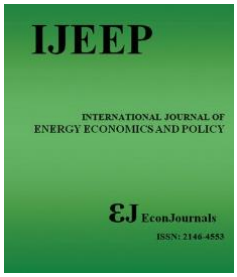


International Journal of Energy Economics and Policy

ISSN: 2146-4553

available at http: www.econjournals.com

International Journal of Energy Economics and Policy, 2025, 15(3), 614-628.

# Detecting Cybersecurity Threats in Digital Energy Systems Using Deep Learning for Imbalanced Datasets

**Zühre Aydın***

Energy Market Regulatory Authority, 06510, Ankara, Türkiye. *Email: zaydin@epdk.gov.tr

**Received:** 03 January 2025 **Accepted:** 06 April 2025 **DOI:** https://doi.org/10.32479/ijeep.19649

**ABSTRACT**

Energy management systems are experiencing significant transformations due to the adoption of innovative business models and advanced digital technologies. This study aims to investigate the intersection of artificial intelligence and cybersecurity within energy infrastructures, specifically focusing on developing a comprehensive methodology that effectively detects security threats in digitalized systems. The research evaluates existing energy policies and regulations while emphasizing the critical role of deep learning algorithms in enhancing cybersecurity through advanced threat detection, predictive analytics, automated responses, and continuous learning capabilities. A significant aspect of this study is the effective handling of imbalanced datasets, which is essential for optimizing deep learning performance in cybersecurity applications. Furthermore, the paper presents a comparative analysis of network intrusion detection systems and proposes a feature selection methodology by a novel feature reduction methodology designed to enhance deep learning capabilities for addressing specific challenges in imbalanced datasets of critical energy infrastructure. The expected results include insights into how artificial intelligence-driven methodologies can effectively mitigate cybersecurity threats in energy systems through a robust hybrid deep learning framework that addresses imbalanced datasets via advanced feature reduction techniques. Ultimately, this research contributes to enhancing both the immediate security of energy infrastructures and their long-term resilience against evolving cyber threats. By clarifying the contributions of deep learning methods to the literature on supervisory control and data acquisition system security, this study aims to bridge existing gaps and provide actionable insights for practitioners and policymakers in the energy sector and integrates regulatory frameworks (EU AI Act, NIST CSF 2.0, ISO/IEC standards) with a hybrid deep learning model addressing spatial, temporal, and structural intrusion patterns in SCADA systems using imbalanced data and a novel feature selection methodology within artificial intelligence.

**Keywords:** Critical Energy Infrastructure, Artificial Intelligence, Cybersecurity, Deep Learning
**JEL Classifications:** C55, L86, O38, Q48

## 1. INTRODUCTION

Deep learning (DL) algorithms significantly enhance cybersecurity (CS) in digitalized energy systems by enabling advanced threat detection, predictive analytics, automated response mechanisms, and adaptive intrusion detection systems (IDS). These capabilities contribute to improved data protection and real-time mitigation strategies. The integration of DL with existing CS frameworks offers a more holistic and dynamic approach to threat management. By combining traditional security protocols with artificial intelligence (AI), organizations can strengthen their defense mechanisms and build a more resilient CS posture. In energy management systems, AI serves as a unifying layer between intelligent devices and digital technologies, enabling the analysis of resource utilization and consumption trends while supporting environmentally optimized decision making (EC, 2010). It is a precursor for energy markets through the Internet of Things (IoT). IoT based data generation causes enormous and sensory data with a wide range of data streams. This huge amount of data, combine it with the latest innovations in AI, ML, Cloud Computing (CC), Big Data and Analytics (BDA), Business Intelligence (BI), Digital Twins (DT), CS for intelligent and secured organizational

processes, smarter decisions, regulation and efficient, flexible and sustainable digital system infrastructure (Tomazzoli et al., 2020; Javed et al., 2023). Therefore, utilities and organizations should understand the digital energy metamorphosis, novel energy strategies and design structures through data management and security concepts.

Various digital transformation project frameworks, methodologies and approaches lead to more complex and misunderstanding than they support transformation (Prisecaru, 2016). Smart Grid (SG) represents an evolved and intelligent version of the conventional network, embodying a two-way exchange through data and energy flow. This results in a smart and exceptionally sophisticated energy distribution system (Wu et al., 2022; Yenioğlu and Ateş, 2022). SG operates increased efficiency, facilitates improved interactions with customers, ensures widespread resilient voltage control, frequency regulation, and utilizes smart management. It also responds effectively to various system events (Zheng et al., 2020; Shahab et al., 2021). For instance, when a feeder or transformer fails, SG restores power flow to the load through its self healing capabilities automatically. Another example is seen in the use of smart meters to shape customer loads, which subsequently decreases peak demand on the power grid and reduces energy costs. The decrease in load triggers a cascade of advantages, including reducing energy loss, balancing the load on the network, and reducing the necessity for extra capital investments in the system (Gulzar et al., 2022).

Traditional network infrastructure consists of numerous substations and control centers, spanning extensive geographical regions. Each substation is equipped with various components, including transformers, lines, actuators, sensors, and phasor measurement units (PMU). Additionally, these substations feature supervisory control and data acquisition (SCADA) componenets that enable remote monitoring of the system elements (Teixeira et al., 2018). The energy sector places considerable emphasis on the protection and consolidation of critical infrastructure systems such as SCADA, given their central role in ensuring operational continuity and national energy security. SCADA systems serve as the foundational layer of critical infrastructure by enabling real time monitoring and control of essential parameters, such as voltage, current, pressure, and throughput, across dispersed assets. These systems integrate graphical user interfaces, alarm systems, data acquisition modules, and analytical tools to manage and supervise operations throughout all stages of energy generation and distribution (Almaleh et al., 2023).

Architecturally, SCADA systems are categorized into three structural models: monolithic, distributed, and network-based systems, each offering varying levels of scalability and interoperability (Marković-Petrović, 2020). SCADA environments incorporate programmable control devices such as Programmable Logic Controllers (PLC) and Remote Terminal Units (RTU), which interface with physical assets like pumps, circuit breakers, and valves, transmitting data to central control units for coordinated decision making (El Mrabet et al., 2018; Cui et al., 2018). Efficient SCADA operation requires seamless synchronization and communication across heterogeneous hardware and communication protocols, facilitated by both short-range and long-range network infrastructures.

The evolution of SCADA has been marked by increased adoption of commercial off-the-shelf components and hybrid communication protocols, contributing to their scalability and affordability. However, this has also heightened their exposure to cyber threats, particularly due to their expanded web based accessibility and integration with external networks (Kamboj et al., 2018). A significant body of literature addresses the cybersecurity vulnerabilities of SCADA systems, encompassing simulation frameworks, threat modeling, risk assessments, and mitigation strategies (Cui et al., 2018; Teixeira et al., 2018).

In light of the increasing frequency and sophistication of cyberattacks targeting Industrial Control Systems (ICS) and energy networks, there is a critical need for advanced cybersecurity solutions tailored to SCADA infrastructures. This study proposes a deep learning based framework aimed at enhancing the cyber resilience of digitalized energy systems. By leveraging the strengths of deep learning in anomaly detection, adaptive learning, and real time response, the approach presented herein contributes to the development of robust cybersecurity architectures capable of addressing the dynamic threat landscape faced by modern SCADA environments.

## 2. CRITICAL ENERGY INFRASTRUCTURE PROTECTION AND POLICY INFLUENCES

The existing power grids consist of multiple substations and control centers, covering extensive geographical areas. Each substation comprises various elements, including power lines, transformers, sensors, actuators and PMU, accompanied by SCADA units to remotely monitor the system components. Distributed Control Systems (DCS) are responsible for monitoring and managing processes distributed across various points within a single location. The definition of critical infrastructure aims to identify sectors that hold the utmost importance for a country's economy concerning security and stability. Definitions of critical sectors may slightly vary among countries due to their distinct cultures and economies. A comparative chart that maps critical infrastructure sectors will facilitate the exploration of general trends and country specific sectors (Upadhyay et al., 2021).

Smart technologies, including Smart Meters, Phasor Measurement Units (PMUs), Advanced Metering Infrastructure (AMI), Electric Vehicles (EV) and Electric Chargers, Renewable Energy Sources (RES) and Distributed Electricity Storage (DES) are introducing a wide area of new smart devices to the CEI that communicates and controls energy distribution. The emergence of novel infrastructure elements, business paradigms, and increased reliance on mobile devices within energy infrastructure settings brings new digital susceptibilities and expands physical entry/access points. These new applications oversee energy usage, encompassing retail service providers, energy and financial market participants, industrial, commercial, and residential consumers, necessitating

protection of confidential consumer and energy market data. Given the evolving landscape, there is a requirement for a comprehensive Critical Energy Infrastructure (CEI) security plan and roadmap, concentrating broadly on energy distribution systems, including control systems, smart grid technologies, and the convergence of cyber and physical security, where physical access to system components may affect cybersecurity (Hakansson et al., 2022).

In the 2018 "Critical Infrastructure Resilience and Security" survey conducted by the OECD, the most common critical infrastructure sectors were analyzed based on responses from 25 OECD countries. According to the survey, all countries regarded the energy sector as a critical infrastructure, ranking it first in importance (Linkov et al., 2018; OECD, 2021; 2022).

The European Commission (EC) drew attention to the risks on the energy sector critical infrastructures such as; power plants and pipelines. EC pointed out that the interruption or destruction of energy critical infrastructure would have a devastating effect on at least two European Union (EU) countries. The critical energy infrastructure (CEI), has become the most critical element of the countries as it has the power to affect all other infrastructures (Carrapico and Barrinha, 2018; EC, 2013; 2022).

The US Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DOE) made the recommendations at the 3rd National Cybersecurity Summit to ensure the security of SCADA critical infrastructures (CISA,2020) for cyber security trainings should be organized for industrial control systems operators and managers, incident response plans against cyber attacks should be updated and tested, a risk-based approach should be adopted to the security of industrial control systems machines and network. Framework for Improving Critical Infrastructure Cybersecurity (NIST) and the Critical Infrastructure Threat Information Sharing Framework are the key documents for CEI in DOE. The US documentation offers a wide range of standards, with the NIST being particularly significant. This document serves a complementary role, providing accessibility to every organization to enhance their cybersecurity level and evaluate their performance in this regard (Gordon et al., 2020; Tvaronavičienė et al., 2020). An established cybersecurity framework introduced by NIST was utilized to understand the necessary solution categories for protecting, detecting, reacting and defending against cyberattacks (Barrett, 2018).

The core components of the NIST cybersecurity framework outlines the methods to enhance the cybersecurity of any organization. This core is comprised of four key components such as; functions, categories, subcategories and references. The foundational components of the NIST framework include five cybersecurity functions and 23 categories of solutions, illustrated in Table 1. Within each function, the enumerated solution categories offer a robust starting point for identifying AI applications that can enhance cybersecurity awareness. For instance, the "Detect" function encompasses activities aimed at promptly identifying intrusions and anomalies to ensure vigilant monitoring, prevention, and recognition of cyber events. AI has the potential to enhance detection speed by monitoring both internal and external information sources, assessing the significance of these sources, and selecting and reducing source features. Moreover, AI can correlate information from various sources to identify unusual activities, thereby minimizing the risk of attacks through AI based intrusion detection within the anomalies and events domain. A a consequence, NIST published the Artificial Intelligence Risk Management Framework (AI RMF), outlining the ideal characteristics for AI systems: They should be valid and reliable, safe, fair and unbiased, secure and resilient, transparent and accountable, explainable and interpretable, and privacy enhanced. NIST aims to provide a framework that assists companies in assessing risks and making voluntary commitments within govern, identify, protect, detect, respond and recovery function steps and related solutions of each step (Barrett, 2018; Tvaronavičienė et al., 2020; NIST, 2023a).

NIST Cybersecurity Framework (NIST CSF 2.0) changes, particularly the inclusion of supply chain security and updated implementation tiers for evaluating cybersecurity readiness. In addition, the NIST AI RMF enhances the broader cybersecurity framework by addressing AI specific risks, focusing on governance, transparency, fairness, and accountability in AI systems. It complements energy system cybersecurity by ensuring that AI driven models are secure, resilient, and aligned with ethical and regulatory standards (Pascoe, 2023; NIST, 2023a; 2023b; NIST CSF, 2024).

In relation to Critical Energy Infrastructure (CEI) security, the Defending the European Energy Infrastructures, DEFENDER project's consortium has thoroughly analyzed CEI threats and needs, leading to the presentation and proposal of a draft roadmap for CEI protection. The DEFENDER project introduces innovative methodologies that offer a comprehensive explanation of fundamental ideas, techniques, fundamental truths and regulations that facilitate and oversee the safeguarding of CEI. These systems are characterized by their dynamic nature, diversity, widespread distribution, discretionary nature and extensive integration with both human elements and their operational surroundings. The DEFENDER platform offers a comprehensive system for data integration, identifying attacks, enhancing situational awareness, selecting optimized attack responses, and visualizing and managing controls. To navigate this intricate security landscape effectively, the strategies for establishing policies, doctrines and standards must possess adaptability, evolutionary potential and responsive management. This flexibility guarantees ample adaptability to effectively address both known and unknown threats in this complex security landscape. Moreover, incorporating integrated data from existing systems such as Intrusion Detection Systems (IDS), SCADA, Smart Meters, AMI, and PMU has been employed. Additionally, DEFENDER aims to create a European-level platform for exchanging incident information and insights into countermeasures. The resulting architecture follows big data principles and is managed using a suite of cutting edge open source services. Throughout the development and implementation process of the roadmap, DEFENDER has defined a series of strategies, milestones and goals. This roadmap outlines near-term, mid-term and long-term milestones in safeguarding CEI, as shown in Table 1 (Gugliandolo et al., 2018).

**Table 1: Critical energy infrastructure protection strategies, DEFENDER Roadmap and Goals**

| Strategies | | | |
|---|---|---|---|
| **1. Risk assessment** | **2. Protective measures** | **3. Manage incidents** | **4. Culture of security** |
| Near-term milestones (Project duration) | | | |
| 1.1. Common terms and measures specific to each CEI segment.<br>1.2. CEI segments categorization in Security Tiers. | 2.1. Evaluate the robustness and self-healing of new platforms, systems, networks, architectures, and policies. | 3.1. Tools to identify incidents across all levels of CEI.<br>3.2. Tools to support and implement incidents management commercially available. | 4.1. Public awareness of CEI resilience efforts.<br>4.2. Pan-European Stakeholders group to share mitigation strategies and define a security roadmap. |
| Mid-term milestones (4-7 years) by 2024 | | | |
| 1.3. Majority of infrastructure and asset owners baseline their security posture via energy subsector specific metrics. | 2.2. Scalable access control for all energy delivery system devices available.<br>2.3. Next-generation, interoperable solutions for secure communications. | 3.3. Incident reporting guidelines accepted and implemented by each energy subsector.<br>3.4. Real-time forensics capabilities and cyber event detection tools commercially available. | 4.3. Active involvement of citizens and Humans in the Loop for CEI protection.<br>4.4. Compelling business case developed for investment in CEI security. |
| Long-term milestones (8-10 years) by 2028 | | | |
| 1.4. Cyber-physical risk assessment tools commercially available. | 2.4. Self-configuring infrastructure enables operations' continuation during incidents. | 3.5. Lessons learned and best practices from cyber/physical incidents shared and implemented. | 4.5. Significant increase in the skilled employees and volunteers in CEI security. |
| Goals | | | |
| Security monitoring of all CEI levels and across cyber-physical domains. | CEI architectures able to continue operating during cyber/physical disruptions. | Fast self-mitigation of cyber/physical incidents, quickly returning to normal operations. | CEI security practices shared among stakeholders, academia, and government. |

The current CEI security roadmap provides high-level strategies that address the security requirements of CEI but does not prescribe a single specific course of action. Instead, agencies and organizations are advised to engage in cybersecurity initiatives, either individually or in collaboration with the EU Network and Information Security (NIS) directive and ENISA, leveraging their unique skills, capabilities, and resources while meeting their specific missions and requirements. The DEFENDER project serves as an autonomous stakeholders' group, contributing to relevant sectorial frameworks or regulatory initiatives aimed at shaping the CEI Security Roadmap (EC, 2013; Gugliandolo et al., 2018; EC, 2022).

In the context of risks and threats, arising from digital services expanding with transformation critical infrastructure operations are a growing concern. As integration in critical infrastructures increases, preventing and detecting disruptions in the industry will be possible with security policies for additional critical infrastructure protection measures. There are a large amount of intrusions or attacks as unexpected bad network connections, therefore securing ICS and SCADA environments essential. Intrusion detection is a way to detect network intrusion and this study gives a methodology for detecting network based anomalies for system continuity. In such detecting studies, artificial intelligence ensures valuable analysis. Policymakers and regulators are recognizing the potential AI applications within deep learning algorithms that could contribute to ensuring the safe operation of the energy sector. After extensive consultation with various stakeholders, the European Commission (EC) and Parliment released the proposal for a regulation on a European approach for AI, known as the Artificial Intelligence Act. In December 2023, the European Commissioner for Internal Market declared that an agreement had been achieved and energy sector included in high risk statement (EC, 2022; EP et al., 2022; NIST, 2023a; NIST CSF, 2024). As outlined within the AI Act from the EC and national strategies report, AI holds promise in aiding grid management, flexibility assets, and conducting electricity market operations. AI regulation in Europe is a challenging task, aiming to balance innovation and safety, with the white paper on AI in outlining policy options to mitigate human and ethical risks of AI use. The AI Act, proposed in April 2021, adopts a risk-based approach rather than a sector-based one, significantly impacting the EU energy sector due to its classification as critical infrastructure closely linked with climate change and environmental objectives (EC, 2020; 2022). Article 3 of the proposed regulation defines an Artificial Intelligence System as software created using one or more of various techniques and approaches such as deep learning, logic based, and statistical approaches, can generate outputs like content, predictions, recommendations, or decisions, influencing their environments based on human-defined objectives. However, potential high risks include transparency issues, reduced human autonomy, cybersecurity threats, market dominance, and potential manipulation of electricity market prices (EC, 2013; EC, 2022; Pascoe, 2023; NIST, 2023a; 2023b; NIST CSF, 2024).

In the context of enhancing intrusion detection within energy SCADA systems, several frameworks and standards offer guidance on information security and AI governance. ISO/IEC 27001 provides a comprehensive framework for information security management systems, focusing on safeguarding information assets across various technologies. ISO/IEC 42001, on the other hand, is tailored specifically for organizations managing AI systems, emphasizing ethical use, transparency, and accountability in AI operations. The NIST AI Risk Management Framework (NIST

AI RMF) offers a structured approach to managing AI related risks, aiming to enhance the trustworthiness and reliability of AI systems. The EU's AI Act establishes regulatory guidelines for AI applications, balancing innovation with safety through clear risk management protocols and human oversight. For energy SCADA systems, which are increasingly integrating AI technologies, aligning with these standards can bolster security measures. Implementing ISO/IEC 27001 ensures robust information security practices, while adopting ISO/IEC 42001 and adhering to the NIST AI RMF can address AI specific risks. Compliance with the EU AI Act further ensures that AI applications within SCADA systems meet stringent safety and ethical standards, thereby enhancing the overall resilience and reliability of critical energy infrastructure (Yatagha et al., 2024; Gstrein et al., 2024; Volkova et al., 2024; EC, 2023; NIST CSF 2024).

Building upon these standards and regulations, the proposed study contributes to the evolving regulatory and technical discourse by developing a hybrid AI based intrusion detection system tailored for SCADA environments, aligning with the principles outlined in ISO/IEC 27001, ISO/IEC 42001, NIST AI RMF, and the EU AI Act. The paper addresses core objectives such as ensuring data confidentiality, integrity, and availability (as per ISO/IEC 27001), while integrating explainable AI and transparency mechanisms (in accordance with ISO/IEC 42001 and the AI Act) through techniques like SHAP analysis and attention mechanisms. Furthermore, the risk based validation and performance evaluation of the deep learning models reflect alignment with the NIST AI RMF's emphasis on trustworthy and robust AI systems. The study's focus on imbalanced data, contextual awareness, and behavior based anomaly detection enhances compliance with both technical resilience (NIST, ISO/IEC 27001) and AI specific governance (ISO/IEC 42001, AI Act). As such, this research not only delivers a technically effective SCADA intrusion detection framework but also ensures its regulatory readiness and alignment with internationally recognized standards for secure and responsible AI deployment.

As outlined by the standards, AI Act and NIST Cybersecurity Framework, high risk AI applications such as SCADA must ensure compliance with transparency, reliability, and resilience requirements.

## 3. SOLUTIONS FOR CRITICAL ENERGY INFRASTRUCTURE THROUGH DEEP LEARNING

The implications of the AI Act for deep learning models in smart grids are particularly relevant when addressing the challenges associated with imbalanced datasets. In SCADA intrusion detection systems, where normal operational data often vastly outnumbers anomalous events, effective model training is critical. The AI Act mandates that data governance practices ensure datasets are sufficiently representative to enhance model performance and reduce false positives. This requirement is vital for developing reliable deep learning models that can accurately detect intrusions without compromising the integrity of critical infrastructure operations. The focus on ethical data practices aligns with the need to address issues related to dataset imbalance, ultimately contributing to safer and more accountable AI applications in energy management (Ferrag et al., 2020; Gstrein et al., 2024; Volkova et al., 2024).

As the types and frequency of cyber threats continue to grow, there is an increasing demand for innovative technologies to secure critical energy infrastructure components, particularly SCADA systems. These systems are essential for monitoring and managing energy flows but remain vulnerable to advanced cyberattacks such as Distributed Denial of Service (DDoS) attacks. Implementing robust IoT security measures is critical for safeguarding decentralized edge devices, enhancing the resilience of these systems against large-scale disruptions. Blockchain technology, another emerging solution, is increasingly adopted for its ability to provide privacy, integrity, and availability; the three pillars of cybersecurity. By creating immutable and transparent data logs, blockchain holds significant promise as a next-generation framework for managing CEI.

On the other hand, DL methods can be detection, prediction, and prevention components for SCADA communications through malicious network traffic detection. In the field of cybersecurity, deep learning techniques have been employed to monitor suspicious network activities. Many of these methods utilize DL to categorize network traffic, aiming to identify various types of attacks. Additionally, a significant portion of research focuses on distinguishing between malicious and non-malicious network traffic (Ahakonye et al., 2023; Zhang et al., 2024).

DL techniques, including Convolutional Neural Networks (CNN), Long Short Term Memory Networks (LSTM), and Graph Neural Networks (GNN), have become widely adopted in cybersecurity applications for digital energy systems due to their capacity to model complex, high-dimensional, and structured data. Recent literature increasingly emphasizes these architectures for detecting malicious behaviors within critical infrastructures.

CNN is particularly effective in extracting localized spatial features from structured inputs such as communication matrices, PMU signals, or spectrogram representations of log data. These characteristics enable CNN to detect subtle patterns of intrusion without requiring manual feature engineering, as demonstrated by Oswal et al. (2023), who confirmed the capability of CNN based architectures to identify spatial regularities in cyber physical environments.

LSTM networks, a subclass of Recurrent Neural Networks (RNN), are designed to capture long range temporal dependencies in sequential data. Their gated memory structure allows them to retain historical context over time, which is essential for detecting time-based threats such as replay or injection attacks in Industrial Control Systems (ICS) and SCADA systems. Yin et al. (2017) demonstrated the effectiveness of LSTM based models in accurately identifying temporally evolving intrusions, reporting improvements in classification performance over traditional methods.

GNN offers a powerful framework for representing graph-structured data, making them especially suited for modeling topologies in SCADA networks, smart grids, and distributed energy systems. These networks propagate feature information across nodes and edges, enabling the detection of relational anomalies and multi-hop attack behaviors that are often overlooked by conventional models. Peng et al. (2024) introduced a dynamic spatiotemporal GNN (DST-GNN) architecture for detecting cyberattacks in grid tied photovoltaic systems, leveraging system dynamics and topology to achieve superior detection performance.

The combined use of GNN, CNN, and LSTM architectures enables a comprehensive, multi dimensional approach to cybersecurity in energy systems. While CNN captures spatial features and LSTM models temporal sequences, GNN provides relational insights across networked components. This synergy supports advanced intrusion detection by simultaneously addressing the spatial, temporal, and topological dimensions of cyber physical infrastructure threats. These DL approaches collectively reduce reliance on traditional rule-based detection mechanisms and improve adaptability to heterogeneous network configurations (Sowmya and Anita, 2023; Zhang et al., 2024). Their capacity to process high-volume data and reveal latent patterns allows for timely and accurate identification of evolving threats, thus reinforcing the operational resilience of digitalized energy systems.

Through detecting and preventing digitalized energy system threats, the system has crucial security difficulties, since there are combining of heterogeneous communication networks such as technological or IoT devices and other wireless components distinguished by varying security risks (Khan et al., 2016). In smart grids, linking smart meters with other interconnected devices raises additional security considerations. The advancement of SCADA systems in smart power energy management amplifies potential threats if these systems fail to employ updated security measures. Intrusions into smart grids pose risks to the availability, integrity, and confidentiality of assets. Additionally, various forms of DoS attacks aim to disrupt network services and may result in significant disruptions such as power outages and unauthorized access to information (Teixeira et al., 2018; Akheel, 2023).

In order to safeguard critical assets within SCADA systems, it is crucial to determine weaknesses and deficiencies in the defense and control mechanisms to prevent potential breaches. This can be accomplished through employing techniques that detect weaknesses in the system and assess the level of protection against potential attacks, utilizing tools to gather pertinent information related to the target system under consideration. Numerous approaches have been suggested in the literature to safeguard SCADA systems against DDoS attacks, encompassing various mitigation and detection methods. Notably, DL techniques have proven to be highly effective in real-time detection of diverse types of attacks, including DDoS attacks (Akheel, 2023). DL based methodologies address these challenges by enabling real-time detection of anomalies, minimizing risks through predictive analysis, and adapting to evolving threats.

The finalized provisions of the EU AI Act classify AI systems into various risk categories, with a particular emphasis on 'high risk' applications that include AI systems used in the management and operation of critical energy infrastructure, such as SCADA and smart grids. These high risk systems are defined in Annex 3 of the Act, which specifies that AI applications intended for safety components in critical infrastructure covering sectors like electricity, water, gas, and heating must adhere to stringent compliance requirements. These stipulations aim to ensure that AI technologies are developed and deployed responsibly, safeguarding public safety and fundamental rights while promoting innovation in energy systems (Sovrano and Masetti, 2022; EC, 2024).

The AI Act's classification of critical energy infrastructures as high risk applications emphasizes the need for deep learning models to address challenges like imbalanced datasets, ensuring reliable and unbiased decision-making. Imbalanced datasets occur when the number of instances in one class significantly outweighs those in another. In cybersecurity, this often manifests as a disproportionate representation of normal versus attack data. For example, in a dataset used for intrusion detection, there may be thousands of normal network traffic instances compared to only a few instances of actual attacks. Cyber threats are constantly evolving, with attackers developing new strategies that can exploit vulnerabilities in critical systems (Presekal et al., 2023; Balla et al., 2023). Researchers can employ techniques such as oversampling the minority class or generating synthetic data to balance datasets. This helps improve model performance by providing more examples of rare events like cyber attacks. Deep learning models must adapt to these changes, which is difficult if they are trained on imbalanced datasets that do not reflect the latest threat scenarios. By mandating transparency, risk management, and fairness, the act supports the development of robust AI systems that can effectively detect and mitigate anomalies in these critical systems (Oswal et al., 2023).

### 3.1. Integration of NIST Cybersecurity Framework with AI-Relevant Subcategories and Imbalanced Data Issues

The NIST CSF 2.0 provides a comprehensive structure for improving the cybersecurity posture of critical energy infrastructures, which is well-aligned with the integration of DL technologies. The "Identify" function highlights the need to inventory AI systems and assess risks such as algorithmic bias or model vulnerabilities. This is particularly relevant in SCADA systems, where understanding dependencies and interconnections is crucial. Imbalanced data risk analysis is a key part of AI risk management during inventory and assessment. Within the "Protect" function, measures like secure data storage for training datasets and access control protocols align seamlessly with DL requirements, ensuring robust operational safeguards. Training and secure practices should address imbalanced data challenges to minimize biases and improve model generalization. For the "Detect" function, DL enhances cybersecurity through real-time monitoring of anomalies and adversarial activities. By incorporating AI-relevant subcategories such as adversarial attack detection, SCADA systems gain an additional layer of resilience. Models trained to handle imbalanced datasets can improve anomaly detection accuracy. The "Respond" function benefits from automated DL models that can rollback compromised

systems or trigger updates in real-time, mitigating the impact of incidents. Finally, the "Recover" function ensures the restoration of compromised systems, where DL models play a role in backup and recovery strategies, offering adaptive learning for future improvements. By bridging the NIST CSF with advanced DL methodologies, critical energy infrastructure gains a dual advantage: adherence to a globally recognized cybersecurity standard and leveraging cutting-edge technology to address unique challenges in the energy sector. The "Govern" function serves as a foundational element, guiding the development and oversight of cybersecurity risk strategies, policies, and responsibilities. In AI contexts, it ensures ethical governance, accountability, and compliance by addressing risks such as algorithmic bias and imbalanced data, aligning AI use with organizational objectives and regulatory frameworks. Write as this with commas AI model inventory, algorithm classification, and dependency mapping (Barrett, 2018; EC, 2022; NIST, 2023b; EC, 2024). For instance, applying the Identify and Detect functions in tandem with AI based feature reduction enhances the ability to pinpoint vulnerabilities in real time, as demonstrated in Table 2. These novel integrated strategies enable energy organizations to develop a more proactive and resilient cybersecurity posture.

While the Artificial Intelligence Act (Regulation EU 2024/1689) was formally adopted in 2024 and will become enforceable in February 2025, particularly for high-risk AI systems in critical domains such as digital energy infrastructures, this regulatory milestone underscores the urgency for aligning AI based cybersecurity solutions with emerging European legal standards and reinforces the role of the Govern function in the NIST Cybersecurity Framework, which mandates the formalization of AI governance structures, ethical oversight, accountability protocols, and compliance mechanisms to ensure lawful, transparent, and responsible deployment of AI systems, especially in contexts involving algorithmic bias and imbalanced data.

### 3.2. Cybersecurity and Deep Learning: Power Grid Intrusion Detection Methodology

DL has been extensively utilized in energy management systems for forecasting, anomaly detection, and cybersecurity monitoring, offering scalable solutions for remote supervision and real time optimization of energy inputs and outputs. According to recent literature, a wide range of machine learning and deep learning models have been employed for these tasks. Traditional algorithms such as k-Nearest Neighbors (kNN), Naïve Bayes (NB), Support Vector Machines (SVM), Artificial Neural Networks (ANN), Decision Trees (DT), and Random Forests (RF) continue to provide foundational baselines in both anomaly detection and system optimization scenarios (Ravipati and Abualkibash, 2019; Oswal et al., 2023). However, more recent advances emphasize the growing effectiveness of deep learning architectures, including CNN for spatial pattern extraction, LSTM for modeling temporal dependencies in time-series energy data (Yin et al., 2017; Yatagha et al., 2024), and GNN for capturing complex topologies in interconnected energy systems and communication infrastructures (Peng et al., 2024; Altaf et al., 2024). Collectively, these models reflect the shift toward more robust, scalable, and context aware intelligence in energy cybersecurity and management domains.

J48, based on the C4.5 decision tree algorithm, serves not only as a classifier but also as a feature selection tool due to its recursive attribute evaluation and interpretability. When integrated with RF, J48 enhances the feature reduction process by identifying and retaining the most relevant variables, thus improving model accuracy and efficiency. RF and J48 offer robust performance in high-dimensional and imbalanced datasets. Collectively, these models allow for a comparative assessment of classification performance within a reduced feature space, supporting the development of efficient intrusion detection systems tailored to digitalized energy infrastructures and SCADA security contexts (Senthilnayaki et al., 2013; Aljawarneh et al., 2019).

NSL-KDD dataset (2023) has features compatible with attack structures on SCADA systems and it is very important through CEI cybersecurity monitoring and contains essential intrusion types. Its imbalanced features include the unequal distribution

**Table 2: NIST components to include AI-relevant subcategories and imbalanced data issues**

| NIST CSF function | Category | AI-relevant subcategories and imbalanced data issues |
|---|---|---|
| Identify | Asset management | AI model inventory, algorithm classification, and dependency mapping |
| | Risk management | AI bias identification, model risk quantification, and mitigation strategies; imbalanced data risk analysis |
| | Supply chain risk management | Risk evaluation for third-party AI systems and datasets |
| Protect | Access control | Role-based access to AI models and datasets |
| | Data security | Secure storage and processing of training data; encryption of AI inputs/outputs |
| | Awareness and training | Specialized training on AI risks and cybersecurity, including challenges in handling imbalanced datasets |
| Detect | Anomalies and events | Monitoring AI behaviors for anomalies; detecting adversarial attacks, feature selection and classifiers within AI; improving detection in imbalanced datasets |
| | Security continuous monitoring | Real-time tracking of model performance and drift, and imbalanced issues |
| Respond | Incident response planning | Protocols for AI specific incidents, such as model poisoning or adversarial examples |
| | Mitigation | Automated rollback to prior model versions; reinforcement learning updates to address imbalanced datasets |
| Recover | Recovery planning improvements | Backup systems for AI model states and training datasets, Post-incident reviews focusing on AI specific vulnerabilities |
| Govern | Governance strategy and policy | Cybersecurity oversight policies, ethical AI governance frameworks, accountability protocols for AI driven decisions, algorithmic bias mitigation strategies, compliance with regulatory standards, and organizational alignment with mission driven AI objectives |

of normal and attack classes, with certain attack types being significantly underrepresented. The NSL-KDD dataset exhibits significant class imbalance, with a majority of records labeled as 'Normal' or common attacks like DoS, while rare attacks such as U2R and R2L are underrepresented, making them harder to detect. Features like src_bytes and dst_bytes are strongly correlated with majority classes, skewing model predictions. Additionally, the testing set introduces unseen attack types, amplifying the challenge of training models to handle imbalanced and diverse data effectively. Deep learning models trained on NSL-KDD must address these imbalances to ensure effective detection of minority class attacks. Techniques like oversampling, undersampling, or cost-sensitive learning can help mitigate these issues and improve model performance in identifying rare but critical threats like U2R and R2L attacks (Serinelli et al., 2020).

NSL-KDD was introduced to address issues of data redundancy and duplicate records. Consequently, the NSL-KDD dataset contains a more modest number of records compared to the KDD Cup 99 dataset, and it demonstrates superior performance relative to KDD Cup 99. To avoid biased outcomes, redundant records were eliminated from the dataset before applying the classifier. The remaining records were found to be rational and adequate in both the training and testing datasets. Many researchers have adopted it as the standard dataset for conducting experiments on various intrusion detection systems. The dataset includes features labeled as normal or attack types in both training and testing datasets, which are utilized for statistical and empirical analysis of intrusion detection techniques (Ingre et al., 2020). The feature types of it under content, basic, host based and traffic categories can be summarized as its 41 network features and five simulated attacks within below:

- Normal; is a normal activity performed by an authenticated user.
- DoS attacks; occur when there is an excessive consumption of bandwidth or unavailability of system resources (Neptune, Smurf, Back, Teardrop, Pod, Land).
- Probe attack; Gain access to the entire network before launching an attack (Ipsweep, Nmap, Satan, Portsweep).
- In User to Root (U2R) attack; the attacker first gains access to a normal user account, then exploits system vulnerabilities to obtain root access (Perl, Loadmodule, Rootkit, Buffer_ overflow).
- In Root to Local (R2L) attack; the attacker obtains local access by sending packets to a remote machine (Imap, Guess_passwd, ftp attacks etc.) (Asgharzadeh et al., 2023; Samunnisa et al., 2023).

The features capture various aspects of network connections, including traffic patterns, error rates, and host behaviors, which are essential for intrusion detection and network security analysis. The dataset's features and attack types divide the entire DL methodology into data processing, feature selection and intrusion detection. In this research, KDDTrain+ training set with total number of instances 125.973 and KDDTest+ testing set with total number of instances 22.544 have been used for attack and normal classes. Attacks features of data set are; attack duration, attack type, network metrics within bytes and counts, protocol_type and service (Table 3).

**Table 3: NSL-KDD analysis through number of attack type instances and dataset type (train and test data distribution)**

| Attack Type Instances | Training dataset | Test dataset |
|---|---|---|
| Normal instances | 67.343 | 9.711 |
| DOS instances | 45.927 | 7.458 |
| Probe istances | 11.656 | 2.421 |
| U2R instances | 52 | 200 |
| R2L instances | 995 | 2.754 |

Recent advancements in graph and DL based intrusion detection have shown promising results in cybersecurity applications across energy and IoT systems. Peng et al. (2024) proposed a dynamic spatiotemporal GNN model for detecting cyberattacks in grid-tied photovoltaic (PV) systems. Their method integrated CNN and GNN derivatives to capture both temporal patterns and the underlying graph topology of the power grid, demonstrating superior detection performance compared to baseline approaches. In Altaf et al. (2024) developed a sequential gated graph convolutional network (GGCN) for analyzing IoT network traffic and identifying sequential botnet attacks. Their model effectively combined time-stamped graph structures with specialized message-passing mechanisms, achieving notable improvements in detection accuracy, up to 25% for Mirai attacks, on imbalanced datasets. Meanwhile, earlier work by Nadiammai and Hemalatha (2014) focused on data mining techniques for intrusion detection, employing hybrid intelligent decision technologies that integrated both supervised classification and unsupervised clustering. Their approach included data filtering and ensemble classification, which proved effective on benchmark datasets such as NSL-KDD. Although the study primarily emphasized classical machine learning, it laid the groundwork for later semi-supervised deep learning models in network-based intrusion detection. The proposed method in the study was restricted to binary classification tasks. However, in the study conducted by Yin et al. (2017), a Recurrent Neural Network (RNN) algorithm was applied for both binary and multiclass intrusion detection. The performance of the RNN model was evaluated and compared against conventional machine learning algorithms, including J48 and RF, demonstrating its effectiveness in modeling sequential network traffic data.

In this paper; there is a comparison of DL methodology of network based intrusion detection for SCADA system continuity within imbalanced data intrusion attack detection scenarios. The paper aims to propose a potential security solution using a simulation framework that incorporates DL techniques for detecting DDoS attacks on SCADA systems. Based on the reviewed taxonomy of deep learning approaches in cybersecurity, the integration of LSTM, CNN, and GNN architectures in the proposed hybrid model is strategically designed to exploit their complementary strengths across the temporal, spatial, and structural dimensions of SCADA data. LSTM, as a recurrent neural network, effectively captures long-term temporal dependencies within sequential SCADA signals, enabling the detection of time-dependent anomalies and evolving attack patterns. CNN contributes by

extracting localized and hierarchical features from transformed representations of network traffic, facilitating the identification of spatial irregularities in communication flows. Meanwhile, GNN offers a graph-based perspective, modeling the relational structure of SCADA systems, such as the interconnections between sensors, actuators, and control units, allowing the model to propagate contextual information and capture topological dependencies. The combined use of LSTM, CNN, and GNN thus enables a holistic and robust intrusion detection framework, improving accuracy, generalization, and responsiveness to complex threats in cyber-physical infrastructures.

## 4. METHODOLOGY: FEATURE SELECTION AND MODELS

This study investigates network intrusion detection by evaluating the performance of advanced deep learning models, CNN, LSTM, and GNN, within the RF based feature reduction framework using the NSL-KDD dataset. These models are selected for their capability to capture spatial, temporal, and relational dependencies, which are often present in cyber-physical intrusion scenarios. The experiments were conducted in Python 3.8 using the Scikit-learn library for preprocessing and feature reduction, and PyTorch or TensorFlow-based frameworks for model development. Each model was trained and validated on the RF-selected feature subset, allowing for a consistent comparative evaluation. The integration of CNN, LSTM, and GNN models allows for a multi-perspective approach to intrusion detection, leveraging spatial, temporal, and topological dimensions, to enhance detection robustness and accuracy across diverse attack scenarios.

According to the RF feature importance analysis and feature reduction through feature importance scores of the NSL-KDD are illustrated in Figure 1. the number of bytes sent by the source (src_bytes), the number of bytes sent by the destination (dst_bytes) and the percentage of connections to the same service (same_srv_rate) have highest first three importance among features.

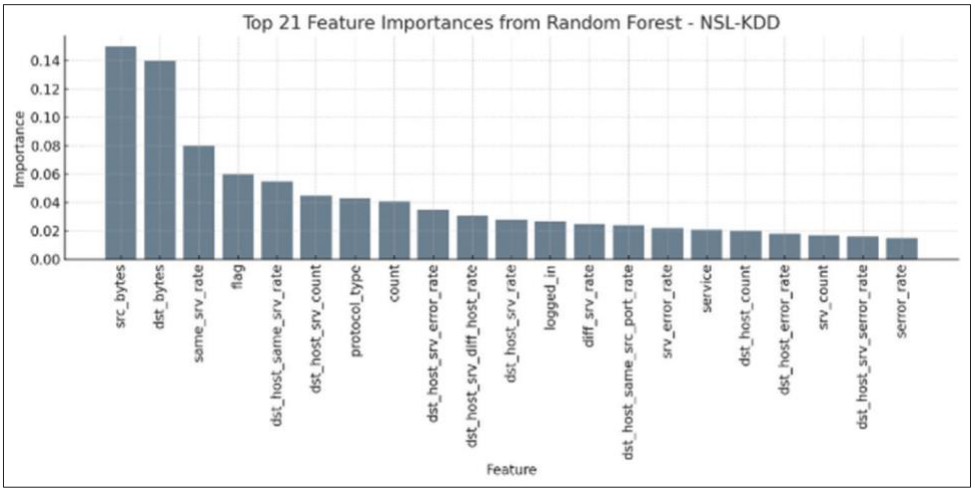
Following the execution of feature reduction and acquiring feature importance scores from RF, the chosen features are presented in Table 4. The proposed methodology resulted in the selection of 21 features out of the initial 41 features.

The application segment of this research introduces an approach for reducing features based on their importance scores to investigate correlations among features and subsequently remove highly correlated ones. Initially, the process involves identifying columns with strong correlations within the dataset. Using the Pandas library, the corr () function conveniently computes correlations between columns in a dataframe. The resulting correlation matrix contains values ranging from 0 to 1, where 0 indicates no correlation and 1 denotes perfect correlation, facilitating the identification of features with high correlations. Following the identification of these highly correlated features, the subsequent step involves their elimination. The variance inflation factor (VIF) serves as a measure for detecting multicollinearity among features

**Table 4: Selected features within RF feature reduction methodology**

| Selected features |
|---|
| F1=src_bytes,<br>F2=dst_bytes,<br>F3=same_srv_rate,<br>F4=flag,<br>F5=dst_host_same_srv_rate,<br>F6=dst_host_srv_count,<br>F7=protocol_type,<br>F8=count,<br>F9=dst_host_srv_serror_rate,<br>F10=dst_host_diff_srv_rate,<br>F11=logged_in,<br>F12=diff_srv_rate,<br>F13=dst_host_same_src_port_rate,<br>F14=dst_host_serror_rate,<br>F15=srv_serror_rate,<br>F16=service,<br>F17=dst_host_srv_diff_host_rate,<br>F18=dst_host_count,<br>F19=srv_count,<br>F20=dst_host_srv_rerror_rate,<br>F21=serror_rate |

**Figure 1:** RF feature importance analysis and feature reduction through feature importance scores of the NSL-KDD



by assessing how much the variance of the estimated regression coefficients increases due to multicollinearity in the model. If a feature's variance exceeds a predefined threshold value, typically set at 5 or 10, it indicates significant correlation with other features within the model. After conducting correlation analysis, the feature selection process resulted in 14 features out of the initial 21. These are depicted in Table 5 as a grey heatmap, where features F1, F2, F3, F5, F8, F9, F10, F11, F12, F14, F15, F16, F20, and F21 exhibit meaningful and highly correlated relationships among themselves.

The process of intrusion detection using deep learning models involves several steps, including feature reduction and the use of evaluation metrics. In summary, it encompasses outlining the procedures for identifying intrusions, minimizing the number of features involved, and assessing the performance of the detection system through various metrics. Table 6 shows the steps implemented approach in detail.

For temporal modeling with LSTM, we organized the selected features into windowed time sequences of network sessions using a sliding window. For GNN, features were mapped onto graph nodes representing host entities, with edges representing communication flows, enabling topological learning over device interactions in SCADA-like architectures. For CNN, the selected features were reshaped into 2D matrices simulating spatial patterns of network traffic, allowing the model to extract localized feature representations and detect spatially correlated anomalies within communication snapshots. In the implementation of CNN, LSTM, and GNN models for SCADA intrusion detection, hyperparameter optimization was conducted to ensure both convergence stability and generalization performance in accordance with established deep learning practices in cybersecurity literature. For all models, the Adam optimizer was employed with an initial learning rate of 0.001 and weight decay set to 0.00001 to prevent overfitting. The CNN architecture consisted of two convolutional layers with 64 and 128 filters, respectively, followed by ReLU activation and max-pooling layers, and a fully connected layer for classification. The LSTM model utilized two stacked LSTM layers with 128 hidden units each, exploiting their capacity to retain long-range temporal dependencies inherent in sequential SCADA data. Dropout regularization (rate = 0.3) was applied between layers to mitigate overfitting. The GNN was implemented using a Graph Convolutional Network (GCN) with two graph convolution layers and 64-dimensional node embeddings, leveraging the adjacency matrix derived from SCADA network topologies to capture spatial and relational dependencies. Each model was trained for 100 epochs with early stopping patience of 10 epochs based on validation loss, using a batch size of 64. These hyperparameter settings are consistent with contemporary studies in intrusion detection systems (IDS), ensuring the models achieved balanced accuracy, sensitivity, and precision, as reflected in the experimental results.

## 5. RESULTS AND DISCUSSION

In the field of SCADA security, choosing the right features is crucial for boosting the effectiveness of classification algorithms, especially when working with imbalanced datasets. The suggested feature reduction method employs a hybrid strategy that merges conventional statistical techniques with cutting-edge deep learning approaches to enhance accuracy and efficiency. By the use of CNN, LSTM, and GNN algorithms in intrusion detection, study shows that even if having a simple structure GNN models has higher accuracy, CNN and LSTM provide competitive results. The experimental study is done on NSL-KDD intrusion data set. The data set's traffic can be classified into five groups: Normal, DOS, U2R, R2L, Probe, or more broadly categorized as Normal versus Anomalous, which encompasses any deviations observed for the binary classification task. An attack map is generated based on the attack class labels and the algorithms utilized. Considered attacks depending on normal and abnormal, behavior precision rates are given in Table 7 and Figure 2 for the models.

**Table 5: Selecting important features based on correlation heat table of RD reducted features**

| Features | F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | F10 | F11 | F12 | F13 | F14 | F15 | F16 | F17 | F18 | F19 | F20 | F21 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| F1 | 1.00 | 0.79 | −0.05 | −0.10 | −0.09 | 0.04 | 0.09 | 0.18 | 0.17 | 0.12 | 0.03 | 0.15 | −0.00 | 0.17 | 0.18 | 0.18 | −0.02 | −0.10 | 0.10 | 0.24 | 0.17 |
| F2 | 0.79 | 1.00 | −0.03 | −0.05 | −0.08 | 0.04 | 0.06 | 0.17 | 0.16 | 0.12 | 0.02 | 0.13 | −0.00 | 0.15 | 0.16 | 0.16 | −0.02 | −0.08 | 0.09 | 0.23 | 0.15 |
| F3 | −0.05 | −0.03 | 1.00 | −0.24 | 0.72 | 0.31 | −0.57 | −0.12 | −0.11 | −0.02 | −0.17 | −0.16 | 0.01 | −0.11 | −0.11 | −0.11 | 0.01 | 0.26 | −0.11 | −0.20 | −0.11 |
| F4 | −0.10 | −0.05 | −0.24 | 1.00 | −0.00 | −0.13 | −0.27 | 0.35 | 0.35 | 0.12 | 0.12 | 0.37 | −0.07 | 0.12 | 0.12 | 0.11 | −0.07 | 0.04 | 0.14 | 0.04 | 0.12 |
| F5 | −0.09 | −0.08 | 0.72 | −0.00 | 1.00 | 0.50 | −0.14 | −0.33 | −0.34 | −0.15 | −0.28 | −0.33 | 0.06 | −0.33 | −0.33 | −0.33 | 0.06 | 0.07 | −0.22 | −0.25 | −0.32 |
| F6 | 0.04 | 0.04 | 0.31 | −0.13 | 0.50 | 1.00 | −0.37 | −0.15 | −0.19 | −0.09 | −0.11 | −0.16 | 0.12 | −0.18 | −0.19 | −0.18 | 0.13 | −0.01 | −0.11 | −0.18 | −0.19 |
| F7 | 0.09 | 0.06 | −0.57 | −0.27 | −0.14 | −0.37 | 1.00 | 0.35 | 0.36 | 0.12 | 0.24 | 0.32 | −0.06 | 0.36 | 0.35 | 0.36 | −0.06 | −0.08 | 0.18 | 0.29 | 0.36 |
| F8 | 0.18 | 0.17 | −0.12 | 0.35 | −0.33 | −0.15 | 0.35 | 1.00 | 0.98 | 0.20 | 0.28 | 0.89 | 0.00 | 0.98 | 0.98 | 0.98 | 0.03 | −0.06 | 0.14 | 0.85 | 0.97 |
| F9 | 0.17 | 0.16 | −0.11 | 0.35 | −0.34 | −0.19 | 0.36 | 0.98 | 1.00 | 0.21 | 0.29 | 0.88 | 0.00 | 0.99 | 0.99 | 0.99 | 0.04 | −0.05 | 0.13 | 0.83 | 0.99 |
| F10 | 0.12 | 0.12 | −0.02 | 0.12 | −0.15 | −0.09 | 0.12 | 0.20 | 0.21 | 1.00 | 0.84 | 0.13 | −0.01 | 0.22 | 0.22 | 0.22 | −0.02 | 0.08 | 0.11 | 0.11 | 0.21 |
| F11 | 0.03 | 0.02 | −0.17 | 0.12 | −0.28 | −0.11 | 0.24 | 0.28 | 0.29 | 0.84 | 1.00 | 0.18 | −0.00 | 0.29 | 0.29 | 0.29 | 0.01 | 0.10 | 0.05 | 0.11 | 0.29 |
| F12 | 0.15 | 0.13 | −0.16 | 0.37 | −0.33 | −0.16 | 0.32 | 0.89 | 0.88 | 0.13 | 0.18 | 1.00 | −0.00 | 0.87 | 0.87 | 0.87 | 0.04 | 0.06 | 0.11 | 0.84 | 0.87 |
| F13 | −0.00 | −0.00 | 0.01 | −0.07 | 0.06 | 0.12 | −0.06 | 0.00 | 0.00 | −0.01 | −0.00 | −0.00 | 1.00 | −0.00 | −0.00 | −0.00 | −0.00 | −0.01 | 0.00 | −0.00 | −0.00 |
| F14 | 0.17 | 0.15 | −0.11 | 0.12 | −0.33 | −0.18 | 0.36 | 0.98 | 0.99 | 0.22 | 0.29 | 0.87 | 0.00 | 1.00 | 1.00 | 1.00 | 0.04 | −0.05 | 0.13 | 0.83 | 1.00 |
| F15 | 0.18 | 0.16 | −0.11 | 0.12 | −0.33 | −0.19 | 0.35 | 0.98 | 0.99 | 0.22 | 0.29 | 0.87 | 0.00 | 1.00 | 1.00 | 1.00 | 0.04 | −0.05 | 0.12 | 0.84 | 1.00 |
| F16 | 0.18 | 0.16 | −0.11 | 0.11 | −0.33 | −0.18 | 0.36 | 0.98 | 0.99 | 0.22 | 0.29 | 0.87 | 0.00 | 1.00 | 1.00 | 1.00 | 0.04 | −0.05 | 0.13 | 0.84 | 1.00 |
| F17 | −0.02 | −0.02 | 0.01 | −0.07 | 0.06 | 0.13 | −0.06 | 0.03 | 0.04 | −0.02 | 0.01 | 0.04 | −0.00 | 0.04 | 0.04 | 0.04 | 1.00 | 0.02 | 0.01 | 0.03 | 0.04 |
| F18 | −0.10 | −0.08 | 0.26 | 0.04 | −0.01 | −0.11 | −0.06 | −0.06 | −0.05 | 0.08 | 0.10 | 0.06 | −0.01 | −0.05 | −0.05 | −0.05 | 0.02 | 1.00 | 0.24 | −0.02 | −0.05 |
| F19 | 0.10 | 0.09 | −0.11 | 0.14 | −0.22 | −0.11 | 0.18 | 0.14 | 0.13 | 0.11 | 0.05 | 0.11 | 0.00 | 0.13 | 0.12 | 0.13 | 0.01 | 0.24 | 1.00 | 0.11 | 0.13 |
| F20 | 0.24 | 0.23 | −0.20 | 0.04 | −0.25 | −0.18 | 0.29 | 0.85 | 0.83 | 0.11 | 0.11 | 0.84 | −0.00 | 0.83 | 0.84 | 0.84 | 0.03 | −0.02 | 0.11 | 1.00 | 0.83 |
| F21 | 0.17 | 0.16 | −0.11 | 0.12 | −0.32 | −0.19 | 0.36 | 0.97 | 0.99 | 0.21 | 0.29 | 0.87 | −0.00 | 1.00 | 1.00 | 1.00 | 0.04 | −0.05 | 0.13 | 0.83 | 1.00 |

Table 7 and Figure 2 illustrates the comparative performance of three deep learning models, CNN, LSTM, and GNN, across two network behavior types: Anomaly and normal. As depicted, LSTM consistently achieves the highest precision in both behavior classes, with a slight decrease from 0.97 (anomaly) to 0.96 (normal), indicating robust generalization across behavioral contexts. GNN follows closely, demonstrating stable performance (0.96-0.95), leveraging topological relationships within SCADA network data. In contrast, CNN exhibits a more pronounced drop in precision from 0.94 to 0.88, suggesting limitations in capturing temporal dependencies or structural variations in normal behavior. These results confirm the effectiveness of LSTM and GNN in maintaining high detection reliability in both anomalous and benign network conditions, supporting their integration within the proposed hybrid intrusion detection framework.

**Figure 2:** Visualization of the normal and abnormal connections behavior precision scores through models

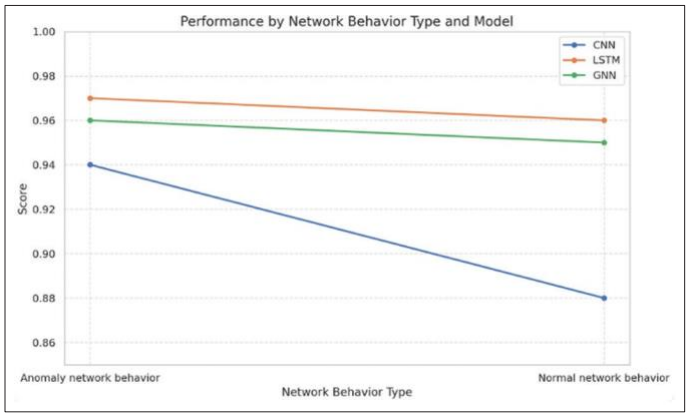



**Table 6: Outlining the steps for intrusion detection using deep learning models, feature reduction, and evaluation metrics**

Step 1: Load NSL-KDD dataset
Step 2: Preprocess the dataset (e.g., encode categorical features, normalize values)
Step 3: Train Random Forest model to determine feature importance
*RandomForest.train (features, labels)*
Step 4: Select top features based on Random Forest feature importance
*selected_features=RandomForest.getImportantFeatures()*
Step 5: Refine selected features using correlation heatmap to remove multicollinearity
Step 6: Split the dataset into training and testing sets
*train_set, test_set=splitDataset (dataset)*
Step 7: Train deep learning models using selected features:
a. Train CNN model
*CNN.train (train_set, selected_features)*
b. Train LSTM model
*LSTM.train (train_set, selected_features)*
c. Train GNN model (ensure graph structure is defined from features or relationships)
*GNN.train (train_set, selected_features)*
Step 8: Test the trained models on the test set:
a. Test CNN model
*cnn_accuracy=CNN.test (test_set)*
*cnn_predictions=CNN.predict (test_set)*
b. Test LSTM model
*lstm_accuracy=LSTM.test (test_set)*
*lstm_predictions=LSTM.predict (test_set)*
c. Test GNN model
*gnn_accuracy=GNN.test (test_set)*
*gnn_predictions=GNN.predict (test_set)*
Step 9: Evaluate model performance and compare results:
a. Calculate precision, recall, and sensitivity for each model
*cnn_precision, cnn_recall, cnn_sensitivity=calculateMetrics (cnn_predictions, test_set.labels)*
*lstm_precision, lstm_recall, lstm_sensitivity=calculateMetrics (lstm_predictions, test_set.labels)*
*gnn_precision, gnn_recall, gnn_sensitivity=calculateMetrics (gnn_predictions, test_set.labels)*
b. Compare accuracy of models
*compareAccuracy (cnn_accuracy, lstm_accuracy, gnn_accuracy)*
c. Compare validation metrics across models
*compareMetrics (cnn_precision, cnn_recall, cnn_sensitivity, lstm_precision, lstm_recall, lstm_sensitivity, gnn_precision, gnn_recall, gnn_sensitivity)*

Anomaly network behavior connection number often exhibits higher scores than normal network behavior in deep learning methodologies because anomalies represent deviations from the expected patterns or norms within the data. In many cases, normal network behavior is well-understood and follows predictable patterns, making it easier for deep learning models to accurately classify. However, anomalies, by their nature, are less frequent and may manifest in various unexpected ways, making them more challenging to detect accurately. As a result, anomalies can have a higher impact on the performance metrics such as sensitivity, precision, or accuracy, especially if the dataset is imbalanced with fewer instances of anomalies compared to normal behavior. Additionally, anomalies often represent potential security threats or system malfunctions, which makes their detection crucial for ensuring the integrity, availability, and security of network systems. Therefore, deep learning methodologies often prioritize the accurate detection of anomaly network behavior to prevent potential security breaches or system failures.

On the other hand, perfomance evaluation of the selected feature according to attack types' accuracy, sensitivity and precision are

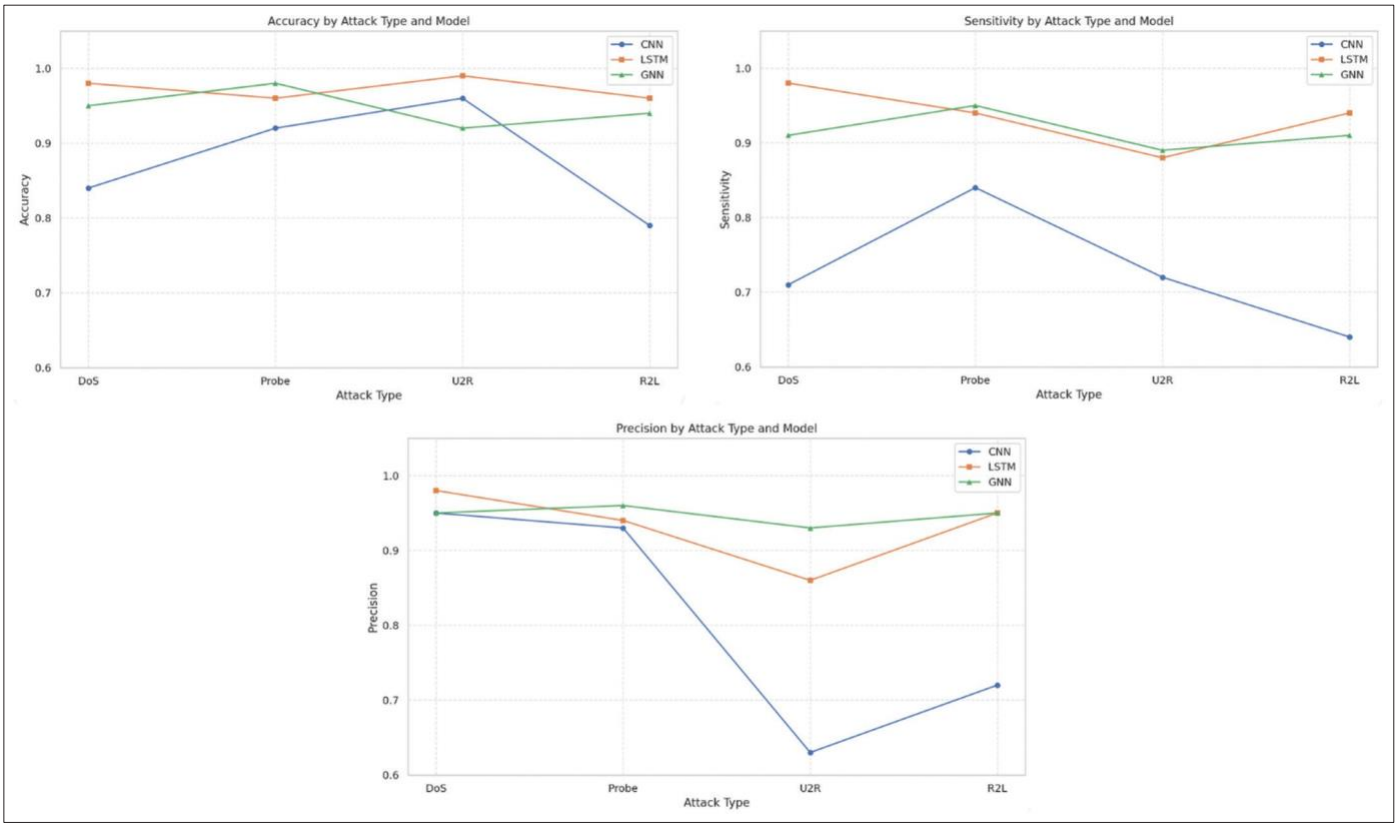
**Table 7: The normal and abnormal connections/network behavior precision scores through models**

| Network behavior/ Precision scores | CNN | LSTM | GNN |
|---|---|---|---|
| Anomaly network behavior | 0.94 | 0.97 | 0.96 |
| Normal network behavior | 0.88 | 0.96 | 0.95 |

**Table 8: A comparative validation score analysis of the models within attack types and accuracy**

| | DoS | Probe | U2R | R2L |
|---|---|---|---|---|
| CNN | | | | |
| Accuracy | 0.84 | 0.92 | 0.96 | 0.79 |
| Sensitivity | 0.71 | 0.84 | 0.72 | 0.64 |
| Precision | 0.95 | 0.93 | 0.63 | 0.72 |
| LSTM | | | | |
| Accuracy | 0.98 | 0.96 | 0.99 | 0.96 |
| Sensitivity | 0.98 | 0.94 | 0.88 | 0.94 |
| Precision | 0.98 | 0.94 | 0.86 | 0.95 |
| GNN | | | | |
| Accuracy | 0.95 | 0.98 | 0.92 | 0.94 |
| Sensitivity | 0.91 | 0.95 | 0.89 | 0.91 |
| Precision | 0.95 | 0.96 | 0.93 | 0.95 |

**Figure 3:** Visualization of the validation score analysis of the models within attack types




presented in the Table 8, Figure 3. The line chart visualizations in Figure 3 illustrate the comparative performance of CNN, LSTM, and GNN models across four attack categories, DoS, Probe, U2R, and R2L, based on accuracy, sensitivity, and precision metrics. The LSTM consistently exhibits the highest accuracy across all attack types, peaking notably at U2R with near-perfect accuracy (0.99), demonstrating its superior ability to capture temporal dependencies in complex sequences. GNN follows closely, particularly excelling in the Probe and R2L categories due to its strength in modeling structural relationships among SCADA components. CNN, while effective in detecting DoS and Probe attacks, shows a noticeable decline in performance for U2R and R2L attacks, especially in precision (approximately 0.63 for U2R), likely due to its limited capacity to handle long-range dependencies or rare event patterns. Sensitivity results reinforce these observations, with LSTM and GNN maintaining robustness, whereas CNN exhibits significant drops for U2R and R2L, indicating weaker detection of true positives in sophisticated or infrequent attack types. These results validate the hybrid use of LSTM and GNN in intrusion detection systems for SCADA networks, offering complementary benefits in sequential pattern recognition and relational inference.

These results support prior research advocating for advanced and hybrid deep learning strategies, such as integrating LSTM, CNN, and GNN, coupled with feature reduction and data balancing techniques. The superior and more stable performance of LSTM and GNN models across attack types, particularly in detecting underrepresented classes like U2R and R2L, demonstrates the effectiveness of temporal, spatial, and relational learning mechanisms in addressing class imbalance. These findings emphasize the necessity of leveraging model complementarity and deep architectural diversity to enhance the robustness and precision of intrusion detection systems in highly imbalanced cybersecurity datasets.

## 6. CONCLUSION AND POLICY RECOMMENDATIONS

Evaluation of future behavior with environmental indicators is a way of real-time decision making and cautions for energy risks. Digitalized energy system continuity needs to follow DL models for robust cybersecurity. The paper presents recommendations in the context of preventing risks, detecting attacks, predictive maintenace, demand and capacity forecasting.

This study demonstrates the application of diverse deep learning architectures for constructing an effective IDS using the NSL-KDD dataset, which is widely recognized for benchmarking IDS performance. Unlike traditional classifiers the proposed hybrid deep learning approach addresses the complex temporal, spatial, and structural characteristics of SCADA related network traffic. Experimental findings reveal that LSTM consistently achieves the highest performance across multiple attack categories, particularly for rare classes like U2R and R2L, due to its superior temporal modeling capabilities. CNN effectively capture localized patterns, while GNN leverage topological dependencies within the data. Compared to earlier studies where deterministic classifiers like kNN yielded strong performance, this work highlights that deep learning models, especially LSTM and GNN, offer greater robustness and accuracy, particularly in the context of imbalanced

and noisy SCADA datasets. Therefore, integrating these advanced models not only enhances precision and sensitivity but also ensures improved generalization and adaptability to real world industrial cyber physical systems such as smart grids.

In conclusion; the study indicates key concepts of energy management systems as a series of stages that aim to result in matured digital transformation and gained sustainability through artificial intelligence integrated cybersecurity standards, acts and directives. Developing an intrusion detection deep learning methodology in energy sector, policymakers should draw upon key frameworks such as NIST AI, the EU AI Act, the EU Cybersecurity Act, the EU DEFENDER initiative, and the OECD Cyber Act for guidance. These frameworks emphasize the importance of adopting standards and best practices, ensuring regulatory compliance, conducting robust risk assessments, and implementing effective risk management strategies. Policies should prioritize data privacy and protection, promote collaboration and information sharing, and invest in capacity building and training initiatives. Continuous monitoring and incident response capabilities are crucial, along with the adoption of emerging technologies like deep learning to enhance intrusion detection systems, Resilience and recovery planning are also essential to minimize the impact of cyber incidents on critical energy infrastructure. Overall, a culture of continuous improvement and adaptation is necessary to address evolving cyber threats and support the ongoing digital transformation of the energy sector.

The proposed feature reduction methodology introduces a hybrid approach that combines traditional statistical techniques with advanced deep learning methods to improve classification accuracy and efficiency. While many existing methodologies report high accuracy, they often neglect computational efficiency. This hybrid approach not only aims for superior accuracy but also emphasizes minimizing runtime, making it suitable for real time SCADA applications

In addition and summary to the results as regulatory measures; for a SCADA intrusion detection deep learning methodology in the energy sector, several policy advices can be derived from frameworks like NIST, the EU AI Act, the EU Cybersecurity Act, the EU DEFENDER initiative, and the OECD Cyber Act. To enhance the cybersecurity of SCADA systems, organizations should implement several key policy recommendations. First, adopting standards and best practices is crucial; aligning with Information Delivery Specifications (IDS) ensures structured data exchange, while frameworks like ISO/IEC 27001 and PCI DSS help establish robust information security management systems to protect sensitive data. As demonstrated through the proposed hybrid AI based SCADA intrusion detection framework, high risk AI systems must adhere to key principles of transparency, reliability, and resilience, as mandated by the EU AI Act and the NIST Cybersecurity Framework. By integrating explainable AI components (e.g., SHAP values), robust deep learning models and risk aware validation techniques, the systems can operate these regulatory expectations within the technical design. Moreover, the alignment with ISO/IEC 27001 for information security and ISO/IEC 42001 for AI management systems further reinforces the framework's compliance with cross cutting standards, ensuring that the deployed AI solutions are not only technically sound but also ethically and legally responsible. Regulatory compliance must also be prioritized through regular audits to adhere to frameworks such as the EU Cybersecurity Act, which mandates the safeguarding of data confidentiality and integrity within the energy sector.

Comprehensive risk management strategies should be developed to identify vulnerabilities in SCADA systems, incorporating regular threat assessments and utilizing deep learning for enhanced intrusion detection capabilities. Data protection measures are essential; implementing stringent controls to safeguard sensitive information and regularly updating cybersecurity policies will address emerging risks. Stakeholder cooperation is vital for sharing insights on threats and best practices, with initiatives like the EU DEFENDER promoting collective cybersecurity resilience. Education and training programs should be established to keep personnel informed about emerging threats and incident response procedures, fostering a culture of cybersecurity awareness. Additionally, robust incident response plans must be developed, including clear procedures for identifying and mitigating security breaches, complemented by regular drills to ensure preparedness. Finally, redundancy and contingency planning should be implemented to maintain operational continuity after a cyber attack, ensuring that backup systems are regularly tested. By adopting these comprehensive recommendations, organizations can significantly bolster their SCADA systems' defenses against cyber threats while ensuring compliance with relevant regulations.

## REFERENCES

Ahakonye, L.A.C., Nwakanma, C.I., Lee, J.M., Kim, D.S. (2023), SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection. Internet of Things, 21, 100676.

Akheel, M.A. (2023), Vulnerability assessment and analysis of SCADA and Foundation Fieldbus on industrial control system (ICS) networks: A literature review. IUP Journal of Computer Sciences, 17(2), 34-68.

Aljawarneh, S., Yassein, M.B., Aljundi, M. (2019), An enhanced J48 classification algorithm for the anomaly intrusion detection systems. Cluster Computing, 22, 10549-10565.

Almaleh, A. (2023), Measuring resilience in smart infrastructures: A comprehensive review of metrics and methods. Applied Sciences, 13(11), 6452.

Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R.P., Braun, R. (2024), GNN-based network traffic analysis for the detection of sequential attacks in IoT. Electronics, 13(12), 2274.

Asgharzadeh, H., Ghaffari, A., Masdari, M., Gharehchopogh, F. S. (2023), Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced Capuchin Search Algorithm. Journal of Parallel and Distributed Computing, 175, 1-21.

Balla, A., Habaebi, M.H., Elsheikh, E.A., Islam, M.R., Suliman, F.M. (2023), The effect of dataset imbalance on the performance of SCADA intrusion detection systems. Sensors, 23(2), 758.

Barrett, M. (2018), Technical Report. Gaithersburg, MD, USA: National Institute of Standards and Technology.

Carrapico, H., Barrinha, A. (2018), European Union cybersecurity as an emerging research and policy field. European Politics and Society, 19(3), 299-303.

Cui, Y., Bangalore, P., Tjernberg, L.B. (2018), An anomaly detection approach based on machine learning and SCADA data for condition monitoring of wind turbines. In: 2018 Probabilistic Methods Applied to Power Systems (PMAPS). IEEE. p1-6.

El Mrabet, Z., Kaabouch, N., El Ghazi, H., El Ghazi, H. (2018), Cyber-security in smart grid: Survey and challenges. Computers and Electrical Engineering, 67, 469-482.

European Commission (EC). (2010), A Digital Agenda for Europe, Communication. Brussels, Belgium: European Commission.

European Commission. (2013), Regulation No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA). Available from: https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a32013r0526

European Commission. (2020), On Artificial İntelligence-A European Approach to Excellence and Trust (White Paper). Brussels, Belgium: European Commission.

European Commission. (2022), Agency for Network and Information Security (ENISA): Risk Management Standards-analysis of Standardization Requirements in Support of Cybersecurity Policy. Greece: ENISA.

European Commission. (2022), National Energy and Climate Plans (NECPs). Available from: https://ec.europa.eu/energy/topics/energy-strategy/national-energy-climate-plans_engordon

European Commission. (2024), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 12 July 2024 laying down harmonized rules on artificial intelligence (AI Act). Brussels: European Commission.

European Parliament, Committee on Industry, Research and Energy. (2022), Committee Report on a European Approach to Artificial İntelligence. Available from: https://artificialintelligenceact.eu/wp-content/uploads/2022/09/aıa-ıtre-rule-57-opinion-adopted-14-June.pdf

Gordon, L. A., Loeb, M. P., Zhou, L. (2020), Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb model. Journal of Cybersecurity, 6(1), tyaa005.

Gstrein, O. J., Haleem, N., Zwitter, A. (2024), General-purpose AI regulation and the European Union AI Act. Internet Policy Review, 13(3), 1-26.

Gugliandolo, E., Giunta, G., Caleta, D., Zahariadis, T., Voliotis, S., Trakadas, P., Skias, D. (2018), Critical infrastructure protection: Prevention, detection, response, and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe. In: Defending the European Energy Infrastructures, Defender. Brussels: European Commission.

Gulzar, M.M., Iqbal, M., Shahzad, S., Muqeet, H.A., Shahzad, M., Hussain, M.M. (2022), Load frequency control (LFC) strategies in renewable energy-based hybrid power systems: A review. Energies, 15(10), 3488.

Hakansson, C. (2022), Where does the compass point? The European Commission's role in the development of EU security and defence policy. European View, 21(1), 5-12.

Ingre, B., Yadav, A., Soni, A.K. (2020), Decision tree-based intrusion detection system for NSL-KDD dataset. In: Proceedings of the International Conference on Information and Communication Technology for Intelligent Systems. Springer. p207-218.

Javed, S.H., Ahmad, M.B., Asif, M., Akram, W., Mahmood, K., Das, A.K., Shetty, S. (2023), APT adversarial defence mechanism for industrial IoT enabled cyber-physical system. IEEE Access, 11, 74000-74020.

Kamboj, P., Trivedi, M.C., Yadav, V.K., Singh, V.K. (2018), Detection techniques of DDoS attacks: A survey. In: 2018 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON). IEEE. p675-679.

Khan, F., Rehman, A.U., Arif, M., Aftab, M., Jadoon, B.K. (2016), A survey of communication technologies for smart grid connectivity. In: Proceedings of the International Conference on Electronics, Electrical Engineering and Computing (ICE Cube). IEEE. p256-261.

Linkov, I., Trump, B.D., Poinsatte-Jones, K., Love, P., Hynes, W., Ramos, G. (2018), Resilience at OECD: Current state and future directions. IEEE Engineering Management Review, 46(4), 128-135.

Marković-Petrović, J.D. (2020), Methodology for cyber security risk mitigation in next generation SCADA systems. In: Cyber Security of İndustrial Control Systems in the Future İnternet Environment. United States: IGI Global.p27-46.

Nadiammai, G., Hemalatha, M. (2014), Effective approach toward intrusion detection system using data mining techniques. Egyptian Informatics Journal, 15(1), 37-50.

National Institute of Standards and Technology (NIST), (2023a), Artificial Intelligence Risk Management Framework (AI RMF 1.0). Available: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

National Institute of Standards and Technology (NIST). (2023b), U.S. Artificial Intelligence Safety Institute. Available from: https://www.nist.gov/artificial-intelligence/artificialintelligence-safety-institute

National Institute of Standards and Technology Cyber Security Framework, (NIST CSF) (2024), Updating the NIST Cybersecurity Framework - Journey to CSF 2.0. Available from: https://www.nist.gov/cyberframework/updating-nistcybersecurity-framework-journey-csf-20

NSL-KDD Data set for Network-Based İntrusion Detection Systems. (2023), Available: https://205.174.165.80/cıcdataset/nsl-kdd [Last accessed 2023 Mar].

Organization of Economic Cooperation and Development (OECD), (2022), OECD Policy Framework on Digital Security: Cybersecurity for Prosperity. Paris: OECD.

Oswal, S., Shinde, S.K., Vijayalakshmi, M. (2023), Deep learning-based anomaly detection in cyber-physical system. In: Big Data Analytics in Intelligent IoT and Cyber-Physical Systems. Singapore: Springer Nature Singapore. p59-71.

Pascoe, C.E. (2023), Public Draft: The NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology. Available from: https://www.nist.gov/cyberframework

Peng, S., Liu, M., Chai, L., Deng, R. (2024), Dst-gnn: A dynamic spatiotemporal graph neural network for cyberattack detection in grid-tied photovoltaic systems. IEEE Transactions on Smart Grid, 16(1), 330-43.

Presekal, A., Ştefanov, A., Rajkumar, V.S., Palensky, P. (2023), Attack graph model for cyber-physical power systems using hybrid deep learning. IEEE Transactions on Smart Grid, 14(5), 4007-4020.

Prisecaru, P. (2016), Challenges of the fourth industrial revolution. Knowledge Horizons - Economics, 8(1), 57-62.

Ravipati, R.D., Abualkibash, M. (2019), Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets-a review paper. International Journal of Computer Science and Information Technology, 11(1), 1-11.

Samunnisa, K., Kumar, G.S.V., Madhavi, K. (2023), Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods. Measurement: Sensors, 25, 100612.

Senthilnayaki, B., Venkatalakshmi, K., Kannan, A. (2013), An intelligent intrusion detection system using genetic based feature selection and Modified J48 decision tree classifier. In 2013 Fifth İnternational Conference on Advanced Computing (ICoAC). p1-7.

Serinelli, B.M., Collen, A., Nijdam, N.A. (2020), Training guidance with KDD Cup 1999 and NSL-KDD data sets of ANIDINR: Anomaly-based network intrusion detection system. Procedia Computer Science, 175, 560-565.

Shahab, M., Wang, S., Muqeet, H.A.U. (2021), Advanced Optimal Design of the IoT-based university Campus Microgrid Considering

Environmental Concerns and Demand Response. In: Proceedings of the International Conference on Smart Grid Technologies.

Sovrano, F., Masetti, G. (2022), Foreseeing the impact of the proposed AI Act on the sustainability and safety of critical infrastructures. In: Proceedings of the International Conference on Theory and Practice of Electronic Governance. p492-498.

Sowmya, T., Anita, E.M. (2023), A comprehensive review of AI based intrusion detection system. Measurement: Sensors, 28, 100827.

Teixeira, M.A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., Samaka, M. (2018), SCADA system testbed for cybersecurity research using machine learning approach. Future Internet, 10(8), 76.

Tomazzoli, C., Scannapieco, S., Cristani, M. (2020), Internet of things and artificial intelligence enable energy efficiency. Journal of Ambient Intelligence and Humanized Computing, 11, 1-22.

Tvaronavičienė, M., Plėta, T., Della Casa, S., Latvys, J. (2020), Cybersecurity management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia, and Lithuania. Insights into Regional Development, 2(4), 802-813.

Upadhyay, D., Manero, J., Zaman, M., Sampalli, S. (2021), Intrusion detection in SCADA-based power grids: Recursive feature elimination model with majority vote ensemble algorithm. IEEE Transactions on Network Science and Engineering, 8(3), 2559-2574.

Volkova, A., Hatamian, M., Anapyanova, A., De Meer, H. (2024), Being accountable is smart: Navigating the technical and regulatory landscape of AI-based services for power grid. In: Proceedings of the International Conference on Information Technology for Social Good. p118-126.

Wu, Y., Wang, Z., Huangfu, Y., Ravey, A., Chrenko, D., Gao, F. (2022), Hierarchical operation of electric vehicle charging station in smart grid integration applications. An overview. International Journal of Electrical Power and Energy Systems, 139, 108005.

Yatagha, R., Nebebe, B., Waedt, K., Ruland, C. (2024), Towards a Zero-day Anomaly Detector in Cyber Physical Systems Using a Hybrid VAE-LSTM-OCSVM model. In: Proceedings of the 33rd ACM International Conference on Information and Knowledge Management. p5038-5045.

Yenioğlu, Z.A., Ateş, V. (2022), Secure Smart Grid Management Maturity within Big Data. In: Technological Development and İmpact on Economic and Environmental Sustainability. United States: IGI Global. p221-244.

Yin, C., Zhu, Y., Fei, J., He, X. (2017), A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954-21961.

Zhang, X., Jiang, G., Li, W., Bai, D., He, Q., Xie, P. (2024), Cross-turbine fault diagnosis for wind turbines with SCADA data: A spatio-temporal graph network with multi-task learning. In: 2024 39th Youth Academic Annual Conference of Chinese Association of Automation (YAC). IEEE. p1684-1689.

Zheng, W., Sun, K., Zhang, X., Zhang, Q., Israr, A., Yang, Q. (2020), Cellular Communication for Ubiquitous Internet of Things in Smart Grids: Present and Outlook. In Proceedings of the Chinese Control and Decision Conference (CCDC). IEEE. p5592-5596.