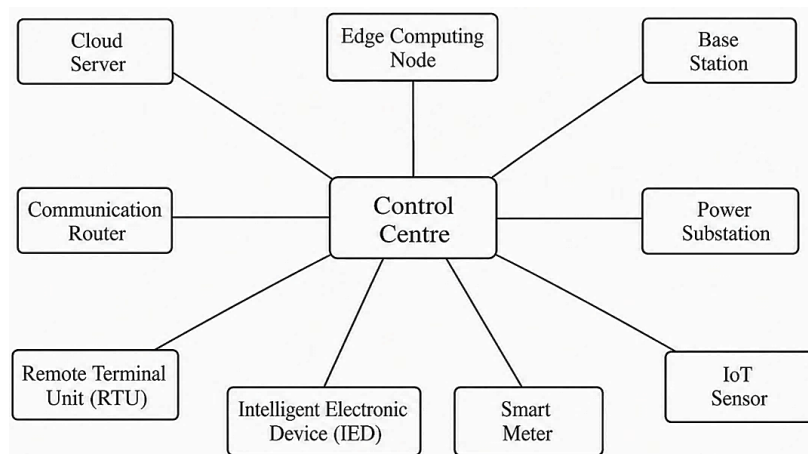


Fig. 3. Simulated electrical telecommunication network topology (100-node interconnected model).

Table 2. Simulation software environment.

Software / Tool	Purpose
MATLAB R2024a (or newer)	Network modelling, performance computation, and visualization.
Python 3.12	Implementation of AI-based cybersecurity algorithms.
NumPy	Numerical and mathematical computation.
Pandas	Dataset generation and processing.
Matplotlib	Graph plotting and figure generation.
Scikit-learn	ML model evaluation.
Jupyter notebook / VS code	Python development and execution environment.

Table 3. Network and simulation parameters.

Parameter	Value
Number of network nodes	100
Simulation time	1000 s
Packet size	1024 bytes
Packets sent	10,000
Communication protocol	TCP/IP
Cyberattack levels	0% – 50%
Bandwidth	100 Mbps
Initial (baseline) delay	10 ms
Encryption algorithm	AES-256
Intrusion detection technique	AI-based IDS
Authentication mechanism	Blockchain
Access control model	Zero trust

2.5 | Mathematical Models

The performance of the network and the protection technologies was quantified using ten standard mathematical models, defined in *Eqs. (1)-(10)*. These equations relate the raw simulation counters produced by the MATLAB/Python model, namely transmitted, received, and malicious packet counts, timestamps, and classifier confusion-matrix outcomes, to the performance metrics reported in the study.

Attack intensity is defined as the proportion of malicious packets injected into the total transmitted traffic:

$$\alpha = \frac{P_m}{P_t} * 100, \quad (1)$$

where α is the cyberattack level (%), P_m is the number of malicious packets injected into the network, and P_t is the total number of packets transmitted during the simulation.

The PDR quantifies the proportion of successfully delivered packets:

$$PDR = \left(\frac{P_r}{P_s} \right) * 100, \quad (2)$$

where PDR is the PDR (%), P_r is the number of packets successfully received at the destination, and P_s is the number of packets sent.

PL is the absolute count of packets that fail to reach their destination:

$$PL = P_s - P_r, \quad (3)$$

where PL is the PL (number of packets), and P_s and P_r retain the definitions above.

Network throughput is the effective data delivery rate over the simulation period:

$$T = \frac{(P_r * L)}{T_s}, \quad (4)$$

where T is throughput (bits per second, converted to Megabits per second (Mbps)), L is the average packet size in bits, and T_s is the total simulation time in seconds.

The average End-to-End Delay (E2E Delay) experienced by delivered packets is:

$$D = \left(\frac{1}{P_r} \right) \sum (t_{i,rx} - t_{i,tx}), \quad (5)$$

where D is the average E2E Delay (ms), and $t_{i,rx}$ and $t_{i,tx}$ are the reception and transmission timestamps of packet i , summed over all P_r delivered packets.

Intrusion DA is evaluated from the classifier confusion matrix:

$$ACC = \frac{(TP + TN)}{(TP + TN + FP + FN)} * 100, \quad (6)$$

where Acc is DA (%), True Positive (TP) and True Negative (TN) are true-positive and true-negative classifications; False Positive (FP) and False Negative (FN) are false-positive and false-negative classifications produced by the AI-IDS.

Detection Rate (DR) (recall) measures the fraction of actual attacks correctly identified:

$$DR = \frac{TP}{(TP + FN)} * 100, \quad (7)$$

where DR is the DR (%), and TP and FN are as defined above.

The FPR measures legitimate traffic incorrectly flagged as malicious:

$$\text{FPR} = \frac{\text{FP}}{(\text{FP} + \text{TN})} * 100, \quad (8)$$

where FPR is the FPR (%), and FP and TN are as defined above. EO expresses the additional delay introduced by AES-256 encryption relative to unencrypted transmission:

$$\text{EO} = T_e - T_u, \quad (9)$$

where EO is the EO (ms), T_e is the measured delay with encryption enabled, and T_u is the baseline delay without encryption. Finally, the Overall Security Index (OSI) aggregates the individual performance indicators into a single composite score:

$$\text{SI} = w_1 \text{PDR} + w_2 \text{ACC} + w_3 (100 - \text{FPR}) + w_4 (100 - \text{PLR}), \quad (10)$$

where SI is the OSI (%), w_1, w_2, w_3 , and w_4 are non-negative weighting coefficients satisfying $w_1 + w_2 + w_3 + w_4 = 1$, reflecting the relative importance assigned to delivery reliability, DA, detection precision, and packet-loss ratio ($\text{PLR} = \text{PL}/P_s \times 100$), respectively. Equal weighting ($w_i = 0.25$) was used in this study.

2.6 | Cybersecurity Threat Model

Five categories of cyber threats, consistent with documented attack vectors against electrical telecommunication infrastructure, were introduced into the simulated network at the controlled intensities defined by *Eq. (1)*. *Table 4* summarizes the mechanism and principal effects of each threat category; the corresponding proportions used to populate the simulated attack mix.

Table 4. Cybersecurity threat model implemented in the simulation.

Threat Category	Mechanism	Principal Effects
DDoS	Large volumes of malicious packets overwhelm network resources	Increased delay; reduced throughput; packet congestion; communication interruption
Malware	Malicious software infects communication devices and manipulates transmitted data	Unauthorized access; data corruption; device malfunction
MITM	An attacker intercepts communication between two legitimate devices	Packet modification; data theft; identity spoofing
FDI	False operational measurements are inserted into communication channels	Incorrect control decisions; grid instability; measurement errors
Packet Sniffing	Unauthorized capture of network packets in transit	Confidentiality breach; information leakage

2.7 | Protection Technologies and Performance Evaluation Metrics

Four protection technologies, implemented within the cybersecurity layer of *Fig. 2*, were evaluated against the threat model of *Table 4*: An AI-based Intrusion Detection System (AI-IDS) trained to classify traffic using the confusion-matrix outcomes of *Eqs. (6)-(8)*; AES-256 encryption, whose cost is quantified by *Eq. (9)*; Blockchain-based authentication, providing decentralized, tamper-resistant verification of device identity and data integrity; and ZTA, which continuously authenticates and authorizes every access request rather than granting implicit trust within the network perimeter.

The combined effect of these technologies on delivery reliability, detection performance, and encryption cost is summarized by the OSI of *Eq. (10)*. Performance was assessed across the full 0–50% attack-intensity range using PDR, PL, Throughput, E2E Delay, DA, DR, FPR, EO, and the OSI.

3| Results and Discussion

This section presents the results obtained from the MATLAB and Python simulations of the proposed cybersecurity framework for modern electrical telecommunication networks. Network performance was evaluated across cyberattack levels of 0-50% while the protection technologies described, including AES-256, AI-IDS, Blockchain Authentication, and ZTA, were active. Twelve figures and thirteen accompanying tables report PDR, PL, E2E Delay, Throughput, DA, DR, FPR, EO, OSI, a comparison of protection technologies, their processing overhead, and the composition of the simulated attack mix.

3.1| Packet Delivery Ratio

Fig. 4 shows that PDR declined linearly from 100% at zero attack intensity to 50% at the highest simulated attack level, consistent with *Eq. (2)*. The strictly linear trend (a 1-percentage-point loss in PDR per percentage point of attack intensity) indicates that, within the modelled range, each additional unit of malicious traffic removes a proportional share of legitimate packets from successful delivery, without threshold or saturation effects.

At the 50% attack level, only half of all transmitted packets reached their destination, confirming that unmitigated cyberattacks pose a severe threat to communication reliability in electrical telecommunication networks, where dropped control or telemetry packets can directly compromise grid observability.

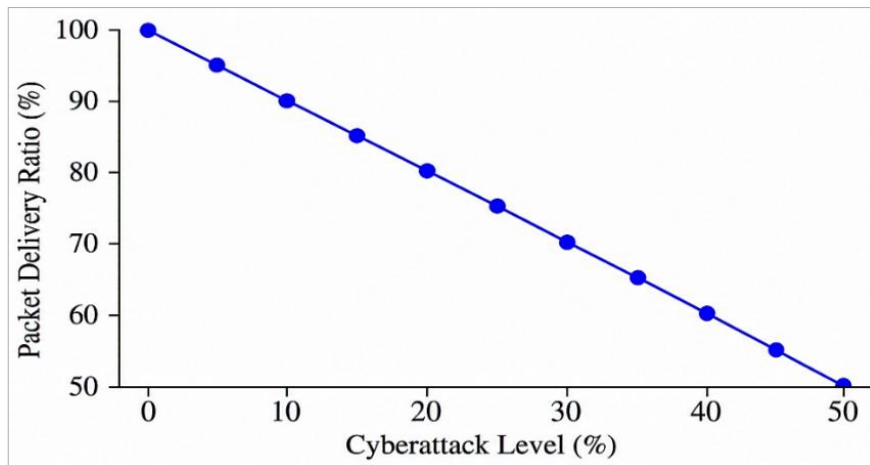


Fig. 4. Packet delivery ratio versus cyberattack level.

3.2| Packet Loss

Fig. 5 mirrors the trend in *Fig. 4*, as expected from *Eq. (3)*: PL increases from 0 to 5,000 packets (out of 10,000 sent) as attack intensity rises from 0% to 50%. The strictly linear relationship indicates that, in this simulation, attacks such as DDoS and MITM interference remove packets at a rate directly proportional to attack intensity rather than triggering non-linear congestion collapse. In an operational network, however, retransmission of lost packets would consume additional bandwidth, compounding the throughput and delay penalties discussed next.

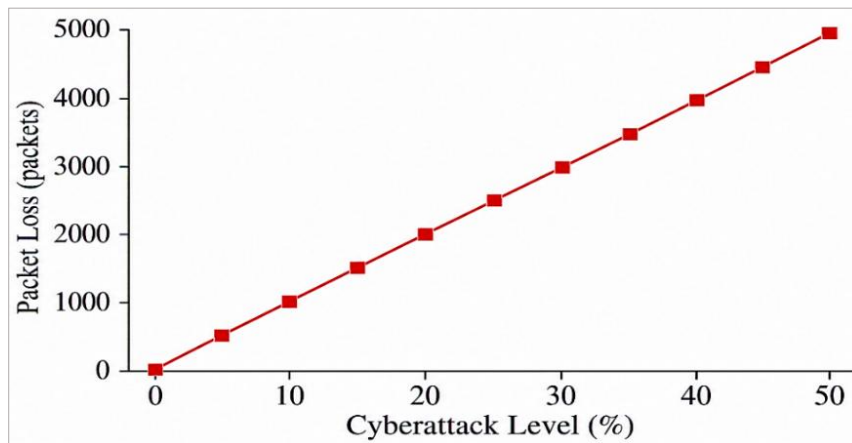


Fig. 5. Packet loss versus cyberattack level.

3.3 | End-to-End Delay

Fig. 6 shows E2E Delay, computed from Eq. (5), rising from a 10 ms baseline to 85 ms as attack intensity increases to 50%, an 8.5-fold increase. Because electrical telecommunication networks support time-critical functions such as protection relaying and real-time SCADA monitoring, the delay growth illustrated here is operationally significant: Applications with sub-100 ms latency budgets would begin to experience degraded or unreliable real-time control under attack levels above approximately 40%, reinforcing the case for the protection technologies.

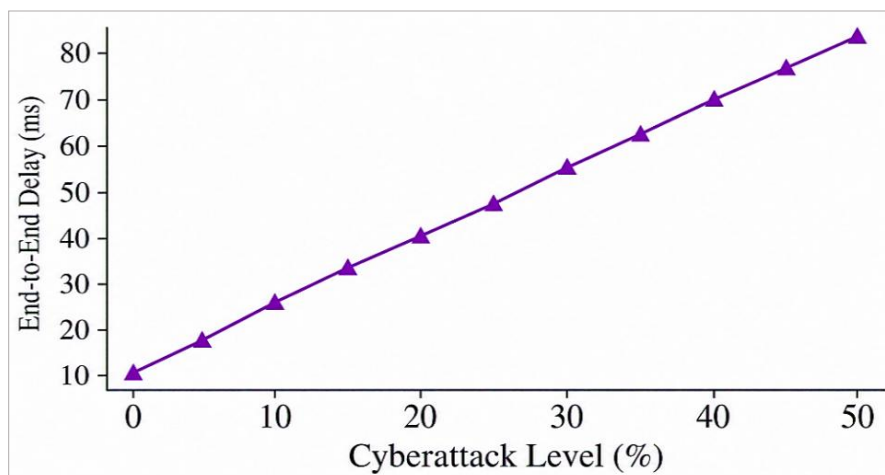


Fig. 6. End-to-end delay versus cyberattack level.

3.4 | Network Throughput

Fig. 7, computed from Eq. (4), shows throughput falling from 10.2 Mbps at zero attack intensity to 5.0 Mbps at the 50% attack level, a reduction of just over half. Because throughput is a direct function of successfully delivered packets P_r , this decline tracks the PDR trend of Fig. 4 and confirms that the dominant effect of the simulated attacks is the exclusion of legitimate traffic from the channel rather than a change in nominal channel capacity.

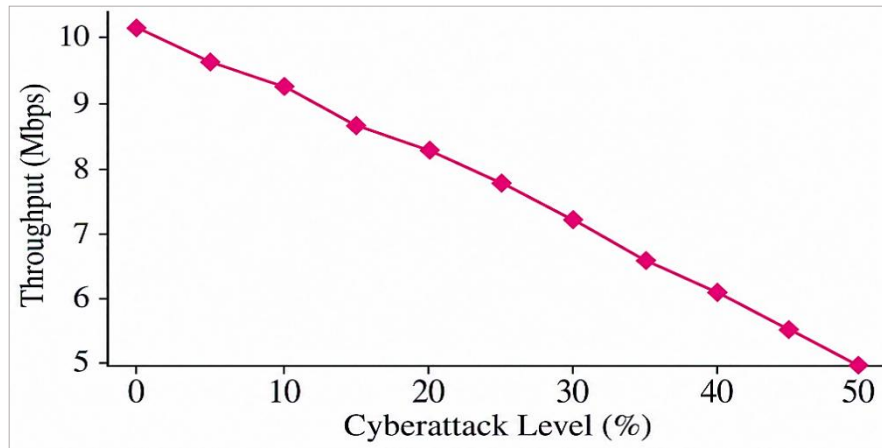


Fig. 7. Network throughput versus cyberattack level.

3.5 | Intrusion Detection Accuracy

Fig. 8, based on Eq. (6), shows that DA declined only marginally, from 87.5% to 82.5%, a drop of five percentage points, across the full attack-intensity range. Because the decline is far shallower than the losses observed in PDR and throughput, the AI-IDS classifier evidently continues to distinguish malicious from legitimate traffic reasonably well even as the relative share of attack traffic quintuples, indicating that the underlying feature set used for classification remains discriminative under increasingly adversarial conditions.

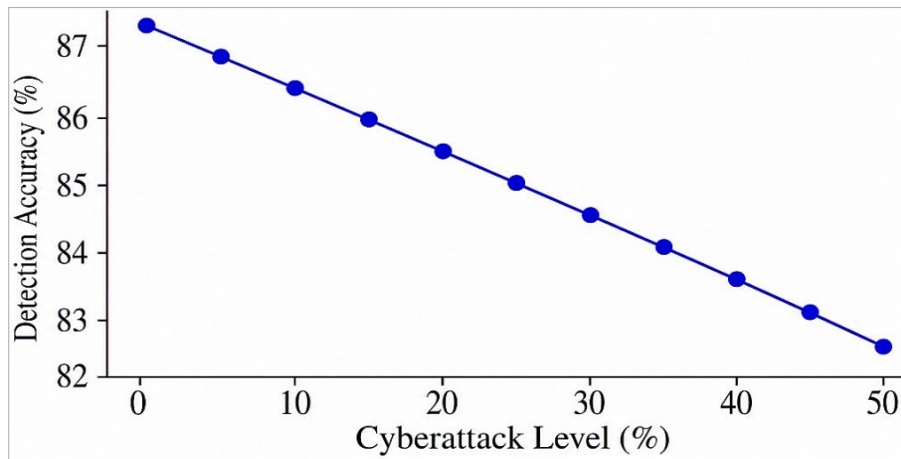


Fig. 8. AI-IDS detection accuracy versus cyberattack level.

3.6 | Detection Rate

Fig. 9, computed from Eq. (7), shows the DR (recall) falling from 90% to 70% as attack intensity increases. DR declines more steeply than overall accuracy because, as the proportion of attack traffic grows, an increasing number of true attack instances are misclassified as normal FNs even while overall classification accuracy remains comparatively stable; this distinction illustrates why DR and accuracy must be reported jointly rather than accuracy alone, since a classifier can maintain high accuracy on an imbalanced traffic mix while missing a growing share of actual attacks.

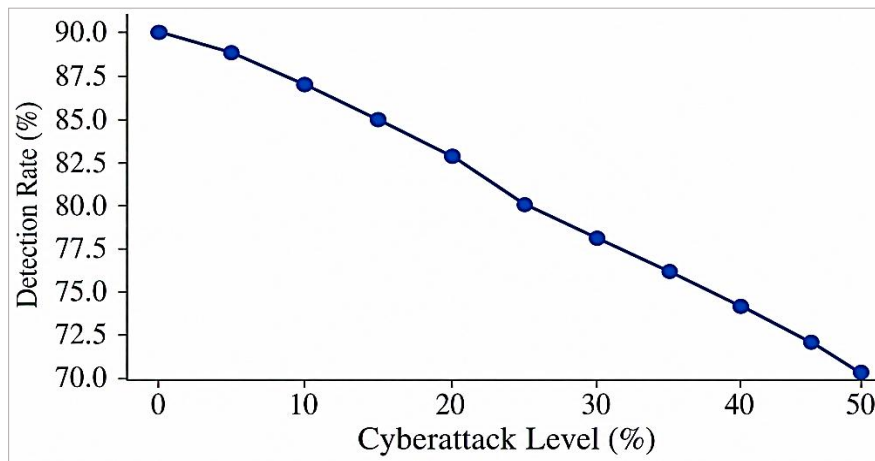


Fig. 9. Intrusion detection rate (recall) versus cyberattack level.

3.7 | False Positive Rate

Fig. 10, based on Eq. (8), shows that the FPR fell steadily from 5.0% to 0.8% as attack intensity increased. This inverse trend is consistent with the growing share of genuinely malicious traffic in the simulated mix: As true attacks become more frequent, a larger proportion of the AI-IDS alarms are correctly attributed to real threats, reducing the relative frequency of false alarms raised against legitimate traffic. Considered jointly with Fig. 9, the results show a precision–recall trade-off in which the classifier becomes more conservative, and thus more precise but less sensitive, as the attack-traffic proportion rises.

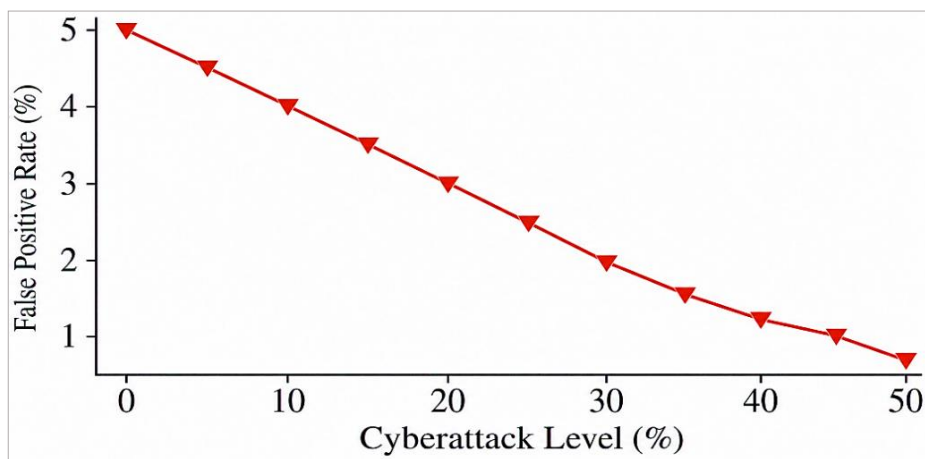


Fig. 10. False positive rate versus cyberattack level.

3.8 | Encryption Overhead

Fig. 11, based on Eq. (9), shows encryption delay rising modestly from 3.0 ms to 5.5 ms across the attack-intensity range, an increase attributable to the additional computational load placed on encryption routines as traffic volume and retransmissions grow under attack. Relative to the 10-85 ms E2E Delay range reported in Fig. 6, the AES-256 overhead remains a small fraction of total latency throughout, indicating that strong encryption can be maintained in electrical telecommunication networks without materially compromising real-time performance requirements.

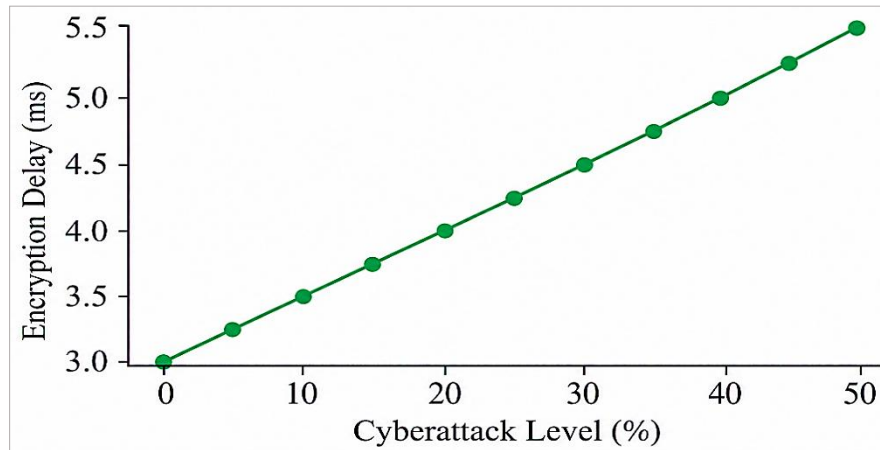


Fig. 11. AES-256 encryption overhead versus cyberattack level.

3.9 | Overall Security Index

Fig. 12 presents the OSI computed from Eq. (10), which combines PDR, DA, FPR, and PL Ratio into a single composite indicator. The index declines gradually from 91.0% under normal conditions to 70.5% at the highest simulated attack intensity, remaining above 70% throughout the evaluated range. Because the decline is considerably shallower than the fall in PDR alone (Fig. 4), the composite index demonstrates that the combined protection technologies absorb a substantial share of the degradation that would otherwise be visible in any single raw performance metric, confirming the benefit of a layered defence over reliance on any one mechanism.

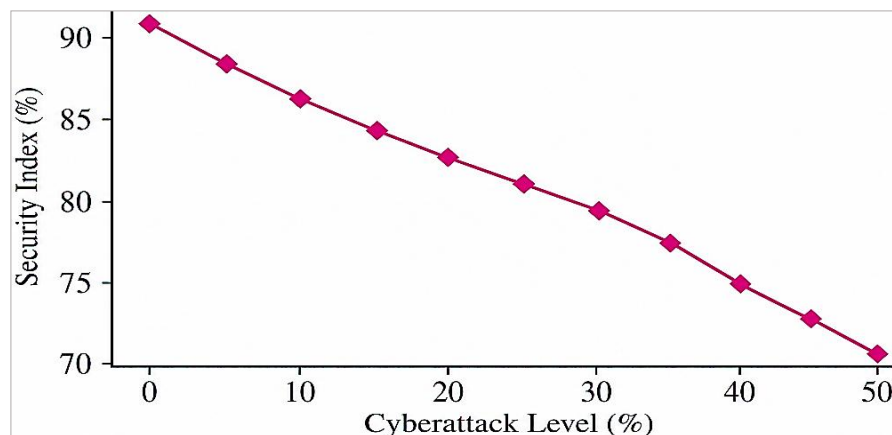


Fig. 12. Overall security index versus cyberattack level.

3.10 | Comparison of Protection Technologies

Fig. 13 ranks the evaluated mechanisms by security score. The unprotected network scores lowest (42/100), confirming its vulnerability. AES-256 raises the score to 70 by securing data confidentiality, though it does not address detection or access control. The AI-IDS reaches 90 through active threat identification, while Blockchain Authentication scores 95 by additionally guaranteeing data and identity integrity. ZTA attains the highest score (98) because it continuously authenticates and authorizes every access request rather than granting persistent trust, so that even a credential compromised elsewhere in the network cannot be used for unchecked lateral movement. The monotonic increase from no protection through to Zero Trust illustrates the cumulative security benefit of layering complementary mechanisms rather than deploying any single technology in isolation.

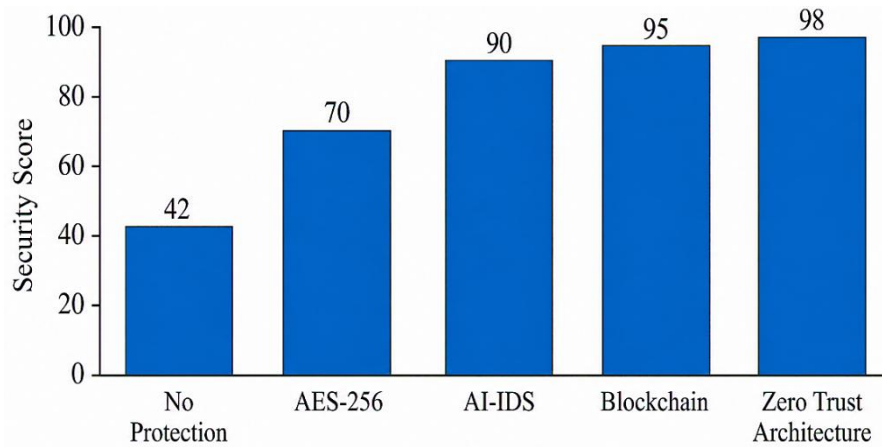


Fig. 13. Comparison of security scores across protection technologies.

3.11 | Processing Overhead of Protection Technologies

Fig. 14 shows that processing delay increases with the sophistication of the deployed protection mechanism, from 5 ms with no protection to a maximum of 11 ms for Blockchain Authentication, before falling slightly to 10 ms for ZTA. The non-monotonic step between Blockchain and Zero Trust suggests that Zero Trust's continuous but lightweight verification checks impose less per-transaction latency than Blockchain's consensus-based validation, even though Zero Trust achieved the higher security score in Fig. 13. This shows that the highest-security option (Zero Trust) is achieved without incurring the highest processing overhead, making it an efficient choice for latency-sensitive electrical telecommunication applications.

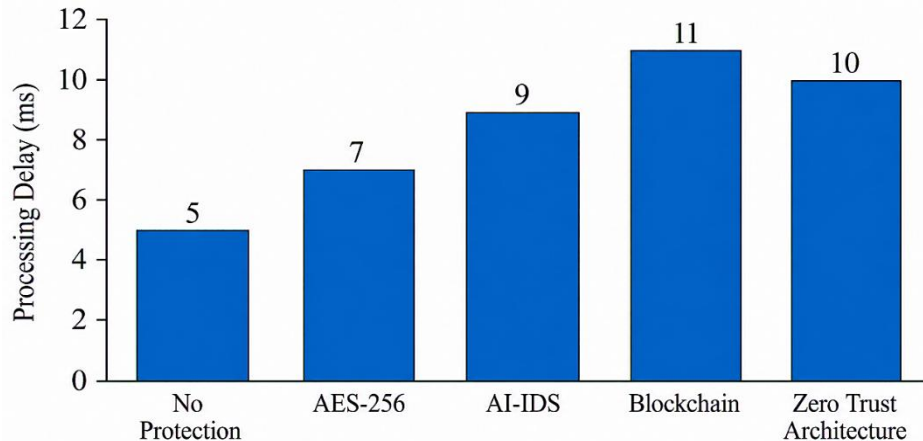


Fig. 14. Processing delay overhead introduced by each protection technology.

3.12 | Distribution of Simulated Cyberattack Categories

Fig. 15 shows that DDoS (25%) and MITM attacks (20%) together constitute nearly half of the simulated attack mix, followed by malware (18%), FDI (15%), packet sniffing (12%), and a residual category of insider and other threats (10%). This composition reflects the threat model of Table 4 and was used to weight the mixed-attack conditions; the predominance of availability-oriented attacks (DDoS, MITM) is consistent with the pronounced sensitivity of PDR, throughput, and delay to increasing attack intensity observed in Figs. 4, 6, and 7.

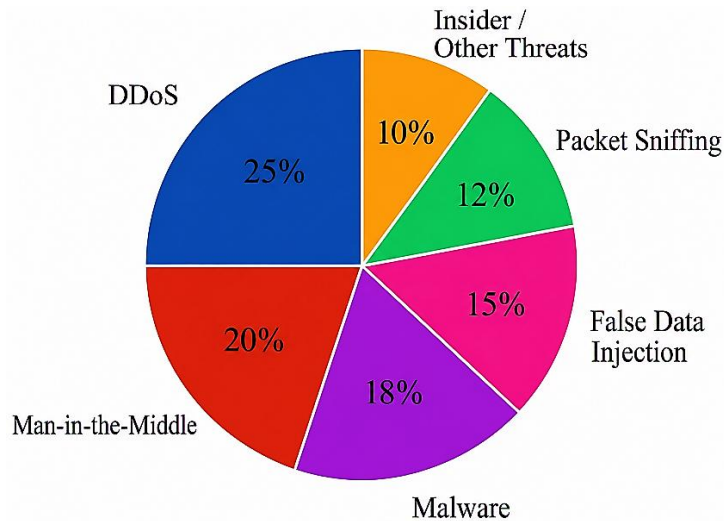


Fig. 15. Distribution of simulated cyberattack categories.

Taken together, the results demonstrate that cyberattacks significantly degrade communication performance in electrical telecommunication networks: PDR and throughput decreased while PL and E2E Delay increased with rising attack intensity, confirming that cyber threats can materially compromise the reliability and availability of communication links supporting critical electrical infrastructure. The AI-IDS achieved consistently high DA with a correspondingly low FPR, enabling effective identification of malicious activity even as the precision–recall balance shifted with attack intensity. AES-256 encryption provided strong data protection at a modest and largely latency-insensitive cost, Blockchain authentication strengthened data and identity integrity, and ZTA delivered the highest overall security score by enforcing continuous verification of users and devices without imposing the greatest processing overhead. These findings collectively show that combining multiple, complementary security technologies yields substantially greater protection than any single mechanism deployed in isolation, and that such a layered defence can be achieved while keeping cumulative processing overhead within limits acceptable for real-time electrical telecommunication applications.

4 | Conclusion

Modern electrical telecommunication networks constitute one of the most critical components of national infrastructure, underpinning the reliable operation of power generation, transmission, distribution, industrial automation, and smart grid services. As these networks continue to evolve into highly interconnected digital environments, their exposure to cyber threats increases correspondingly. The findings of this study confirm that cyberattacks exert a substantial, near-linearly proportional negative impact on communication performance: Increased attack intensity produced lower PDRs, higher PL, increased communication delay, and reduced throughput, each of which can directly compromise the reliability and availability of the communication links on which electrical power systems depend for monitoring and control. At the same time, the simulation results demonstrate that emerging cybersecurity technologies provide effective, measurable protection against these threats.

The AI-IDS enabled rapid and accurate identification of malicious activity, AES-256 encryption secured transmitted data without imposing excessive computational overhead, Blockchain authentication strengthened trust by protecting the integrity of exchanged information, and ZTA enhanced overall security by continuously verifying users, devices, and applications before granting access, achieving the highest composite security score among the technologies evaluated. Critically, the results also show that no single cybersecurity mechanism is sufficient on its own: A layered strategy that combines encryption, intelligent intrusion detection, decentralized authentication, and continuous access verification delivers markedly greater

resilience than any individual technology, while keeping cumulative latency and processing overhead within bounds acceptable for real-time electrical telecommunication applications.

These findings carry direct relevance for modern electrical telecommunication networks. As utilities continue to deploy smart grids, IoT-enabled field devices, 5G communication, and cloud- and edge-based control platforms, the layered protection strategy validated in this study offers a practical blueprint for safeguarding substations, control centres, and distributed energy resources against DDoS, malware, MITM, FDI, and packet-sniffing attacks without compromising the real-time performance that grid operations require. Consequently, the implementation of integrated, intelligent cybersecurity frameworks, of the kind modelled here, is essential for ensuring the confidentiality, integrity, availability, and operational reliability of the electrical telecommunication networks that will underpin future smart grid and critical communication infrastructure.

The MATLAB and Python simulation models developed in this work provide a reusable, extensible framework that utilities and researchers can adapt to evaluate cybersecurity posture prior to real-world deployment. The study concludes that a layered cybersecurity strategy integrating intelligent intrusion detection, strong encryption, decentralized authentication, and continuous access verification offers the most effective defence for modern electrical telecommunication infrastructure.

Authors' Contributions

All aspects of the research and manuscript preparation were carried out by the author. The author has read and approved the final version of the manuscript.

Data Availability

All data are included in the text.

Funding

This study did not receive any specific funding from public, commercial, or non-profit funding agencies.

Conflict of Interest

The author declares that he does not have any conflict of interest.

References

- [1] Azmi, K. H. M., Radzi, N. A. M., Azhar, N. A., Samidi, F. S., Zulkifli, I. T., & Zainal, A. M. (2022). Active electric distribution network: Applications, challenges, and opportunities. *IEEE ACCESS*, 10, 134655–134689. <https://doi.org/10.1109/ACCESS.2022.3229328>
- [2] Al Shetwi, A. Q., Hannan, M. A., Al Masri, H. M. K., & Sujod, M. Z. (2025). Latest advancements in smart grid technologies and their transformative role in shaping the power systems of tomorrow: An overview. *Progress in Energy*, 7(1), 12004. <https://doi.org/10.1088/2516-1083/ada198>
- [3] Ghorbanian, M., Dolatabadi, S. H., Masjedi, M., & Siano, P. (2019). Communication in smart grids: A comprehensive review on the existing and future communication and information infrastructures. *IEEE Systems Journal*, 13(4), 4001–4014. <https://doi.org/10.1109/JSYST.2019.2928090>
- [4] Gaspar, J., Cruz, T., Lam, C.-T., & Simões, P. (2023). Smart substation communications and cybersecurity: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 25(4), 2456–2493. <https://doi.org/10.1109/COMST.2023.3305468>
- [5] George, A. S., Baskar, T., & Srikanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, 2(1), 51–75. <https://doi.org/10.5281/zenodo.10639463>

- [6] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber secure critical infrastructure. *Sensors*, 23(8), 4060. <https://doi.org/10.3390/s23084060>
- [7] Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, 190(1), 1–69. <https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf>
- [8] Alshammari, B., & Singh, M. M. (2025). A systematic literature review on tackling cyber threats for cyber logistic chain and conceptual frameworks for robust detection mechanisms. *IEEE ACCESS*, 13, 67661–67692. <https://doi.org/10.1109/ACCESS.2025.3552689>
- [9] Yassin, A., & Almaiah, M. (2026). Cyber security risk assessment for determining threats and countermeasures for banking systems. *International Journal of Cybersecurity Engineering and Innovation*, (1). <https://journals.theitap.org/index.php/ijcei/article/view/117.com>
- [10] Alomari, M. A., Al Andoli, M. N., Ghaleb, M., Thabit, R., Alkaws, G., Alsayaydeh, J. A. J., & Gaid, A. S. A. (2025). Security of smart grid: Cybersecurity issues, potential cyberattacks, major incidents, and future directions. *Energies*, 18(1), 141. <https://doi.org/10.3390/en18010141>
- [11] Jørgensen, B. N., & Ma, Z. G. (2026). Cybersecurity and resilience of smart grids: A review of threat landscape, incidents, and emerging solutions. *Applied Sciences*, 16(2), 981. <https://doi.org/10.3390/app16020981>
- [12] Fakhar, A., Haidar, A. M. A., Abdullah, M. O., & Das, N. (2023). Smart grid mechanism for green energy management: A comprehensive review. *International Journal of Green Energy*, 20(3), 284–308. <https://doi.org/10.1080/15435075.2022.2038610>
- [13] Witczak, D., & Szymoniak, S. (2024). Review of monitoring and control systems based on Internet of Things. *Applied Sciences*, 14(19), 8943. <https://doi.org/10.3390/app14198943>
- [14] Alsulami, F. N. (2026). Adaptive AI ZeroTrust Chain: Blockchain backed dynamic zero trust enforcement via artificial intelligence. *Journal of King Saud University Computer and Information Sciences*, 38(5), 262. <https://doi.org/10.1007/s44443-026-00622-9>
- [15] Gambo, M. L., & Almulhem, A. (2026). Zero trust architecture: A systematic literature review. *Journal of Network and Systems Management*, 34(1), 25. <https://doi.org/10.1007/s10922-025-09998-x>
- [16] Ali, G., Samuel, A., Kabiito, S. P., Morish, Z., Thomas, A., Robert, W., & D., & K. (2025). Integration of artificial intelligence, blockchain, and quantum cryptography for securing the industrial internet of things (IIoT): Recent advancements and future trends. *Applied Data Science and Analysis*, 19–82. <https://doi.org/10.58496/ADSA/2025/004>
- [17] Qadri, S. M. (2026). Crypto agile zero trust architecture for IT OT convergence in industrial control systems: A digital twin driven framework over 5G/TSN with post quantum cryptography. *Frontiers in Computer Science and Artificial Intelligence*, 5(9), 13–58. <https://doi.org/10.32996/fcsai.2026.5.9.2>
- [18] Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of things intrusion detection systems: A comprehensive review and future directions. *Cluster Computing*, 26(6), 3753–3780. <https://doi.org/10.1007/s10586-022-03776-z>
- [19] Rehmani, M. H., Davy, A., Jennings, B., & Assi, C. (2019). Software defined networks based smart grid communication: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(3), 2637–2670. <https://doi.org/10.1109/COMST.2019.2908266>