Chapter 8
An AI-Driven Framework for Intelligent Intrusion Detection and Network Traffic Analysis

Alvaro Guarnido
http://orcid.org/0009-0005-8595-9505
Illinois Institute of Technology, USA & Universidad Politecnica de Madrid, Spain

Paul Nyamohanga
http://orcid.org/0009-0007-0055-2250
Illinois Institute of Technology, USA

ABSTRACT

This research project presents an AI-based intrusion detection framework for smart renewable energy grids. It enhances the traditional binary detection to a multi-class model capable of identifying different types of cyberattacks, including DoS, malware, phishing, MITM, SQL injection and zero-day. The proposed system utilizes the Smart Grid Intrusion Detection Dataset. It combines the Random Forest with the Autoencoder machine learning models to reach an accuracy of 97.8%, with the objective of minimizing false positives. Temporal analysis is included in order to discover attack patterns across hours, days of the week and operational phases of the energy grids. In addition, this project trains an XGBoost predictive model to determine attack likelihood or type based on recent temporal sequences. The study contributes to a predictive cybersecurity approach, anticipating attacks and strengthening resilience in intelligent energy infrastructures.

DOI: 10.4018/979-8-3373-8252-4.ch008

I. INTRODUCTION

The rapid evolution of smart renewable energy grids has changed the way energy is produced, distributed and managed. By integrating advanced communication technologies, IoT devices and decentralized energy sources, these grids have enabled disruptive technologies such as real-time monitoring, communication or the optimization of energy flow. However, expanding interconnectivity also exposes critical infrastructures to diverse cyber threats capable of disrupting stability and compromising operational safety. Intrusion detection systems (IDS) hence play a vital role in guaranteeing the reliability and resilience of smart energy networks (Ahmadi et al., 2026).

Traditional Intrusion Detection Systems (IDS) approaches focus on static binary detection, classifying network activity as normal or malicious (1 or 0). This method is very simple and unable to provide information about temporal dynamics or specific types of cyberattacks. This simplification limits the capability to anticipate evolving threats in highly dynamic environments, such as energy grids. Furthermore, most existing datasets and models ignore the temporal context of intrusions, overlooking patterns that may emerge based on the time of day, day of the week, or operational phase of the grid. Understanding these time-dependent behaviors is imperative for developing and implementing predictive and proactive cybersecurity defenses (Kabir et al., 2025) (Kalech, 2019).

According to the challenges in the current era, this study presents an AI-enhanced intrusion detection framework that integrates temporal behavior analysis and multi-class attack classification using the Smart Grid Intrusion Detection Dataset. The proposed system goes beyond binary detection by identifying specific types of attacks, including denial of service (DoS), malware, phishing, man-in-the-middle (MITM), SQL injection and zero-day. At the same time, the system analyzes their temporal distribution patterns. The methodology follows an implementation process of these four steps (Eze et al., 2025):

- Data preparation and feature engineering: raw data is cleaned and enhanced with temporal features (time, day of the week, day, time segment, and weekend indicators) (Kalech, 2019).
- Temporal pattern analysis: different types of attacks are visualized, and data and statistics such as heatmaps and histograms are extracted based on frequency per time period (hour, weekday). Statistical tests such as Chisquare and ANOVA are applied to confirm the time dependency of attacks (Kabir et al., 2025).