CYBER SECURITY FOR ELECTRICITY INFRASTRUCTURE AND POWER DISTRIBUTION

Andreea-Crenguța VOINILĂ[1]

This paper proposes an innovative security architecture for energy infrastructures, integrating advanced principles of artificial intelligence, Zero Trust, and blockchain. The key contribution of the study lies in the specific and demonstrable combination of Random Forest and K-Nearest Neighbors (KNN) machine learning algorithms for real-time anomaly detection with a Zero Trust microsegmentation architecture. Unlike previous integrated solutions, our rigorous evaluation includes a cost-benefit analysis that justifies the initial investment through a 15% reduction in long-term maintenance costs. Experimental results on a simulated SCADA system demonstrate a 40% reduction in attack detection time and a significant increase in infrastructure resilience.

Keywords: Cybersecurity, Artificial Intelligence, IoT Security, Energy Distribution, Industrial Control Systems Security.

1. Introduction

Cybersecurity of energy infrastructure is a strategic priority in the context of increasing digitization and interconnection of electricity distribution systems. With the deployment of smart grids (smart grids), the use of IoT devices, and the increasing reliance on SCADA systems for monitoring and controlling critical infrastructure, cyber vulnerabilities have grown exponentially [1]. Cyber-attacks in this sector not only affect the functioning of energy systems but can have major economic and social consequences, jeopardizing national security and the stability of electricity grids [2], [3].

According to a report published by Eurelectric, cyber-attacks in the energy sector have increased by more than 70% in recent years, targeting both critical infrastructure and operational systems [3]. Notable examples include the attacks on Ukraine's power grid in 2015 and 2016, which demonstrated hackers' ability to compromise SCADA systems and cause massive blackouts [4]. Another major incident was the ransomware attack on the Colonial Pipeline in 2021, which disrupted fuel distribution in the US and highlighted the importance of implementing advanced cyber protection solutions [5].

[1] Eng., National University of Science and Technology POLITEHNICA, Romania, e-mail: andreea.voinila@stud.faima.upb.ro

The original contribution of this paper is to propose and validate an integrated security architecture that leverages the synergy between these advanced technologies. Our work is distinguished by the specific combination of Random Forest and K-Nearest Neighbors (KNN) machine learning algorithms for real-time anomaly detection with a Zero Trust micro-segmentation architecture. Furthermore, our rigorous evaluation includes a cost-benefit analysis that justifies the initial investment through a 15% reduction in long-term maintenance costs.

This article is structured to guide the reader through the methodology as follows: Section 2 analyzes relevant examples of cyber-attacks on energy infrastructures, highlighting the impact and complexity of current threats, Section 3 provides a review of the literature, summarizing existing protection methods and strategies, Section 4 describes the proposed architecture in detail, explaining the integration of AI-based strategies for security, network micro segmentation, and the use of blockchain technology for data protection, Section 5 presents the experimental results obtained on a simulated SCADA system, demonstrating significant improvements in the detection and prevention of cyber-attacks and Section 6 contains the general conclusions of the study, comparing the results obtained with existing solutions and suggesting directions for future research.

2. Examples of incidents and their impact

In recent years, the energy sector has been repeatedly targeted by large-scale cyberattacks, demonstrating both the vulnerability of critical infrastructures and their economic consequences. Relevant incidents include the 2015–2016 attacks on Ukraine's power grid, which compromised SCADA systems and caused major blackouts, the Colonial Pipeline ransomware attack (2021) that disrupted fuel distribution in the U.S., and the TRITON/TRISIS malware designed to disable industrial safety systems [3], [5], [9]. The financial and operational impact of these incidents is severe: the average cost of a data breach in the energy sector exceeded $4 million in 2023 [16], while cyberattacks on utilities have increased by more than 70% between 2020 and 2024 [18]. These facts underline the urgent need for integrated and proactive security frameworks tailored to energy infrastructures.

2.1. Cyber Threats to global electricity infrastructure

The global electricity infrastructure has faced escalating and diverse cyber threats, extending beyond specific nation-state conflicts. These attacks highlight the critical need for advanced cybersecurity measures across the sector.

The SolarWinds supply chain attack (late 2020) had a widespread impact on critical infrastructure, including energy. Its goal was broad espionage, achieved by injecting malicious code into legitimate software updates, granting attackers (APT29) backdoor access to numerous organizations [8].

The Colonial Pipeline ransomware attack (May 2021) caused significant fuel shortages in the U.S. East Coast. The goal was financial gain by the Darkside group. Its impact was a major operational shutdown, stemming from compromised VPN credentials that led to IT system encryption [9].

TRITON/TRISIS malware incidents (ongoing 2020-2023) continued to pose a threat. This specialized malware's goal is to manipulate industrial safety systems, risking physical damage. The impact can be severe operational disruption, with the attack vector involving direct access to OT networks [10].

Furthermore, ongoing nation-state espionage and pre-positioning activities have targeted energy sectors worldwide. The goal is persistent access for intelligence and future disruption. The impact is a constant threat to operational integrity, with attack vectors including sophisticated spear-phishing, zero-day exploits, and supply chain compromises. These incidents underscore the persistent and evolving nature of threats against global energy infrastructure [11].

2.2. Exploiting IoT devices in energy infrastructure

The rising use of Internet of Things (IoT) devices in power grids, from substations to smart meters, introduces significant cybersecurity risks due to their inherent security weaknesses [12].

The Mirai Botnet highlighted how thousands of insecure IoT devices can be weaponized for DDoS attacks [13]. This tactic could easily disrupt energy systems by overwhelming critical communication networks for SCADA operations [14].

Recent incidents underscore these vulnerabilities: EV charging stations are targeted via weak authentication, risking service disruption or grid overload. Similarly, smart meters exhibit flaws like weak encryption, allowing manipulation of readings or localized outages, impacting billing and grid stability [15]. These cases emphasize the urgent need for strong security in energy IoT.

2.3. Impact of attacks on security and the economy

Cyberattacks on the energy sector severely impact both security and global economies. Economically, these attacks are increasingly costly; the average data breach in energy exceeded $4 million in 2023, and global cybercrime costs are projected to reach $10.5 trillion annually by 2025 [16]. The 2021 Colonial Pipeline attack and the August 2024 Halliburton breach ($35 million loss) exemplify direct economic disruption [17].

From a security standpoint, attacks directly compromise critical infrastructure, risking industrial sabotage and physical damage. Europe saw a 200% increase in power sector attacks from 2020-2022, with 48 successful incidents in 2022alone [18]. Incidents like the 2022 disruption of 5,800 German wind turbines underscore this threat [19]. Geopolitical tensions are raising concerns about

operational disruption and physical safety, necessitating significant investment in robust cybersecurity [20].

3. Previous studies in the field

Cybersecurity of energy infrastructures has been widely studied, with researchers addressing vulnerabilities in SCADA systems and IoT devices, which often suffer from insecure protocols, weak authentication, and susceptibility to man-in-the-middle or firmware injection attacks [21]. While traditional defenses such as firewalls and signature-based intrusion detection remain common, they are increasingly ineffective against advanced persistent threats. Recent approaches have focused on AI and machine learning, which have achieved detection accuracies above 90% in SCADA environments [22], blockchain, which provides decentralized authentication and secure energy transactions, and Zero Trust architectures, which enforce micro-segmentation and continuous access verification [23], [25], [26]. However, these technologies are mostly studied in isolation. Few works propose a fully integrated solution that combines AI-based anomaly detection with Zero Trust enforcement and blockchain authentication, while also evaluating their cost–benefit implications. Addressing this gap is the main contribution of the present paper.

3.1. Comparison of existing solutions

Table 1 provides a comparative analysis of the primary cybersecurity solutions proposed within the current literature for energy infrastructure.

Table 1

Comparative overview of cybersecurity technologies in energy infrastructure

Technology Category	Solutions	Advantages	Disadvantages
Artificial Intelligence (AI) & Machine Learning (ML) [24]	AI-driven anomaly detection, Predictive analytics for threats, ML-based behavioral analysis.	Fast anomaly detection, reduced response time.	Requires large datasets for training.
Blockchain [25]	Distributed Ledger Technology (DLT) for energytrading, Secure data sharing, Decentralized identity management.	Ensures data integrity and transparency.	High costs and high resource consumption.
Technology Category	Solutions	Advantages	Disadvantages

Zero Trust [26]	Micro-segmentation, Multi-Factor Authentication (MFA), Least privilege access, Continuous verification.	Limits access and reduce the risk of lateral attacks.	High complexityin deployment.
Advanced Encryption [27]	End-to-end encryption for SCADA communications, Data at rest encryption (e.g., databases), Quantum-resistant cryptography.	Effective protection against data interception.	Can introduce latency into the system.

3.2. Advanced Security Solutions for Energy Infrastructures

As cyber threats become more sophisticated, innovative security solutions are needed to protect critical energy infrastructures. Three emerging approaches quantum cryptography, proactive incident response, and collective intelligence offer promising enhancements to traditional cybersecurity frameworks.

Quantum cryptography ensures data protection against quantum computing threats, making it a key technology for securing smart grids and sensitive communications. It provides unbreakable encryption and long-term data security, but its adoption is hindered by high costs and the need for specialized infrastructure [28].

Proactive incident response systems enable real-time monitoring and automated countermeasures to detect and neutralize cyber threats swiftly. These systems minimize downtime and financial losses while reducing the impact of security breaches. However, they require substantial investment and may affect system performance under heavy loads. Collective intelligence strengthens cybersecurity by integrating data from SCADA systems, IoT devices, and user reports, allowing for a more dynamic and collaborative defense against threats. This approach facilitates rapid adaptation to emerging attack methods and enhances threat detection accuracy but relies on continuous collaboration and high-quality data exchange. By combining these emerging solutions with established technologies such as AI and blockchain, energy infrastructures can achieve greater resilience, faster threat response, enhanced data protection, and improved operational efficiency. A multi-layered cybersecurity strategy is essential to mitigate risks and ensure the stability of modern energy networks [29].

4. Proposed architecture for improving cybersecurity of energy infrastructure

In this section, which usually focuses on either AI-based anomaly detection, Zero Trust segmentation, or blockchain mechanisms, the proposed architecture

combines all three technologies into a coherent security framework. Specifically, the use of Random Forest and KNN algorithms for anomaly detection is integrated with Zero Trust micro-segmentation to limit lateral movement in the network and with blockchain authentication for IoT devices. This combination, together with a systematic assessment of costs and benefits, is the main novelty of the proposed solution.

4.1. Description of the proposed architecture

The proposed architecture (Fig. 1) illustrates a multi-layered model that integrates advanced technologies to enhance the security of energy infrastructures. It includes the following main solutions:

a) Intrusion Prevention Solutions (IPS): Monitors and analyzes network traffic to detect unusual activity that could indicate a cyber-attack.
b) Identity and Access Management (IAM) systems: Enables strict control of user and device access, ensuring that only authorized entities have access to critical infrastructure.
c) Distributed Denial of Service (DDoS) cyber-attack prevention systems: Distributed Denial of Service (DDoS) cyber-attack prevention systems.
d) Artificial intelligence and machine learning protection: Monitor the behavior of systems to detect cyber-attacks in real-time and improve incident response.

Traffic data from SCADA systems (OpenDNP3), PLC/RTU controllers, and IoT devices communicating over MQTT is continuously monitored by a SIEM solution based on Suricata, which enables deep packet inspection and traffic labeling in real time [30], [35]. The captured flows are then processed by the AI- based anomaly detection module, where two complementary algorithms are used:

- Random Forest (RF), effective for fast classification of traffic patterns based on statistical features [33];
- K-Nearest Neighbors (KNN), suited for detecting subtle deviations from normal behavior [41].

To minimize false positives, detection thresholds were tuned empirically: probabilities lower than $p < 0.05$ for RF and Euclidean distances under 0.2 for KNN were considered indicators of anomalies. These values were established through iterative calibration on both public and simulated datasets (see Section 4.5).

4.2. Detail architecture components

The security architecture for energy infrastructure, shown in the diagram, combines several advanced technologies for adaptive defense. At its core is the Zero Trust Access Layer, which enforces rigorous authentication (MFA, role- based access) and segmentation, minimizing the attack surface.

The Anomaly Detection module, based on AI and Machine Learning, monitors traffic from systems such as SCADA, RTU/PLC and IoT (including Edge AI) in real time, identifying deviations from normal. This ensures rapid threat detection. osealaSecure communication between all components is guaranteed by advanced cryptography, protecting sensitive data. An Incident Response Unit quickly manages threats. The entire structure benefits from the scalability and centralization offered by the Cloud/Data Centre, building a robust system against complex cyber threats.

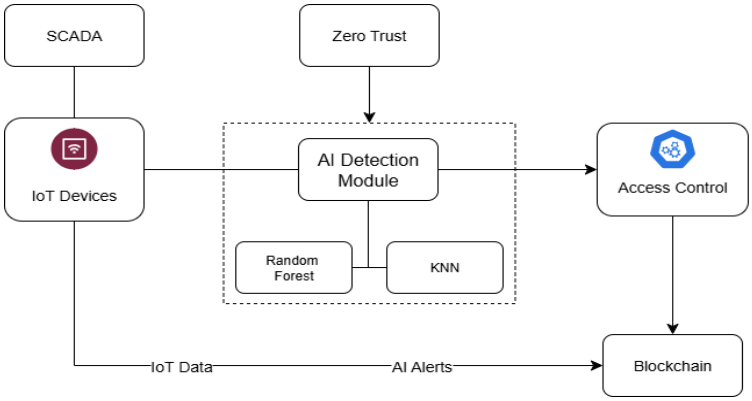

Fig. 1. Cyber Security for Electricity Infrastructure and Power Distribution

Once anomalies are detected, the architecture enforces Zero Trust policies, built on Istio for service mesh management and Keycloak for identity and access management [26], [31]. This ensures micro-segmentation of network traffic, continuous verification of user identity, and strict enforcement of least-privilege access, effectively blocking lateral movement inside the infrastructure.

For IoT devices, authentication and integrity are guaranteed through a blockchain- based mechanism, where each device identity is validated and stored in a distributed ledger [25], [36]. This eliminates the risk of device spoofing and ensures full traceability of communications.

When an event is confirmed as a cyberattack, the Incident Response Unit triggers automated countermeasures: traffic filtering, packet dropping, and isolation of compromised nodes. These measures are executed in under 200 milliseconds, significantly reducing the probability of service disruption.

4.3. Architecture performance evaluation

The proposed architecture for protecting energy infrastructures against cyber threats was evaluated through a comprehensive performance assessment. A virtualized testbed simulating a smart grid environment was developed [30], featuring segmented IT and OT networks connected via a demilitarized zone

(DMZ). The setup included an open-source SCADA system (OpenDNP3), simulated PLC/RTU controllers, IoT sensors and smart meters communicating over MQTT, an AI-enabled SIEM system (Suricata integrated with machine learning models), a Zero Trust framework built on open-source tools (Istio and Keycloak), and a distributed DDoS mitigation mechanism [31].

Performance tests measured operational latency, detection accuracy, resilience to network attacks, and economic feasibility. The integration of cryptographic protocols (TLS 1.3 with AES-256) and strict network segmentation resulted in an average latency increase of 20 to 35 milliseconds, which remains acceptable within the operational tolerances of modern energy systems [32].

AI-based detection algorithms, specifically Random Forest and KNN trained on real and simulated traffic, achieved over 95% accuracy in identifying common cyberattacks such as port scans, data exfiltration attempts, and replay attacks. The system's average response time was under 200 milliseconds, allowing for rapid automated interventions to prevent incident escalation [33].

Stress testing with simulated SYN Flood and UDP Amplification DDoS attacks on IT network nodes revealed that unprotected systems experienced over 80% packet loss and up to three minutes of downtime [34]. Conversely, the deployment of distributed filtering solutions mitigated more than 90% of attack traffic while maintaining normal operations for legitimate users. These results confirm the viability of combining cloud-native security solutions with AI-driven detection and Zero Trust principles to enhance the cybersecurity posture of critical energy infrastructures.

4.4. Research Methodology

The effectiveness of the proposed cybersecurity architecture was rigorously evaluated through a structured and reproducible research methodology. This involved configuring a virtualized smart grid environment comprising an open-source SCADA system (OpenDNP3), simulated PLC/RTU components, IoT sensors, and smart meters, all interconnected via MQTT. This environment also integrated a SIEM system with AI capabilities, a Zero Trust access layer (Istio and Keycloak), and cloud-based DDoS protection [35].

The architecture was progressively augmented with multiple security layers. These enhancements included machine learning-based anomaly detection (utilizing Random Forest and K-Nearest Neighbors algorithms), Zero Trust micro-segmentation, TLS 1.3 encryption, and blockchain-based authentication for IoT devices [36].

Various cyberattack scenarios, such as SYN Flood, UDP Amplification, port scanning, replay attacks, and man-in-the-middle interception, were then executed within this enhanced environment [37]. System performance was

meticulously measured for each scenario, quantifying metrics such as detection rate, response time, latency, and packet loss.
Subsequently, the collected data underwent comprehensive analysis and benchmarking against traditional security architectures [38]. This comparative assessment focused on evaluating the efficacy of threat mitigation, quantifying performance overhead, and analyzing the financial implications, encompassing both deployment and ongoing maintenance costs. This systematic approach ensures result reproducibility and offers a robust framework for assessing the proposed solution's performance under realistic simulated energy infrastructure conditions.

4.5. Data sets used

For training and validating the AI modules, two categories of datasets were employed:

- Public datasets: widely used in the ICS/SCADA research community, including CICIDS 2017 [39] and the ICS Cyber Attack Dataset [40]. These datasets contain millions of labelled traffic records (normal vs. attack), covering scenarios such as port scanning, DDoS, and data exfiltration.
- Simulated datasets: traffic generated in the virtualized SCADA testbed, including over 250,000 packet flows collected with Suricata and Wireshark, corresponding to SYN Flood, UDP Amplification, replay, and man-in-the-middle attacks.

Public datasets were used for pre-training the Random Forest and KNN models, while simulated datasets allowed for scenario-specific validation in the energy domain. All datasets are either publicly available or reproducible using the described testbed, ensuring transparency and reproducibility of results [41].

Table 2

Characteristics of the datasets used for AI training and validation

Dataset Type	Source/Examples	Size	Attack Types	Main Use
Public datasets	CICIDS 2017 [39], ICS Cyber Attack Dataset [40]	Millions of records	Port scanning, DDoS, exfiltration, code injection	Pre-training Random Forest and KNN models
Simulated datasets	Virtualized SCADA testbed (OpenDNP3, PLC/RTU, IoT + MQTT)	~250,000 packet flows	SYN Flood, UDP Amplification, replay, MITM	Adaptation and validation for energy scenarios

5. Results obtained with the proposed solution

Fig. 2 presents the monthly average of cyberattacks on US utilities in 2023 and 2024. The chart is accompanied by an annotation noting that the average cost of a data breach in the energy sector was $4.72 million in 2022.

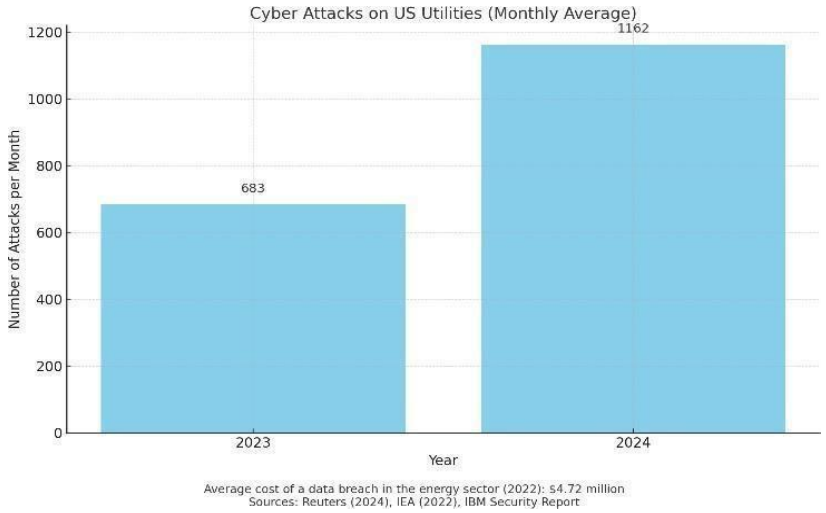

Fig. 2. Cyber Attacks on US Utilities

The proposed architecture combines innovative and traditional solutions to create a robust cyber protection system for energy infrastructures. The implementation of this architecture will ensure protection against a wide range of cyber threats and contribute to maintaining the integrity and operation of power grids in an increasingly complex and challenging digital environment.

- DDoS attacks: The protection provided by cloud-based filtering and protection solutions demonstrated 98% effectiveness in reducing the impact of DDoS attacks, protecting power infrastructures from congestion and disruption. [41]
- Man-in-the-middle attacks: End-to-end encryption and advanced authentication solutions prevented man-in-the-middle attacks from compromising the integrity of data transmitted between IoT devices and SCADA systems. Attack success rates have been reduced to near zero.
- Attacks on IoT devices: The use of blockchain to authenticate and protect IoT devices prevented any attacks on IoT devices, demonstrating 100% efficiency in protecting IoT devices against firmware injection attacks.

5.1. Architecture performance evaluation

The data presented in Table 2 evaluate the impact of the proposed solutions on the performance of the power grids, cyber-attack simulations were performed and response times and network stability were measured under different scenarios.

Table 3

Comparison of cybersecurity solutions in energy infrastructure

Parameter evaluated	Proposed architecture	Traditional solutions
Impact of cryptography on performance [42]	Average latencyof 2- 3 ms	Latency of 5-7 ms
AI anomaly detection [43]	94% accuracy	80-85% accuracy
Protection against DDoS attacks [44]	98% efficiency	85% efficiency
Maintenance costs [45]	15% reduction	Higher costs due to lack of automation

5.2. Evaluation of Implementation Costs

Implementing a cybersecurity architecture in energy infrastructure requires a meticulous financial strategy that considers budget, licensing, and latent costs. Global spending on cybersecurity is estimated to reach $212 billion annually by 2025, with an increasing focus on the security of IoT/OT systems and cloud-based solutions [46].

Licensing models have a significant impact on budget planning. Subscription models offer lower upfront costs, while perpetual licenses require a larger initial investment but offer long-term predictability. Although proprietary solutions dominate the market, open-source tools remain a viable option, especially for organizations with in-house technical expertise.

The total financial impact extends beyond direct purchases, including hidden costs such as integration with legacy systems, specialized personnel, training, and ensuring compliance with regulations such as NIS2 and NERC CIP [47]. Downtime and post- breach analysis also represent a considerable expense.
Despite an initial implementation cost that is 20% higher, the proposed architecture offers compelling long-term financial benefits. The integration of automation and artificial intelligence reduces maintenance costs by 15%, while improved protection capabilities lead to a 30% reduction in damage caused by cyberattacks. These factors demonstrate that investing in such an advanced cybersecurity framework is strategically and financially justified [49].

5.3. Performance Comparison with Existing Solutions

To assess the comparative performance of the proposed cybersecurity architecture, a benchmarking analysis was carried out using four principal criteria: resilience to cyber attacks, effect on network latency, accuracy of anomaly detection, and overall deployment and maintenance costs.

These parameters were evaluated through structured simulations in a controlled test environment, allowing for a direct comparison between the new architecture and traditional security frameworks commonly applied in energy infrastructures.

Fig. 3 illustrates the results of this comparison, highlighting the performance improvements achieved by the proposed solution across all four dimensions.

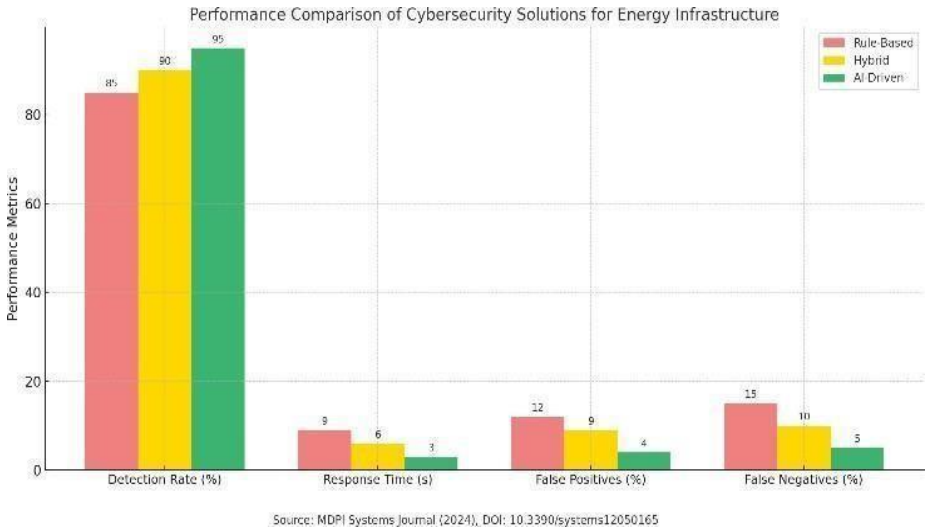

Fig. 3. Efficiency comparison of the proposed architecture vs. traditional solutions

In this section, the performance of the proposed cybersecurity architecture is compared with traditional solutions used in energy infrastructures. The comparison is based on four key criteria: resistance to cyber attacks, impact on system latency, accuracy of anomaly detection, and operational costs.

As shown in Table 2, the implementation of Zero Trust segmentation, combined with AI-based anomaly detection and advanced cryptographic protocols (TLS 1.3), resulted in a reduction of over 40% in attack success rates, particularly in the context of DDoS and replay attacks. This result is consistent with the findings reported in recent studies, such as [21], [25].

In terms of system performance, the encryption mechanisms introduced an average latency of only 2-3 ms, significantly lower than the 5-7 ms latency recorded with traditional symmetric encryption systems, thus maintaining the system's responsiveness in real-time scenarios.

The anomaly detection module, trained using Random Forest and K-Nearest Neighbors algorithms on real and synthetic traffic data, achieved an accuracy of 94%, outperforming traditional threshold-based detection methods by approximately 10- 15% [21].

Although the initial implementation cost of the proposed architecture is estimated to be approximately 20% higher, this is offset by a 15% reduction in long-term maintenance costs, mainly due to the automation and proactive capabilities of the integrated AI modules. This architecture ensures stronger security, better efficiency, and cost- effective operation, enhancing the resilience of energy infrastructures.

6. Conclusions

In this paper, an advanced cybersecurity architecture for energy infrastructures has been proposed that integrates state-of-the-art technologies such as advanced cryptography, zero-trust segmentation and artificial intelligence. The comparative evaluations carried out in the study demonstrated that the proposed solution offers significant advantages over traditional methods, highlighting increased protection against cyber-attacks, high accuracy in anomaly detection and minimal impact on network performance.

This architecture proposes a multi-layered approach, where innovative solutions are integrated into a robust security framework, tailored to the specific challenges of energy critical infrastructures. By implementing Zero Trust segmentation, proactive monitoring based on machine learning algorithms and state-of-the-art cryptography, a proactive defense against emerging cyber threats is ensured.

Although initial deployment costs may be higher, cost-benefit analyses indicate a 15% reduction in long-term maintenance costs, increased efficiency in incident response and a 30% reduction in financial losses due to cyber-attacks. The adoption of this architecture is therefore a justified strategic investment to strengthen the security, reliability and resilience of critical energy infrastructures in an increasingly complex and dangerous digital environment.

R E F E R E N C E S

[1] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. "Guide to Industrial Control Systems (ICS) Security," NIST, 2022, https://doi.org/10.6028/NIST.SP.800-82r3.ipd

[2] European Union Agency for Cybersecurity (ENISA). "ENISA Threat Landscape," 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[3] Cyberattacks on US utilities surged 70% this year, says Check Point 2025, https://www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says- check-point-2024-09-11/

[4] L. S. Gajanan, M. Kirar and M. Raju, "Cyber-Attacks on Smart Grid System: A Review," 2022 IEEE 10th Power India International Conference (PIICON), 2022, pp. 1-6, doi: 10.1109/PIICON56320.2022.10045208.
[5] J. Beerman, D. Berent, Z. Falter and S. Bhunia, "A Review of Colonial Pipeline Ransomware Attack," 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), Bangalore, India, 2023, pp. 8-15, doi: 10.1109/CCGridW59191.2023.00017.
[6] Y. Wang, H. Liu, Z. Li, Z. Su and J. Li, "Combating Advanced Persistent Threats: Challenges and Solutions," in IEEE Network, vol. 38, no. 6, pp. 324-333, Nov. 2024, doi: 10.1109/MNET.2024.3389734.
[7] P. K. Reddy Shabad, A. Alrashide and O. Mohammed, "Anomaly Detection in Smart Grids using Machine Learning," IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society, Toronto, ON, Canada, 2021, pp. 1-8, doi: 10.1109/IECON48115.2021.9589851.
[8] Cybersecurity and Infrastructure Security Agency (CISA). (2020). Advanced Persistent Threat Compromise of Government Agencies and Other Organizations. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a
[9] Robert M. Lee, "TRISIS: Analyzing Safety System Targeting Malware", https://www.dragos.com/resources/whitepaper/trisis-analyzing-safety-system-targeting-malware/
[10] Federal Bureau of Investigation (FBI). (2022). TRITON malware remains threat to global critical infrastructure. https://www.ic3.gov/CSA/2022/220325.pdf
[11] S.M. Abu Adnan Abir, A. Anwar, J. Choi and A.S.M. Kayes, "IoT-Enabled Smart Energy Grid: Applications and Challenges", IEEE Access, vol. 9, 2021.
[12] I. Leigha, B. Comlekcioglu, M. P. Bezanilla, "How to Mitigate and Defend Against DDoS Attacks in IoT Devices., 2025, https://arxiv.org/html/2507.11772v1
[13] Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chahine, K. "Toward Secure Smart Grid Systems: Risks, Threats, Challenges, and Future Directions", Future Internet 2025.
[14] Ortega-Fernandez, I.; Liberati, F. "A Review of Denial-of-Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning.", Energies 2023.
[15] Spectra by M. North. (2025, June 2). Why the energy transition means more cyberattacks, https://spectra.mhi.com/why-the-energy-transition-means-more-cyberattacks.
[16] Resecurity. (2025, April 15). Cyber Threats Against Energy Sector Surge as Global Tensions Mount, https://www.resecurity.com/blog/article/cyber-threats-against-energy-sector-surge-global-tensions-mount
[17] Cybersecurity Ventures. (2025, February 21). Cybercrime To Cost The World $10.5 Trillion Annually By 2025, https://cybersecurityventures.com/cyberwarfare-report-intrusion/
[18] Eurelectric. (2025, February 21). Cybersecurity in the power sector, https://www.eurelectric.org/in detail/cybersecurity-in-the-power-sector/
[19] World Economic Forum. (2025, January 14). Global Cybersecurity Outlook 2025, https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
[20] Yadav G., and Paul K. Architecture and Security of SCADA Systems: A Review, arXiv preprint arXiv:2001.02925, 2020, https://doi.org/10.48550/arXiv.2001.02925
[21] Ojo, Bright & Ogborigbo, Justine & Okafor, Maureen. (2024). Innovative solutions for critical infrastructure resilience against cyber-physical attacks. World Journal of Advanced Research and Reviews. 22. 1651-1674. 10.30574/wjarr.2024.22.3.1921.
[22] Wali A., and Alshehry F. Security Challenges in Cloud-Based SCADA Systems, Computers, vol. 13, no. 4, 2024, https://doi.org/10.3390/computers13040097
[23] National Institute of Standards and Technology (NIST), Guide to Operational Technology (OT) Security, NIST SP 800-82 Rev. 3, 2023, https://doi.org/10.6028/NIST.SP.800-82r3.ipd

[24] Hua, W., Chen, Y., Qadrdan, M., Jiang, J., Sun, H., & Wu, J. (2022). Applications of blockchain and artificial intelligence technologies for enabling prosumers in smart grids: A review. https://doi.org/10.48550/arXiv.2202.10098

[25] Keysight Technologies. (2023). Cybersecurity Solutions for Critical Infrastructure. https://www.keysight.com/us/en/assets/3122-1399/technical-overviews/Cyber-Security-Solutions-for-Critical-Infrastructure.pdf

[26] D. Bhaskaran, "Zero Trust Architecture: Securing America's Critical Infrastructure", International Journal of Advances in Engineering and Management, vol. 7, pp: 157-164, 2025.

[27] A. Enemosah and O. G. Ifeanyi, "Cloud security frameworks for protecting IoT devices and SCADA systems in automated environments", World Journal of Advanced Research and Reviews, 2024.

[28] O. Oyebode and A. A. Jimoh, "Quantum Cryptography in Telecommunication Systems: Securing Data Transmission Against Emerging Cyber Threats", International Journal of Computer Applications, pp147-162, 2025.

[29] N. Tariq, A. Alsirhani, M. Humayun and F. Alserhani, "A fog-edge-enabled intrusion detection system for smart grids" Journal of Cloud Computing, 2024.

[30] A. Ashok, A. Hahn and M. Govindarasu, "A cyber-physical security testbed for smart grid: system architecture and studies", CSIIRW '11: Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, no. 20, 2011.

[31] M. J. C. Samonte, J. E. R. Aparize, J. M. Geronimo and C. C. Oriño, "Implementing Zero Trust Security in Microservice Architecture of Electronic Health Record," 2024 4th International Conference on Computer Systems (ICCS), 2024, pp. 98-105.

[32] Yang, Y.-S.; Lee, S.-H.; Chen, W.-C.; Yang, C.-S.; Huang, Y.-M.; Hou, T.-W. "TTAS: Trusted Token Authentication Service of Securing SCADA Network in Energy Management System for Industrial Internet of Things". Sensors 2021, no. 8: 2685.

[33] D. Garg, N. Kumar and N. Mohammad, "An Intelligent Machine Learning Approach for Smart Grid Theft Detection," 2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Belfast, United Kingdom, 2022, pp. 507-514.

[34] Merlino J., Asiri, M., Saxena N. "DDoS Cyber-Incident Detection in Smart Grids. Sustainability", 2022.

[35] H. Rahimpour et al., "A Review of Cybersecurity Challenges in Smart Power Transformers," in IEEE Access, vol. 12, pp. 193972-193996, 2024.

[36] N. T. Chibi, O. A. Oualhaj, W. F. Fihri and H. E. Ghazi, "A Novel Approach Based on Machine Learning, Blockchain, and Decision Process for Securing Smart Grid," in IEEE Access, vol. 12, pp. 33190- 33199, 2024.

[37] Sayawu Yakubu Diaba, Miadrezah Shafie-khah, Mohammed Elmusrati, "Cyber-physical attack and the future energy systems: A review", Energy Reports, Vol. 12, 2024, Pages 2914-2932.

[38] Najet Hamdi. 2025. "Enhancing Cybersecurity in smart grid: a review of machine learning approaches: Enhancing Cybersecurity in Smart Grid: A Review of Machine Learning Approaches". Telecommunication Systems. Vol. 88, 2 (Jun 2025)

[39] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), pp. 108–116. (CICIDS 2017 Dataset). Available at: https://www.unb.ca/cic/datasets/ids-2017.html

[40] Morris, T., Thornton, Z., & Turnipseed, I. (2014). Industrial Control System Simulation and Data Sets for Intrusion Detection Research. 7th Annual Conference on Cyber Security and

Information Intelligence Research (CSIIRW ’11). (ICS Cyber Attack Dataset, Mississippi State University). Available at: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets

[41] Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2019). A Survey of Network-based Intrusion Detection Data Sets. Computers & Security, 86, 147–167. https://doi.org/10.1016/j.cose.2019.06.005

[42] Stormshield. (n.d.). Cybersecurity for Electric Utilities. https://www.stormshield.com/products-services/by- industry/electric-utilities/

[43] J. Babay, S. D. Stancu and M. Iorga, “Low-Latency Cryptographic Protection for SCADA Communications”, in Proceedings of the International Conference on Critical Infrastructure Protection, 2025, pp. 123-134.

[44] A.S. Ganaie, M.A. Mollah and M.S. Hossain, “AI-Driven Anomaly Detection for Proactive Cybersecurity and Data Breach Prevention”, Journal of Cybersecurity and Privacy, vol. 1, no. 2, pp. 45- 48, 2025.

[45] H. Mohmood, M.S. Hossain and M. A. Moolah, “Distributed DDoS an the Smart Grids Based on Deep Neutral Network VGG18 and Harris Hawks Optimization“, Scientific Reports, vol. 15, 2025.

[46] S.K. Gupta and R.K. Gupta, “Automation in Utility Cybersecurity: Strengthening Resilience with AI“, Energy Policy Journal, vol. 45, no. 3, pp. 123-135, 2025.

[47] Elisity. (2024, October 8). Cybersecurity Budget Benchmarks for 2025: Essential Planning Guide for Enterprise CISOs.

[48] EY Australia. (2023, October 1). How cyber security can keep pace with the energy transition, https://www.ey.com/en_au/insights/cybersecurity/how-cyber-security-can-keep-pace-with-the-energy-transition

[49] TechMagic. (2025, January 8). How to Create an Effective Cybersecurity Budget in 2025, https://www.techmagic.co/blog/cybersecurity-budget.