

Reliable Detection of Cyber Threats in Smart Grids Using a Hybrid XGBoost and LSTM Framework

Arul Princy A.¹, Veera Ramana M.², Nithish R.³,
Vishnu Sankar R.⁴

¹Assistant Professor, ^{2,3,4} Student, Department of Computer Science and Engineering,
NPR College of Engineering and Technology, Natham, Dindigul, India.

E-mail: ¹arulprincy@nprcolleges.org, ²veeraramana11@gmail.com, ³rnithish291@gmail.com,

⁴vishnusankar1025@gmail.com

Abstract

The smart grid utilizes communication, measurement, and automation techniques that help to monitor the power system but increase vulnerability to cyber attacks. FDIA and DoS are two types of cyber attack that either tamper with measurements or limit access to information and therefore need a detection technique capable of capturing the dynamics of measurements. In this study, a hybrid classification model that combines XGBoost and LSTM is introduced to classify smart-grid observations as normal state, FDIA state, and DoS state. The XGBoost algorithm will be utilized for performing static feature analysis, and the LSTM will model the temporal dependencies based on the consecutive measurement windows. The output of the two algorithms is then merged using the weighted decision fusion method. The proposed scheme is evaluated based on data created based on IEEE 39-Bus New England power system test case, after applying preprocessing techniques such as missing values interpolation, min-max normalization, ten-sample windows, and 80% training and 20% testing ratio. Experimental results report an overall accuracy of 82.12%, with class-wise F1-scores between 0.81 and 0.82 and a false-positive rate of 5.1%. The proposed system is further combined with a real-time monitoring interface using Flask, email alerts through SMTP, and logging events. This monitoring system has achieved an average latency of 0.23 seconds per sample, 1.5 seconds average alert time, ability to handle up to 50 simultaneous sessions, and 99.7% average uptime during the experiment.

Keywords: Smart Grid Cybersecurity, Cyber Threat Detection, XGBoost, Long Short-Term Memory (LSTM), Hybrid Deep Learning, False Data Injection Attack, Real-time Monitoring.

1. Introduction

The transformation of traditional power generation systems to smart grids through integration of advanced communication systems, sensor devices, automation systems, and monitoring techniques is a step towards greater efficiency, but at the same time, it increases the cybersecurity threat faced by vital power infrastructure. Thus, the detection of malicious activities in the environment of smart grids has become a subject of study [1].

False data injection attacks (FDIA) and denial-of-service (DoS) attacks are some of the major threats to the functioning of a smart grid. In FDIA attacks, the measurements can be distorted, whereas in denial-of-service attacks, the availability of information needed for monitoring and controlling can be compromised. The problem with detecting these attacks is that the observations related to these attacks can be similar to those of normal behavior of the system.

Deep-learning techniques have demonstrated potential for identifying cyberattack patterns in smart-grid data [2]–[5]. However, smart-grid measurements contain both structured feature relationships and temporal dependencies. Therefore, a detection framework that considers these complementary characteristics can provide a more comprehensive representation of system behavior.

The proposed study develops a hybrid system consisting of XGBoost and LSTM networks for the detection of cyber threats in a smart grid environment. XGBoost is used for structural feature extraction, whereas the LSTM network is used for analyzing sequential data with temporal relationships. Decision fusion is done based on the outputs to categorize them as normal operations, FDIA, and DoS. Additionally, the system is developed with a real-time monitoring interface and automatic email alerts.

2. Related Works

The application of deep learning for smart-grid cybersecurity has been widely researched due to the capability of deep learning to detect complex patterns from data. Ruan et al. [1] analyzed the use of deep learning in smart-grid cybersecurity and highlighted the opportunities

presented by data-driven methods to detect cyber attacks. Nasir et al. [2] studied the performance of different deep learning algorithms for the FDIA attack detection problem.

Several studies that focused on the temporal attributes of FDIA. For example, He et al. [3] presented a deep learning-based approach for the real-time detection of FDIA, while Niu et al. [4] studied the dynamic detection of FDIA through deep learning. Yang et al. [5] proposed a method for the detection of AC-FDIA using LSTM-autoencoders, emphasizing on the significance of temporal correlation in smart grid data.

Ensemble and machine-learning approaches have also been explored. Gupta et al. [7] suggested a data-driven ensemble approach to detecting FDIA attacks, whereas Alenazi and Mishra [8] assessed XGBoost and Gaussian Naïve Bayes for detecting cyberattacks in IoT settings. This literature offers justification for using the complementary learning strengths of these methods, as well as tree-based approaches on structured cybersecurity datasets.

Further research in the field of security of smart grids has included the development of integrated and distributed security schemes. An AI-blockchain security scheme was introduced by Ghadi et al. [9], whereas secure federated deep learning for FDIA detection was investigated by Li et al. [10]. Singh [11] studied the application of data-driven deep learning models for the detection of cyber and physical attacks on the power systems. IEEE 39-bus system, available from the repository at Texas AM University Electric Grid Test Case Repository, is one such benchmark environment [12]. Privacy-preserving intrusion detection using federated learning techniques was also investigated [13], whereas Mohammed et al. [14] was proposed an optimized deep-learning model for FDIA detection.

Although the research provides significant progress in the respective area, the available methods usually focus on specific elements like temporal modeling, ensemble classifiers, distributed training, or advanced deep learning structures. The development of a more holistic method that incorporates the use of structured features, temporal dependency modeling, and real-time threat monitoring is essential for further research. This paper aims to address this challenge by incorporating XGBoost and LSTM into a real-time threat monitoring system.

3. Problem Statement and Objectives

3.1 Problem Statement

Connectivity of smart grid systems opens up opportunities to cyber-attacks, which will cause manipulation or disruption of operational information through FDIA and Denial-of-Service attacks, respectively. These cyber-attacks present a difficult challenge for detection in the sense that malicious activities could have complex relationship features as well as time-dependent features. Detection techniques have shown to perform quite effectively but using a single learning method to model these two aspects has been found to be inadequate. Moreover, existing research-based detection schemes are mainly concerned about the effectiveness of classification with little consideration to monitoring and notification of threats.

This study therefore focuses on the development of a hybrid framework to detect cyber-threats that incorporates static features modeling and time-dependent features modeling together with threat classification and notification for smart-grid environments.

3.2 Objectives

The objectives of the research are:

- To develop a hybrid XGBoost–LSTM model for cyber-attack detection in smart grids by combining the advantages of structural features and time dependency models.
- To classify smart grid observations into three classes: normal behavior, FDIA attack, and DoS attack by utilizing static and temporal data simultaneously.
- To evaluate the classification performance of the designed hybrid framework in terms of accuracy, precision, recall, F1 score, and false-positive rate, as well as to determine how well the model performs consistently in three classes.
- To compare the performance of the designed hybrid model with XGBoost model and LSTM model independently, in terms of classification accuracy and false-positive rate.
- To implement a smart-grid cyber-threat monitoring and alerting system for real-time cyber-attack detection.

4. Proposed Methodology

4.1 System Architecture

The research aims to design a hybrid approach to cyber threat detection which combines XGBoost and LSTM techniques to capture the static and temporal properties of cyber threats in smart grids. The architecture of the approach comprises five main stages, namely, data collection and preprocessing, feature extraction, static feature analysis using XGBoost, temporal sequence analysis using LSTM, and decision fusion and alerting. The overall architecture of the proposed approach is devised based on the objectives of this research, which focuses on enhancing the reliability of cyber threat detection through the joint use of measurement structures and temporal cyber attack properties. The overall architecture of the cyber threat detection system is presented in Figure. 1.

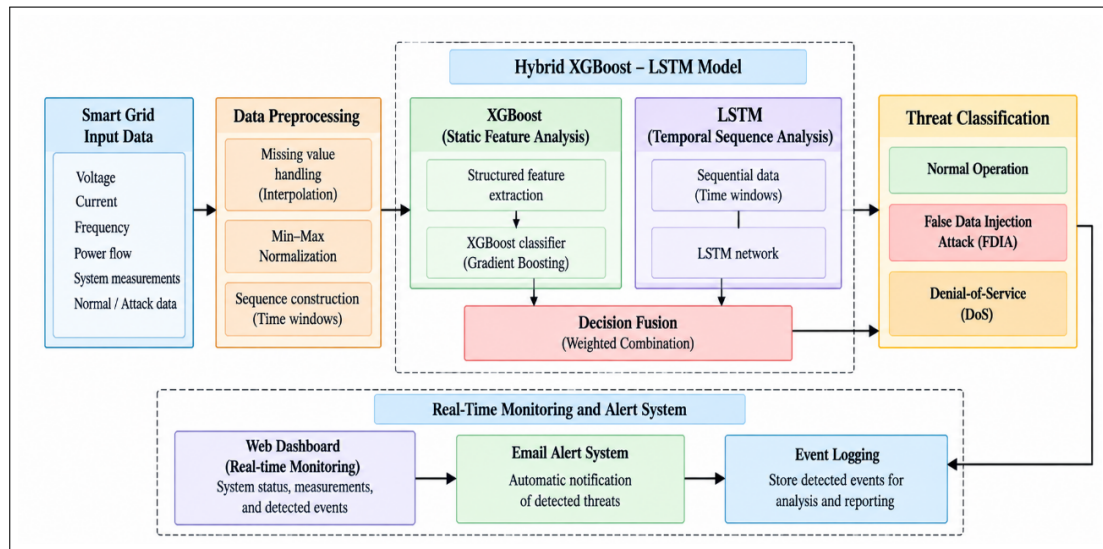


Figure 1. Proposed hybrid XGBoost-LSTM architecture for cyber threat detection.

The data acquisition stage receives smart grid measurement data representing both normal operating conditions and cyber attack scenarios. The gathered data are later processed to be consistent and ready for machine learning model analysis. Missing values are replaced using interpolation, and min-max normalization is performed to convert the input features to be in a uniform range of 0-1. In the case of time-series analysis, the preprocessed data are placed in consecutive windows to allow the LSTM model to learn the temporal behavior of the system. The data processing process provides a unified representation of the inputs for the static and time components of the proposed solution.

Post-preprocessing of the extracted features, these features undergo processing through two different learning models. XGBoost model is used to identify the static attributes of smart grid measurement, while the LSTM model is used for analyzing the sequence dependency between the consecutive data points. The decisions made by these two models are then combined using the decision fusion method. The decision fusion output becomes the final decision whether the observation is normal operations, false data injection attacks (FDIA), or denial-of-service (DoS) attacks.

4.2 XGBoost for Static Feature Analysis

XGBoost is used for the static feature analysis module in the proposed framework. It is a gradient boosting algorithm that builds a powerful classifier by incrementally building a collection of decision trees in such a way that subsequent learners mitigate the errors made by previous learners. In the proposed framework, XGBoost analyzes the structured smart grid measurement data such as voltage, current, frequency, and power flow data. These measurements provide important information regarding deviations from normal operating conditions and potential attack-related abnormalities.

The usage of XGBoost can be explained with its capability to predict the nonlinear association between the heterogeneous structured features while managing the model complexity with the help of regularization. As a result, the model offers a good tool for capturing static feature patterns of normal and malicious operation regimes. The output of the XGBoost block gives a preliminary classification that is further mixed with the time series prediction made by the LSTM. The approach helps in keeping the benefits of the structured features modeling while overcoming the limitation of static classification not being able to capture attacks in a sequence.

4.3 LSTM for Temporal Dependency Modeling

The LSTM network serves as the temporal analysis module for the proposed architecture. While the traditional static classifier is meant to be a static model, LSTM is specifically designed to maintain its stateful memory and thus model dependencies in sequential data. The LSTM module consists of three types of gates: input, forget, and output gates which control the information stored and forwarded to subsequent layers by the LSTM unit. In case of cyber threat detection in the smart grid, the LSTM network can model the temporal dynamics in the

measurements.

Preprocessed readings are split into time windows that consist of ten consecutive readings. They are fed as a sequence to the LSTM network. The designed neural network has two layers with 64 and 32 LSTM cells. In addition, the dropout technique with the rate of 0.2 is used to decrease the risk of overfitting. Softmax activation is used for the dense output layer that provides the final three-class classification. The training process uses the Adam optimizer with the learning rate of 0.001 and the categorical cross-entropy as the loss function.

4.4 Hybrid Fusion Strategy

The results from both the XGBoost model and LSTM model are combined using a weighted voting scheme to arrive at the final classification result. The value of the weight parameter will be estimated during the validation phase in such a way that the relative significance of the static classifier and temporal classifier can be adequately considered. The rationale behind the fusion approach lies in the complementary nature of the two models.

The aim of the proposed hybrid decision-making process is to minimize the drawbacks that may come from depending on a single machine learning technique. The static analysis may detect anomalies in the features of an individual sample, whereas the temporal analysis may detect attack patterns that evolve over time through a series of samples. Combining both these outputs will result in a more complete model of the behavior of the cyber attacks.

4.5 Real-time Monitoring and Alert System

For practical implementation, the proposed classification approach is implemented with the help of a real-time monitoring system. The monitoring system makes use of Flask in conjunction with HTML and CSS for creating the web-based interface, through which the system can monitor events and the current status of the system. In case there is a cyber threat that is identified, then the event gets classified into the relevant attack category and the severity level is determined.

An email notification system based on SMTP is implemented to generate instant alerts to the administrator. The emails generated include information related to the attack as well as the time when the attack was detected. Moreover, the detection records are logged for future analysis and reporting purposes. The real-time component therefore directly addresses the research

objective of developing a system capable of detection, classification, and automated notification rather than limiting the study to model-based classification alone.

4.6 Dataset Description

The dataset employed was developed based on the IEEE 39-bus benchmark model of the power system of New England, which is available publicly from the Texas AM University Electric Grid Test Case Repository [9]. The IEEE 39-bus system is an artificial benchmark system that consists of 39 buses, 10 generators, and 46 transmission lines and is frequently used for power system studies.

The proposed system was employed as the power system environment in the current cybersecurity study, and cyber attack scenarios were included to reflect the scenarios of false data injection (FDI) and denial-of-service (DoS). The employment of FDIs and DoSs in benchmark power systems from IEEE is also justified by the cyber-physical power systems' research [10]. The findings have been categorized into three categories for the current classification problem: normal operation scenario, false data injection attack (FDIA), and DoS attack.

The resulting dataset was prepared for both static and temporal analysis using the proposed hybrid XGBoost-LSTM framework. The feature set comprises the electrical measurements that have been made in the power system, including the voltage, current, frequency, and other measurements related to the power. Missing values were taken care of by interpolation, while the min-max normalization process was used to normalize the features to fall in the range of [0,1]. Afterward, the observations were arranged in windows of ten samples each to facilitate temporal analysis using the LSTM algorithm. Finally, the prepared dataset was divided into training 80% and testing 20% subsets.

5. Results And Findings

5.1 Experimental Configuration

The proposed framework was implemented and evaluated in a Python-based development environment with the following (Table 1) hardware and software specifications:

Table 1. Hardware and software configuration

Component	Specification
Processor	Intel Core i5/i7
RAM	8 GB
Storage	200 GB HDD/SSD
Operating System	Windows 11
Programming Language	Python 3.8+
Framework	Flask
Frontend	HTML, CSS
Development Environment	Visual Studio Code

XGBoost model utilized 100 estimators, a max depth of 6, a learning rate of 0.1, and subsample proportion of 0.8. The LSTM model comprised of two hidden layers of 64 and 32 units each with a dropout ratio of 0.2. The model was trained using the Adam optimization algorithm with a learning rate of 0.001 and categorical cross-entropy loss for up to 50 epochs. The above parameters were utilized for evaluation of the performance of the suggested hybrid approach in experimental settings of the research.

5.2 Classification Performance

The classification performance of the proposed approach is tested for three categories: normal operations data, false data injection attack (FDIA), and denial of service (DoS). The results obtained, as shown in Table 2 below, are relatively consistent for the three classes.

Table 2. Classification Performance by Class

Class	Precision	Recall	F1-Score	Support
Normal (Class 0)	0.82	0.83	0.82	1245
FDIA (Class 1)	0.81	0.82	0.81	1180
DoS (Class 2)	0.83	0.81	0.82	1205

The overall classification accuracy reported for the evaluated model was 82.12%. The relatively narrow variation among the precision, recall, and F1-score values suggests that the model maintained a comparatively consistent classification capability across the three classes. The results therefore indicate that the evaluation was not dominated by performance on a single class.

5.3 Confusion Matrix Analysis

The confusion matrix (Figure 2) depicts the class-wise distribution of correct and incorrect classification of samples. Out of the 1,245 normal cases, 1,033 were accurately classified as normal, 112 were classified as FDIA and 100 were classified as DoS. Out of the 1,180 FDIA cases, 968 were accurately classified as FDIA, 98 were classified as normal and 114 were classified as DoS. Out of the 1,205 DoS cases, 1,003 were accurately classified as DoS, 95 were classified as normal and 107 were classified as FDIA.

The distribution of the misclassified samples suggests that error was made between each of the three classes. Specifically, the result suggests some degree of overlap between FDIA and DoS cases, while few attack cases were classified as normal.



Figure 2. Confusion matrix

5.4 Comparative Performance

The performance of the proposed approach was compared with standalone XGBoost, and standalone LSTM.

Table 3. Comparison with existing approaches

Method	Accuracy (%)	FPR (%)	Type
Standalone XGBoost	78.5	8.2	Static
Standalone LSTM	80.1	6.8	Temporal
Proposed Hybrid	82.12	5.1	Hybrid

According to the results from the Table 3, the new method achieved higher accuracy and less false-positive rate compared to the other methods tested in this study. The performance variation is attributed to the nature of the designed approach, which seeks to incorporate both static and dynamic data analysis. It should however be noted that these results are specific to the data used in this study.

5.5 Real-time Performance

The monitoring tool developed was assessed on the basis of its performance and monitoring capabilities. Figure 3 below depicts the real-time desktop-based monitoring dashboard used for displaying system statuses, measuring trends, cyber-threat classification, and detecting events. The dashboard allows viewing the monitoring process in general and visualizing the detected cyber-threats.

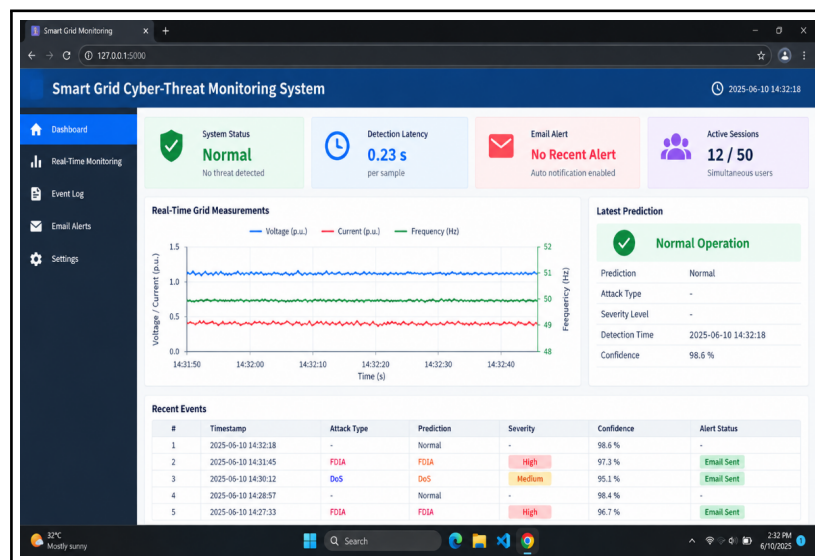


Figure 3. Real-time smart-grid cyber-threat monitoring dashboard

5.6 Summary of Findings

Overall, the performance achieved through experimental evaluation was 82.12%, where the F1-score varied between 0.81 and 0.82 for all the three classes examined. From the confusion matrix, it can be seen that the model is able to classify 1,033 normal data, 968 FDIA data, and 1,003 DoS data. False positive percentage for the proposed approach was 5.1%, as compared to 8.2%, 6.8%, and 5.9% for the other approaches.

In addition to that, the real-time analysis also showed a detection latency of 0.23 seconds per sample, an average delay in alerts delivery of 1.5 seconds, up to 50 simultaneous sessions at the same time, and 99.7% uptime of the system.

6. Conclusion and Future Work

From the experimental results, the combination of static and temporal analysis can be considered an ideal solution to classify the cyber threats to the smart-grid. The proposed model was able to provide an equally high class-wise performance with F1-scores of 0.82 for Normal class, 0.81 for FDIA and 0.82 for DoS class, but with an overall accuracy of 82.12% claimed for the entire system. In addition, a 5.1% false positive rate proves the effectiveness of the hybrid decision mechanism in terms of reduced threat misclassification compared to the standalone models used in this experiment. The implementation also illustrates the practicality of threat detection, continuous monitoring, alerting and logging. From the experimental results, the detection delay and the alert notification delivery time were 0.23 seconds and 1.5 seconds respectively. Experiment was conducted using a data set developed from a benchmark, and not all the cyber attack scenarios against smart-grids were considered.

References

- [1] Ruan, Jiaqi, Gaoqi Liang, Junhua Zhao, Huan Zhao, Jing Qiu, Fushuan Wen, and Zhao Yang Dong. "Deep learning for cybersecurity in smart grids: Review and perspectives." *Energy Conversion and Economics* 2023, vol. 4, no. 4: 233-251.

- [2] Nasir, Qassim, Manar Abu Talib, Muhammad Arbab Arshad, Tracy Ishak, Romaissa Berrim, Basma Alsaïd, Youssef Badway, and Omnia Abu Waraga. "Comparison of Deep Learning Algorithms for Site Detection of False Data Injection Attacks in Smart Grids." *Energy Informatics* 2024, vol. 7, no. 1: 71.
- [3] He, Youbiao, Gihan J. Mendis, and Jin Wei. "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism." *IEEE Transactions on Smart Grid* 2017, vol. 8, no. 5: 2505-2516.
- [4] Niu, Xiangyu, Jiangnan Li, Jinyuan Sun, and Kevin Tomsovic. "Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning." *IEEE power energy society innovative smart grid technologies conference (ISGT)*, 2019, 1-6.
- [5] Yang, Liqun, You Zhai, and Zhoujun Li. "Deep Learning for Online AC False Data Injection Attack Detection in Smart Grids: An Approach using LSTM-Autoencoder." *Journal of Network and Computer Applications* 2021, vol. 193: 103178.
- [6] Singh, Rashi, Nasib Singh Gill, and Preeti Gulia. "Attentional LSTM-Ensemble Architecture for Intrusion Detection in Smart Grids." *Scientific Reports* 2025, vol. 15, no. 1: 41977.
- [7] Gupta, Tania, Richa Bhatia, Sachin Sharma, Ch Rami Reddy, Kareem M. AboRas, and Wael Mobarak. "A Data-Driven Ensemble Technique for the Detection of False Data Injection Attacks in the Smart Grid Framework." *Frontiers in Energy Research* 2024, vol. 12: 1366465.
- [8] Alenazi, Mordi, and Shailendra Mishra. "Cyberattack Detection and Classification in IOT Systems Using XGBoost And Gaussian Naïve Bayes: A Comparative Study." *Engineering, Technology Applied Science Research* 2024, vol. 14, no. 4: 15074-15082.
- [9] Ghadi, Yazeed Yasin, Tehseen Mazhar, Tariq Shahzad, Ines Hilali Jaghdam, Sanwar Khan, Muhammad Amir Khan, and Habib Hamam. "A Hybrid AI-Blockchain Security Framework for Smart Grids." *Scientific reports* 2025, vol. 15, no. 1: 20882.
- [10] Li, Yang, Xinhao Wei, Yuanzheng Li, Zhaoyang Dong, and Mohammad Shahidehpour. "Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach." *IEEE Transactions on Smart Grid* 2022, vol. 13, no. 6: 4862-4872.

- [11] Singh, Kamal. "Detection Of Cyber and Physical Disturbances in Power Systems Using Data-Driven Deep Learning Methods." *International Journal of Critical Infrastructure Protection* 2026: 100844.
- [12] Texas AM University Electric Grid Test Case Repository, "IEEE 39-Bus System," Department of Electrical and Computer Engineering, Texas AM University. Available <https://electricgrids.engr.tamu.edu/electric-grid-test-cases/ieee-39-bus-system/>
- [13] Raza, Mubashar, Muhammad Jasim Saeed, Muhammad Bilal Riaz, and Muhammad Awais Sattar. "Federated Learning for Privacy-Preserving Intrusion Detection in Software-Defined Networks." *IEEE Access* 2024, vol. 12: 69551-69567.
- [14] Mohammed, Saad Hammood, Mandeep S. Jit Singh, Abdulmajeed Al-Jumaily Investigation, Mohammad Tariqul Islam, Md Shabiul Islam, Abdulmajeed M. Alenezi, Mohamad A. Alawad, and Muaadh A. Alsoufi. "IG-APSO-DNN: Deep Learning Intrusion Detection Model to Detect False Data Injection Attacks in Smart Grids." *Ad Hoc Networks* 2025: 104053.