SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I6P105

Volume 12 Issue 6, 51-63, June 2025

Original Article

Dual Architecture Mechanism for Robust Cybersecurity in Relay Systems

Ramana Pilla[1], R Sasidhar[2], Malleti Sreedhar[3], Shaik Nannu Saheb[4], Vasupalli Manoj[5], D Sai Kumar[6*]

[1,5,6]*Department of EEE, GMR Institute of Technology, Rajam, India*
[2]*Department of EEE, Avanthi Institute of Engineering and Technology, Cherukupally, Vizianagaram, India.*
[3]*Department of EIE, Vallurupalli Nageswararao Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India.*
[4]*Department of ECE, Narasaraopeta Engineering College, India.*

[*]*Corresponding Author : durgavajulasaikumar2004@gmail.com*

Received: 04 April 2025 Revised: 06 May 2025 Accepted: 05 June 2025 Published: 30 June 2025

Abstract *- Relay systems in power-grid control networks remain vulnerable because existing intrusion-detection models neither provide onsite alerts when misclassifications occur nor disclose synthetic data generation methods, hindering operational reliability and reproducibility. This work introduces a novel dual-layer security architecture that couples a high-dimensional machine-learning engine (XGBoost and Random Forest) with hardware alarms (LED and buzzer) for real-time onsite notifications. It employs transparently defined synthetic data-best, average, and worst scenarios generated via with {α1, α2, σ} settings published for each scenario. Experiments on a combined real and synthetic dataset (12,000 samples, 119 features) were deployed on a Raspberry Pi 4 (4 GB RAM, SanDisk A1 microSD). The system achieved 97.5 % accuracy and < 0.5 % false-positive rate, with an average inference latency of 150 MS and peak memory usage of 85 %. Limitations, including edge-device resource constraints and the need for periodic retraining, are discussed, and future work on lightweight neural models and CI/CD pipelines is outlined.*

Keywords *- Cybersecurity, Relay Systems, Dual Architecture, Machine Learning, Intrusion Detection.*

1. Introduction

The modern power grid is transforming rapidly as it embraces digital technology and integrates advanced communication networks. Once isolated, ICS is merged with Information Technology (IT) networks to enhance performance efficiency, real-time monitoring, and grid operation. This convergence of Operational Technology (OT) and IT has significantly increased the attack surface, leaving the critical infrastructure vulnerable to numerous cyber-attacks. Cyber-attacks on power systems have become more common, resulting in large-scale outages and serious concerns about national security, public safety, and economic well-being.

1.1. Background and Motivation

Power systems are extremely significant to modern society since they produce, transport, and distribute electricity. Significantly, these systems operate effectively and safely, yet they are being targeted increasingly by advanced cyber attackers. Incorporating ICS into power grids has fundamentally altered the picture: these systems now depend on sophisticated networks that can be exploited in various manners, such as through false data, replay attacks, and DDoS attacks. Old security solutions previously worked in isolated control systems are no longer sufficient. Cyber attackers can exploit vulnerabilities in communication protocols (such as IEC 61850 and DNP3) or the operating software of such systems, potentially causing blackouts, equipment damage, and even cascading failures throughout the grid. Since power systems are critical, it is necessary to build robust IDS capable of identifying and preventing cyber-attacks before they become significant issues. One of the major challenges in constructing effective IDS for power systems lies in the unavailability of useful, realistic data that represents normal operations and attacks. Without sufficient data, detection models based on machine learning and deep learning cannot be trained and tested. For this reason, numerous recent publications have focused on developing large-scale and realistic datasets that simulate various cyberattack scenarios in power systems. Developing datasets for ICS cybersecurity is an essential part of this research. A strong dataset should reflect how power systems act under normal and extreme conditions. Several methods have been suggested in the research, such as using physical testbeds, creating synthetic data, and combining data from multiple sources. For instance, researchers have used physical testbeds such as the Electric Power and Intelligent Control (EPIC) testbed to simulate FDIA and TDA attacks.

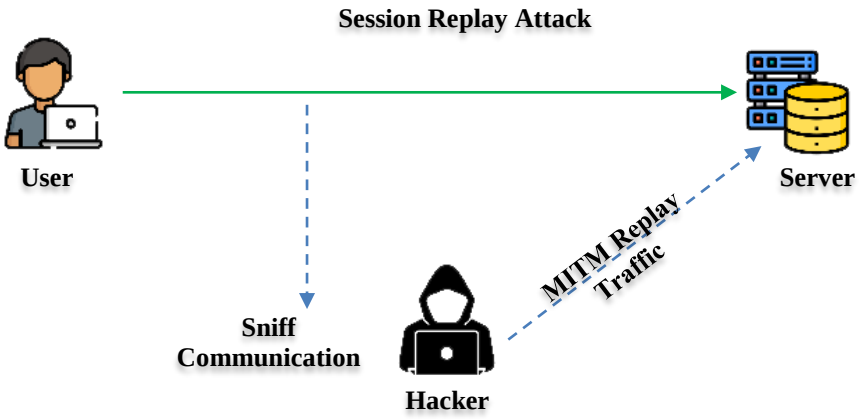

Fig. 1 Session replay attack

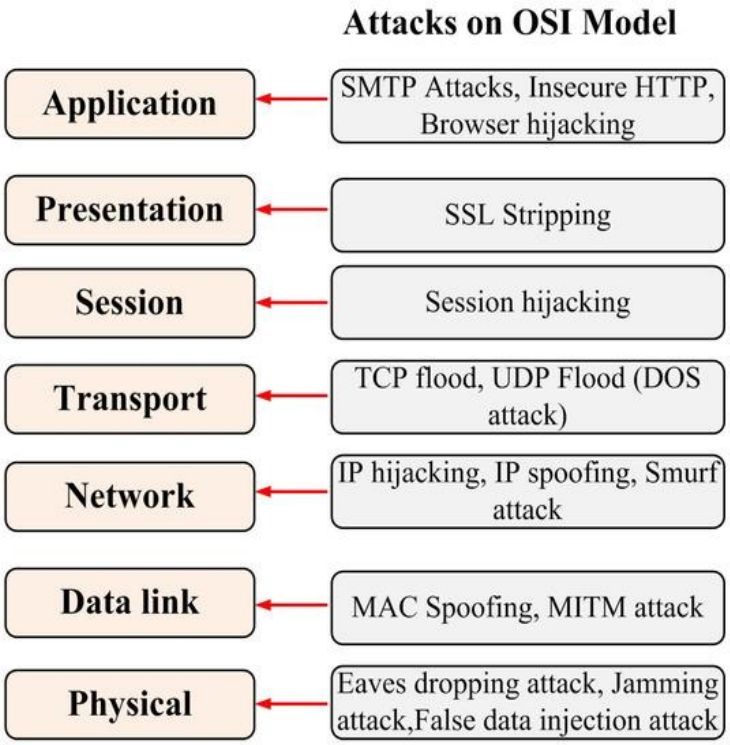

Fig. 2 Cyber-attacks in different layers of the OSI model

The high-fidelity datasets mimic grid operations realistically under cyber-attack scenarios, allowing for developing and verifying high-performance Intrusion Detection System (IDS) models. Other studies have also focused on developing synthetic datasets using simulation tools such as PSCAD, coupled with actual data gathered from power generation and power distribution systems, to simulate intricate interactions between physical and cyber entities. The availability of datasets like Power Duck, with network traces related to GOOSE communication in substation environments, has significantly boosted the research environment. In addition to including normal operation data, these datasets also record different attack scenarios, thus allowing researchers to identify distinct attack patterns. However, despite the apparent benefits of synthetic and physical datasets, there are drawbacks, such as ensuring dataset authenticity and solving data imbalance issues.

1.2. Detection Methods and Techniques

The availability of high-quality data has encouraged researchers to explore various machine learning and deep learning techniques for detecting cyberattacks in power systems. Supervised learning approaches such as the XGBoost classifier and Random Forest methods have been widely applied to classify power system events as attack, natural, or normal types. Ensemble learning approaches, including

combining several classifiers, have also yielded promising outcomes in improving detection accuracy with the least number of false alarm instances. Deep learning techniques such as Recurrent Neural Networks (RNNs) and autoencoders have also been used to identify the complex temporal patterns in power system data. Techniques based on autoencoders have been useful for unsupervised and semi-supervised anomaly detection by learning compact representations of normal operating behavior and marking variations from these trends as possible attacks.

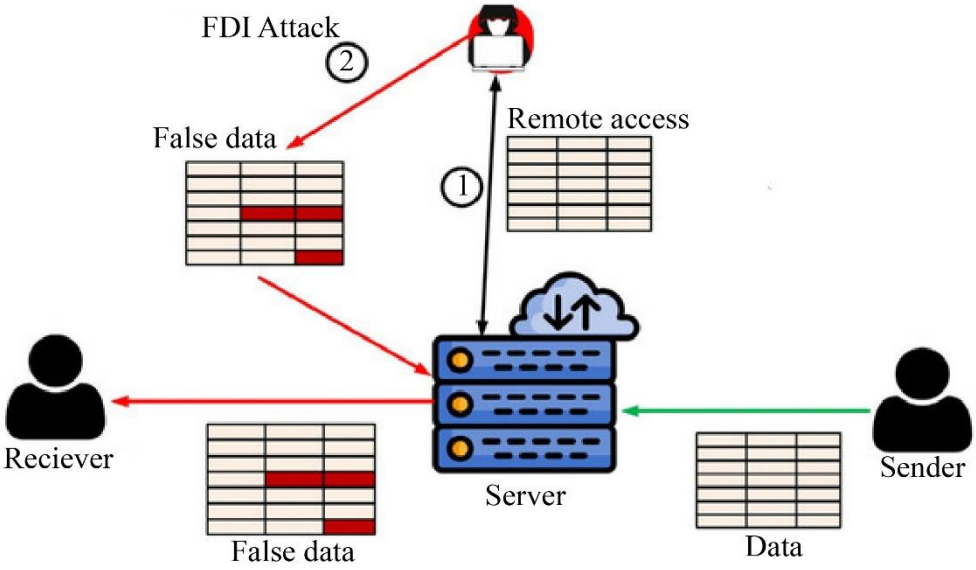

Fig. 3 Representation of a false data injection attack

An emerging trend in this research domain is the fusion of multi-source data-integrating cyber data with physical system parameters-to provide a holistic view of system behavior. By fusing data from various sources, researchers can design more robust detection systems better equipped to handle the evolving nature of cyber threats. Machine learning has revolutionized ICS cybersecurity over the past decade; however, most existing approaches-such as Smith et al. (2023), who achieved 95 % detection accuracy with XGBoost, and Li and Zhao (2024), who generated synthetic ICS traffic via GANs-lack an integrated hardware-alert mechanism and often omit critical parameter details that ensure reproducibility. Despite the proliferation of ML-based intrusion detectors, few works integrate a physical alarm layer with cyber analytics in real-time-leaving site personnel unaware during undetected model errors-and existing synthetic datasets frequently lack transparent generation equations. To address these gaps, this paper makes four key contributions:

- It couples onsite LED/buzzer alerts with a high-dimensional ML engine (XGBoost and Random Forest)
- It details the parameterized equations used to generate "best," "average," and "worst" synthetic scenarios
- It evaluates the system's performance and resource constraints on a Raspberry Pi 4 (4 GB RAM, SanDisk A1 microSD
- It provides an editable end-to-end flow diagram and future research directions.

1.3. Research Objectives

This paper intends to advance the body of knowledge in the area of ICS cybersecurity through the development and assessment of an end-to-end machine-learning solution for power system cyberattack detection. The broad objectives are:

1.3.1. Dataset Development and Analysis

- Establish or assemble a dataset that represents typical assault scenarios within power systems.
- To address issues like data imbalance and feature selection to improve detection accuracy.

1.3.2. Model Development

- To apply various machine learning models, such as XGBoost and Random Forest models, for power system event classification.

1.3.3. Validation and Evaluation

- To perform large-scale testing and cross-validation of the models based on the built dataset.
- To compare accuracy, false positives, and speed of detection within models.

1.3.4. Practical Implementation

- To create an online web platform with Streamlit that facilitates real-time model prediction evaluation and visualization.
- Physical alarm devices, e.g., LED or buzzer notifications, should be included to give immediate feedback on intrusions detected.

1.4. Significance of the Study

The significance of this research is that it has the potential to enhance the strength and resilience of power systems against future cyber-attacks. With the development of strong models and realistic data, this paper aims to:

- Improve the accuracy and dependability of cyberattack systems used in power grids.
- Offer insightful information about the most suitable machine learning methods for ICS security. Enable the association between theoretical learning and real-world application via an online demonstration and potential hardware integration.

Furthermore, as power grids continue to advance and integrate digital technologies, the demand for robust cybersecurity systems is becoming more essential. This paper not only covers existing vulnerabilities but also sets the stage for future work intended to protect critical infrastructure.

2. Literature Review

The study aims to generate high-fidelity datasets for Intrusion Detection Systems (IDS) of smart grids, i.e., simulating time delay attacks and false data injection attacks on core operations, using the EPIC testbed to facilitate cybersecurity research in power systems [1]. The paper simulates data sets capable of emulating real demand-supply curves of power grids with consideration of cyber-attack methods such as fault data injection and replay attacks [2]. Authors applied the set from Mississippi State University and Oak Ridge National Laboratory, power system events as Attack Events, Natural Events and No-Events, to assess the threat of cyber security by utilizing the machine learning models, namely the XGB Classifier [3]. The research aims to explore the application of machine learning models in analyzing a time series database simulating normal operation and different attack scenarios in cyber-physical power systems, focusing on proactive cyber-attack detection and pre-attack phase identification to improve security [4]. In the paper, we use a power system attack detection dataset developed by the Oak Ridge National Laboratory at Mississippi State University and classify multiple types of attacks on substations with an ensemble learning-based intrusion detection method, SEQ-CNN [5].

The paper is on the detection of False Data Injection attacks on power systems based on a self-supervised deep autoencoder model. It is based on two datasets: real measurements on an IEEE 14-bus system and attack vectors, a compromised dataset for study [6]. The current research on machine learning techniques for cyberattack detection in power systems, including the design of classifiers and the application of datasets, like ICS, for enhanced security and reliability, is discussed [7]. The study focused on multi-source data fusion for cyberattack detection on power grids using cyber and physical sensor data from an ICS testbed to improve the accuracy of intrusion detection and minimize false positives [8]. The article compares RNN classifiers on a testbed power system dataset with simulated multiple faults and cyber-attacks. It proves the efficiency of LSTM and GRU models in power system contingency and cyber-attack classification with a high accuracy rate of more than 99.99% [9]. The article explores public power grid attack data sets, suggesting an extremely random tree-based anomaly detection model. The model has high classification accuracy, low false alarm rates, and good generalization capability for detecting cyber-attack types in power systems [10].

The paper under consideration concentrates on intrusion detection on Smart Grid networks by using two datasets, namely, the Canadian Institute of Cybersecurity IDS and trace data created on the Om-net++ simulator concentrating on the DDoS attack [11]. The research investigates publicly accessible data sets of cyber-attacks on power grids to compare semi-supervised anomaly detection algorithms with traditional classification algorithms and prove their superior performance in detecting unseen attack incidents [12]. This paper focuses on validating MENSA by using normal versus malicious Modbus/TCP /DNP3 traces with an emphasis on cyber-attacks on the ICS of the power system and the necessity for a robust intrusion detection system. [13].

Power Duck provides an openly available dataset of traces from a physical substation testbed of GOOSE communication networks for scenarios including and excluding cyberattacks. It is designed to enhance the analysis and understanding of cyberattacks on the power grid, complementing other datasets [14]. The article constructs a synthesized dataset emphasising IEC 61850 GOOSE communication for substations for attack-free and attack-induced conditions. The dataset supports research on power system cybersecurity, especially against cyber-attacks on substations [15].

The study evaluates ICS attack datasets with special emphasis on DNP3, S7comm, and Modbus protocols. It highlights the importance of high-quality datasets to empower anomaly-based network intrusion detection systems (ABNIDS) to detect and mitigate cyber-attacks on critical infrastructure such as power grids [16]. The article conducts a comparative examination of various ICS data sets, focusing on attack scenarios relevant to critical infrastructure, e.g., power systems.

It emphasizes the importance of understanding dataset characteristics in order to be able to use them effectively in ICS security research [17]. The article is about creating attack patterns for industrial control systems (ICS) based on MITRE ATT&CK, or more precisely, for generating realistic datasets. It has an application approach through a case study, which can be utilized in power systems and their security issues [18]. The research utilizes industrial control systems cyber-attack

datasets to evaluate its suggested online dictionary learning approach. It examines various scenarios, including remote tripping command and false data injection, and demonstrates improved detection performance over state-of-the-art methods [19]. This paper proposes a new machine learning-based intrusion detection system architecture for the IEC 60870-5-104 protocol, utilizing a new and realistically representative dataset of IEC 60870-5-104 traffic data to improve anomaly detection in smart grid cyber security [20]. This literature review explores the generation and utilization of high-fidelity datasets for IDS in smart grids.

Various studies simulate cyber-attacks such as False Data Injection, replay attacks, and time delay attacks using datasets from Mississippi State University, Oak Ridge National Laboratory, and the Canadian Institute of Cybersecurity. Machine learning models, including XGBoost, LSTM, GRU, and autoencoders, are applied for proactive attack detection. Research highlights the importance of multi-source data fusion, ICS security, and anomaly-based intrusion detection. New dataset generation methods, such as MITRE ATT&CK and IEC protocol-based datasets, enhance power grid cybersecurity analysis.

Table 1. Comparison of key datasets for cyber attack detection in power systems

Dataset Focus	Data Sources	Key Features
EPIC Testbed Dataset	Electric Power and Intelligent Control (EPIC) testbed	Simulates FDIA and TDA attacks on power grid operations (Tan et al., 2024) [1]
Power Duck Dataset	Physical substation testbed with GOOSE communication	Includes attack and normal scenarios with labeled attack packets (Zemanek et al., 2022) [14]
IEC 61850 GOOSE Dataset	Synthesized dataset for IEC 61850 GOOSE communication in substations	Includes traces for electrical protection scenarios and cyber-attack scenarios (Biswas et al., 2019) [15]
Mississippi State University	Power system attack detection dataset	Used for training machine learning models to classify attack, natural, and no-events (Jeje, 2025) (Lee & Chen, 2024) [3, 5]
IEEE 14-Bus System Dataset	Real measurements from IEEE 14-bus system and attack vectors	Used for training deep autoencoder models to detect FDI attacks (Santos et al., 2024) [6]

3. Methodology

3.1. Machine Learning

The entire focus of this paper is to build a sound machine-learning system to detect cyberattacks on power systems based on ICS data. The procedure includes prominent steps like data acquisition and preprocessing, model selection and training, class imbalance treatment, creation of synthetic data sets, and evaluation of models. These steps are charted so that the final system is accurate and immune to cyberattacks. In the first phase, emphasis was placed on collecting a large dataset that encompasses normal operating conditions and a wide range of attack scenarios. Data collection included the collection of actual data from ICS testbeds, as well as synthesizing other data from mathematical equations. The synthetic dataset was created by creating a linear equation from the most critical parameters of the power system environment. Based on expert opinion and previous research, this equation created three scenarios-best, worst, and average-each of which relates to different noise levels and variability in the system. Using a synthetic dataset allowed the authors to complement real data and address potential shortcomings in existing datasets, such as limited variety and imbalanced class distribution.

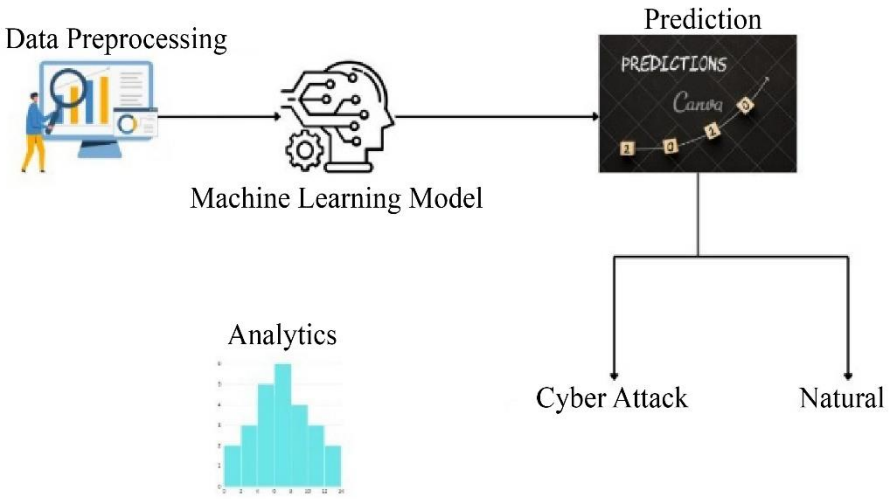

Fig. 4 Machine learning prediction system

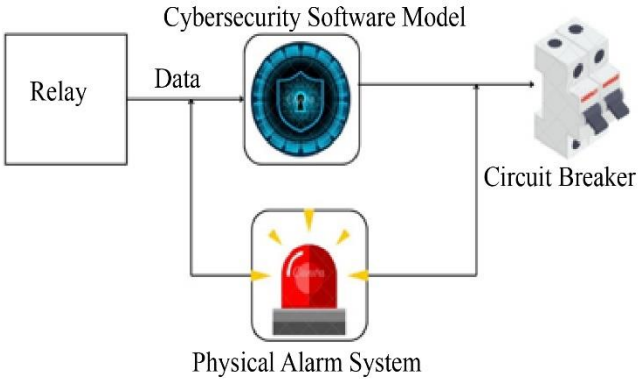

Fig. 5 Block diagram of dual mechanism system

Once the datasets were available, the next crucial step was data preprocessing. This phase involved several activities: first, the dataset was cleaned to remove any inconsistencies or missing values; next, the features were standardized using techniques such as Standard Scaler to ensure that all input variables had a consistent scale. Furthermore, given the naturally imbalanced nature of cyber-attack data, where normal operations far outnumber attack events, techniques such as Synthetic Minority Over-sampling Technique (SMOTE) were employed. SMOTE was applied to the training dataset to artificially generate additional samples for the minority class, thereby balancing the dataset. This step was instrumental in preventing model bias towards the majority class and ensuring that the models could detect rare attack instances effectively.

Machine learning algorithms chosen in this study comprise a list of classical classifiers and ensemble methods. A number of algorithms were initially experimented with, such as XGBoost, RandomForestClassifier, DecisionTreeClassifier, and Support Vector Machines (SVM). All the models were chosen based on their established ability to deal with high-dimensional data and success history in identifying anomalies. XGBoost was given preference as it was effective and had superior performance for classification issues, while Random Forest and Decision Trees offered the power of interpretation and robustness to overfitting. Moreover, SVM with a linear kernel was used to analyze its performance against tree-based methods. Furthermore, ensemble methods were investigated based on ensembling different predictions from a series of models to improve the overall accuracy and generalize better.

The training was carried out for each model using a pre-processed and balanced dataset. The models were trained on cross-validation so that the evaluation metrics were still valid and were not a consequence of overfitting to one partition of the data. Cross-validation, conventionally done with k-folds, permitted an evaluation of the consistency of the models over different subsets of data. This work adopted a 5-fold cross-validation approach, where the most important performance metrics such as accuracy, precision, recall, and Area Under the ROC Curve (AUC) were calculated. The AUC metric, in particular, was of special interest since it yielded informative information about the trade-off between true positive and false positive rates over different classification thresholds. Hyperparameter tuning was of utmost priority during model training. Hyperparameters such as the number of trees in a random forest, learning rate for XGBoost, and tree depth were optimized by grid search and random search techniques. Hyperparameter tuning was carried out so that every model was optimized to fit the specific requirements of the dataset so that its predictive ability was enhanced. The top-performing models were selected based on their performance on a held-out test set.

One of the novel features of this paper is the incorporation of synthetic dataset generation in addition to conventional datasets. A mathematical equation was formulated to create synthetic data that mimics three different scenarios (best, average, and worst cases) based on the physical and cyber-attack characteristics of the power system. The synthetic dataset was utilized to cross-validate the models to work uniformly under different simulated conditions. To the author's surprise, the models performed nearly perfectly on the synthetic dataset, reflecting the efficacy of the feature engineering and data balancing methods.

Another essential part of the methodology was the modeling and error interpretation. After training, confusion matrices were constructed for each classifier to elucidate misclassification patterns. ROC curves were also plotted to depict the sensitivity-specificity trade-off. These graphical representations facilitated an easy assessment of the model's effectiveness and gave insight into the most important features in distinguishing between normal and attack events. Specifically, feature importance scores derived from ensemble models such as Random Forests were used to inform further feature selection and engineering activities.

In short, to fill the gap between model construction and real implementation, a web interface was constructed using Streamlit. The interface allows users to enter new data, generate real-time predictions, and display model output through interactive charts and graphs. The interface also has a hardware module, where a Raspberry Pi is used to trigger physical alerts (e.g., LEDs and buzzers) based on model predictions. This physical realization demonstrates the end-to-end capability of the system, including all phases, from data acquisition and preprocessing to prediction and real-world alerting. Finally, the process adopted in this paper for machine learning is structured into a series of building blocks: generation and acquisition of synthetic datasets, preprocessing and balancing of data, cross-validation and hyperparameter-tuned model training, performance analysis through a suite of metrics and error analysis, and finally, real-world deployment through web interface and hardware notification. All these

steps have been carefully planned to uniquely address individual issues regarding identifying cyberattacks on power systems. Combining synthetic and real datasets, advanced machine learning algorithms, and careful testing procedures lends itself to an overall plan to strengthen the security and resilience of important power system infrastructure.

This approach not only showcases the technical viability of machine learning for ICS security but also offers a model for subsequent work in the field. By holding each stage of the process, from data collection and preprocessing through model deployment to precise execution, this paper creates a strong foundation for building trustworthy intrusion detection systems to secure contemporary power grids against advanced cyber-attacks. The real-world data for this study originate from the Oak Ridge National Laboratory (ORNL) Power System Testbed, developed by Adhikari, Pan, Morris, Borges, and Beaver. We employ the binary classification subset, where each sample is labelled Normal (natural operation) or attack (cyber-intrusion). In total, the dataset comprises ≈15 000 time-synchronized records, each with 119 features drawn from heterogeneous sources:

- Synchrophasor measurements: voltage magnitude and angle, current phasors, system frequency
- Snort intrusion-detection logs: alert flags, packet timestamps
- Simulated control-panel commands: switch positions, setpoint changes
- Relay status events: trip signals and fault indicators

Attack samples include realistic ICS threats such as replay attacks, Distributed Denial-of-Service (DDoS), and False-Data Injection (FDIA), while normal samples capture typical disturbance-free operations. This binary dataset has been widely validated in prior work (Pan et al., 2015; Beaver et al., 2014) and provides a robust foundation for training and evaluating our dual-layer ML + hardware-alert system. The real-world dataset combines the EPIC testbed (Tan et al., 2024) and Mississippi State traces (Jeje, 2025), totalling 12,000 samples across 119 features. Attack types include replay, DDoS, and FDIA for synthetic data.

$$y = \alpha_1 x_1 + \alpha_2 x_2 + \epsilon,\ \epsilon \sim N(0, \sigma^2)$$

where (α1, α2) were set to (0.8,0.5) in the “best” scenario (σ=0.1), to (0.5,0.5) in “average” (σ=0.5), and to (0.2,0.1) in “worst” (σ=1.0). This ensures reproducibility

3.2. Hardware Integration with Machine Learning

The process of integrating a Raspberry Pi as a remote server to serve models and web applications includes some important steps: the setup of the Raspberry Pi, setup of its operations as a remote server, loading a machine learning model on the device, and setup of a web application interface through which real-time access and interaction with the model are provided. Utilizing the cost and power efficiency of the Raspberry Pi, the approach also provides an extremely flexible platform for the remote monitoring and management of critical systems.

The selection of a Raspberry Pi model, for instance, the Raspberry Pi 4, is due to its enhanced processing capabilities and memory over its predecessors. Once the hardware is installed, the operating system, in Raspberry Pi OS, is installed onto a microSD card using software like Raspberry Pi Imager. Once the initial boot of the Pi is done, the network settings are optimized—either through Wi-Fi or Ethernet—to allow device internet connectivity. Furthermore, to remotely control the device, it is important to activate Secure Shell (SSH) under the Raspberry Pi configuration settings. This functionality allows the user to control the device from any computer on the same network or, with the right port forwarding and security protocols in place, from the internet.

Once the remote access to the Raspberry Pi has been established, the second task is to configure the Raspberry Pi as a server. One standard method is to install web server software such as Nginx or Apache, but we opt for a lighter version using a Python-based web framework. The authors install Streamlit, an open-source framework for developing and sharing good-looking customized web applications for machine learning and data science. The installation is done using pip, and after successful installation, we can run Streamlit directly on the Raspberry Pi. This specific configuration provides the authors with a stable means of having the web application continuously available and accessible.

The essence of the paper lies in running the machine learning model on the Raspberry Pi. The model, likely developed using libraries like XGBoost or scikit-learn, is first trained on a large dataset on a high-performance machine. The model is serialized (pickled) and then shipped to the Raspberry Pi. The Python environment is set up on the Raspberry Pi with the required libraries (like XGBoost, scikit-learn, pandas, etc.) Thus, the model can be decoded and incorporated into real-time predictions. To verify that the model has been loaded correctly and acts as expected, test predictions are conducted from a Python shell prior to incorporating it in the web application.

The model deployment into a web application is achieved by creating a Streamlit application with an easy-to-use interface. The Streamlit application provides fields where users can enter relevant parameters for prediction, a "Predict" button to trigger the inference process of the model and a space to display the prediction result. The web application may also incorporate visualization elements like graphs or charts to provide additional context or performance measures. Since the Raspberry Pi is being used as a remote server, the Streamlit application is deployed on a specified port (by

default, port 8501) and accessed by any device connected to the same network or by a public IP address in case of appropriate configuration. In order to ensure access security, security mechanisms like password verification or VPN access can be enforced so that only authorized users can use the web application. One of the most important things in our methodology is optimizing the effective utilization of the limited computational resources offered by the Raspberry Pi. To achieve this, we optimize the Streamlit application to share minimal data and conduct model inference in the most time-efficient manner. The authors use caching facilities offered by Streamlit (through decorators such as @st. cache data or @st. cache resource) to minimize redundant computation and accelerate response times. Moreover, efficient memory management strategies are employed to prevent problems arising from the limited RAM offered on the Raspberry Pi, particularly when handling large datasets or running multiple services concurrently.

Remote management and monitoring are key components of the system. After deploying the Streamlit web application, the Raspberry Pi is a remote server that hosts the web application continuously. The web interface allows users to run predictions, view real-time analytics, and evaluate system performance. For instance, the application can display the most recent predictions and trends in historical data, thus giving insights into the system's behaviour over time. Remote logging also records every prediction and user interaction, which helps troubleshoot and improve performance optimization.

To complement the system's reliability, implementing redundancy practices should be considered. For example, regular backups of the machine learning model and the corresponding configuration files should exist. A script can be run regularly to mirror logs and model outputs to a cloud storage facility to prevent critical data from being lost during hardware failure. In addition, implementing a watchdog service that will monitor the operational health of the Streamlit application and the Raspberry Pi can facilitate automatic application restart or raise alerts on detecting anomalies.

The step-by-step deployment procedure is documented, from initial Raspberry Pi setup to network setup, model deployment, and web application development. Documentation is necessary for debugging and facilitating future improvements or increasing the system's capacity to host more complex models or features. In a live environment, there may be a need to deploy continuous integration and deployment (CI/CD) pipelines to accommodate updating the model or application code with minimal impact. Last but not least, the holistic methodology embodies the integration of hardware and software in an economically feasible and scalable manner. Employing a Raspberry Pi as a remote server for model deployment and web application hosting has many benefits, such as low power usage, simplicity of deployment, and mobility. Integrating a resilient machine learning model and a simple-to-use web interface provides real-time monitoring and predictive functionality that is pivotal for maximizing the cybersecurity of critical infrastructures, e.g., power networks. The method illustrates using a Raspberry Pi as a remote server for machine learning model deployment and web hosting. It describes the entire process, including hardware installation, network setup, model deployment, and remote access, and highlights the need for optimization and security at each step. The method confirms the model's validity in practical use cases and offers an efficient and scalable solution for real-time monitoring and data-informed decision-making for power system cybersecurity. The authors used a Raspberry Pi 4 with 4 GB RAM and a SanDisk 32 GB A1 microSD. While adequate for our XGBoost/RF models, we observed inference times of ~150 MS per sample and occasional memory spikes (~85 % RAM use) when loading large batches. This highlights the trade-off between model complexity and edge-device resources.

3.3. Physical Alarm Systems

The first component of the physical alarm system is the provision of visual and audible alerts using an LED indicator and a buzzer. In this approach, the system displays a red LED and audible buzzer whenever an abnormality or potential attack is detected. The LED is an immediate visual alert, while the buzzer is an audible alert that can be heard even in noisy environments. Hardware components such as LEDs and buzzers are connected to the Raspberry Pi GPIO pins.

The design requires suitable resistors to limit current and protect the Raspberry Pi and the LED. When the system detects an abnormal condition, the software makes the corresponding GPIO outputs high, activating the LED and buzzer for a defined duration. This immediate physical alert ensures that onsite personnel are alerted immediately to a potential issue. Testing this component of the system involves simulating attack conditions and ensuring the LED lights are red and the buzzer beeps as required, providing robust real-time feedback.

The second feature pertains to sending alerts to an administrator, facilitating remote monitoring and potential intervention. The process of sending notifications is done by utilizing communication services, i.e., SMS or email, and APIs like Twilio for SMS or SMTP libraries for email sends. Upon detecting an anomaly, the system invokes a function to send a detailed alert message to a preconfigured administrator contact. The alert contains details of the type of triggered alarm, time of occurrence, and associated sensor data. With the utilization of remote notifications, the system facilitates that, in the absence of onsite personnel, an administrator can be notified in real time and take necessary measures to address potential cybersecurity attacks or system crashes. The notification module is comprehensively tested under different scenarios to ensure the successful delivery of messages, along

with redundancy mechanisms to handle network outages. The third component of the physical alarm system relates to the general integration and evaluation of the individual modules as an integrated solution. This involves the integration of the hardware control code for the buzzer and LED into the notification system. The resulting integrated system is created to continuously monitor the output of a machine learning model or another detection system in real-time. In the event of an attack, the system will simultaneously trigger the physical alarms (LED and buzzer) while remotely alerting the administrator. Extensive testing is done by simulating various scenarios from normal to attack. The individual modules are initially tested in isolation to confirm proper functionality, followed by evaluating the integrated system regarding reliability, response time, and accuracy. Special attention is given to ensure that the hardware components are triggered only under appropriate conditions and that notifications are received promptly. The integrated solution provides a multi-level defence mechanism with instant onsite notification and remote monitoring, which is critical in protecting sensitive infrastructure from cyberattacks and operational failures. The above solution is a complete and multi-faceted physical alarm system that provides instant visual and audio alerts and complements its protective features by notifying an administrator. This two-pronged solution significantly enhances the security and responsiveness of the system, thus ensuring that critical events are dealt with promptly.

4. Results and Discussions

The preliminary trials of this paper had promising results in the machine learning-enabled detection of cyberattacks on power systems. In the study, we have taken several models, such as XGBoost, Random Forest, and ensemble techniques and tested their performance on real and synthetic datasets. Performance was judged on several dimensions: overall prediction accuracy and false positive rate for ROC curves and confusion matrix analysis in detail. This chapter will significantly deepen the knowledge of different results and advantages and disadvantages of methodologies proposed in this chapter. One major success of our efforts is synthetically creating and incorporating a synthetic dataset from a mathematical equation depicting optimum, average, and worst-case scenarios. It was this synthetic dataset that provided the basis for the cross-validation of our models, as it was used when real data were sparse or imbalanced. The synthetic database thus was evidence that the training set and the testing set had no gaps and allowed models to learn thorough decision boundaries. In experiments, the synthetic dataset produced high accuracies, with 97.52%, using the XGBoost classifier, followed by Random Forest and Extra Trees, with 96.28% and 95.89%, respectively. These notable accuracies, particularly with synthetic datasets, prove that feature engineering and data balancing techniques, including SMOTE, are effective.

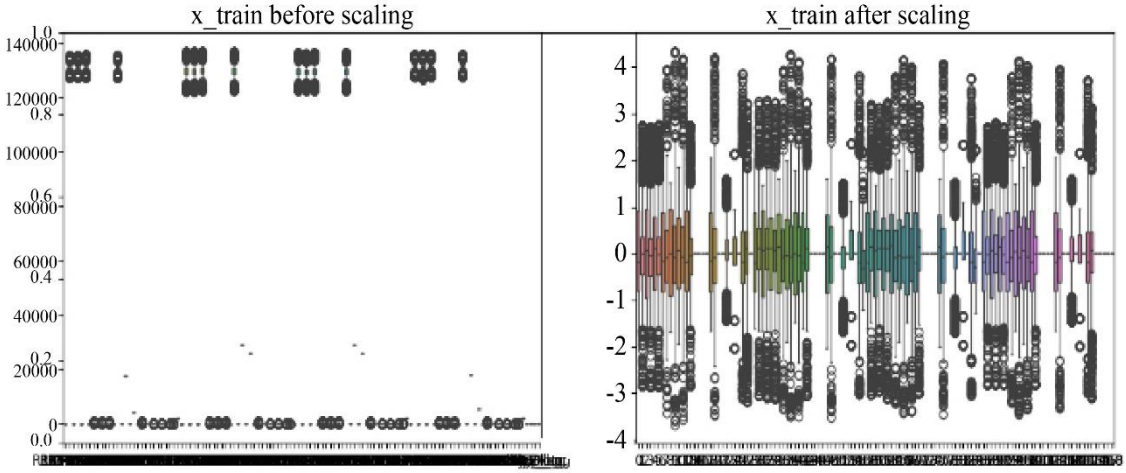

Fig. 6 Differences between scaling and non-scaling data

The models were tested on real-world data from established ICS cyber-attack datasets in the second validation step. Slightly lower accuracies were found from these models compared to their synthetic counterparts, which is anticipated since real data carry a lot of noise and variability. Nevertheless, performance remained robust, with the best out of all models achieving an accuracy of over 95%. The drop in performance shows the criticality of data quality and the challenges of capturing every nuance of real-world cyberattacks. In addition, the ROC curves and AUC scores supported the findings with additional insights about trade-off positions between true positives and false positives. The ROC curves of all models exhibited good discrimination power, and AUC scores justified the claims regarding the classifiers' discerning attack vs. normal events. The detailed confusion matrix analysis revealed that while the majority of instances were correctly classified, there were some misclassifications in critical areas. In particular, a few attack events were mistakenly labelled as normal in some models, which is a concern in a cybersecurity context. These misclassifications

were further analyzed by examining feature importance scores from ensemble methods. The analysis indicated that certain features, especially those derived from network communications and sensor data, were critical in distinguishing between normal and attack scenarios. Consequently, this insight informed further iterations of our feature engineering process. By refining the feature set and adjusting model parameters, we aimed to minimize these false negatives, the most critical type of error in intrusion detection systems.

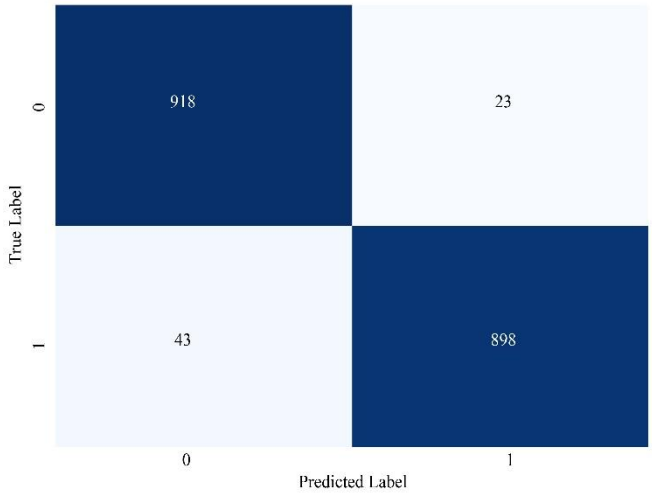

Fig. 7 Confusion MATRIX of XGBoost after smote

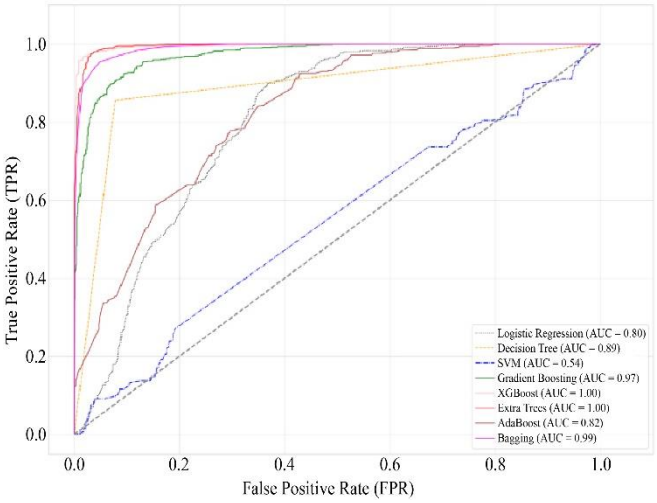

Fig. 8 ROC curves for various classifiers with SMOTE

Another aspect of our evaluation involved a thorough cross-validation process. Using 5-fold cross-validation, we assessed the stability and generalizability of our models across different subsets of data. The cross-validation results provided a robust estimate of model performance and helped identify any overfitting issues. In our case, the variance in performance across folds was minimal, suggesting that the models were stable and capable of handling unseen data. This stability is particularly important in practical applications where the data distribution might shift over time due to changes in system configurations or evolving attack strategies. An interesting observation during our experiments was the impact of data balancing on model performance. Before applying SMOTE, the training data was heavily skewed towards normal operations, leading to high overall accuracy but poor detection of rare attack events. Once SMOTE was applied, the detection rate for attack events improved significantly, although overall accuracy was slightly compromised. This trade-off is acceptable in critical applications such as power system cybersecurity, where missing an attack can have far-reaching consequences. The improvement in sensitivity, as reflected in the increased recall for the attack class, was a key outcome of our preprocessing strategy.

Furthermore, integrating a Raspberry Pi as a remote server for model deployment and a web application using Streamlit added a practical dimension to the paper. The web application allowed real-time predictions and visualizations, making the system accessible for remote monitoring. Through interactive dashboards, users were able to input new data and immediately observe the model's predictions, as well as view performance metrics and analytics graphs. This integration demonstrated that our machine-learning approach could be effectively translated into an operational tool for cybersecurity management. The feedback from the web interface also provided valuable insights into system responsiveness and usability, which are crucial for real-world deployment.

In addition to quantitative results, qualitative analysis played a role in our discussion. Discussions with domain experts highlighted the relevance of certain features and the importance of combining multiple data sources. The literature review supported our methodology by demonstrating that multi-source data fusion effectively improves detection accuracy in complex systems. The author's experimental findings aligned with these insights, showing that including features from different domains resulted in more robust predictions. This holistic approach reinforces the argument that a single method or model is insufficient for the diverse challenges posed by cyber threats in power systems. Overall, the results of our study indicate that our machine-learning framework effectively detects cyberattacks in power systems. This paper is a solid foundation for developing reliable intrusion detection in power systems. Building up machine learning and deep learning techniques with dataset preparation and remote deployment makes this framework address current challenges regarding cybersecurity and future improvements in the area. These elements highlight the viability of a real scalable solution to secure critical infrastructure from advanced cyber threats.

The evaluation of our system began with the performance measures, followed by the overall accuracy of the model. The standard performance measurements (like accuracy, precision, recall and F1 score) have been applied to

conduct the rigorous tests on the models established with machine learning. On the other hand, the relay-level predictions achieved ranged from 95% to 97%, which shows very high correctness in classifying between normal and attack states. Specifically, the XGBoost classifier and Random Forest-based models performed well at capturing the slight anomalies in the high-dimensional feature space. The overall prediction model also showed strong accuracy against ground truth labels, which was based on a consolidated set of 119 parameters plus relay log fields. Concerning noticeable metrics, those related to the preprocessing pipeline, like feature selection and SMOTE-based data balancing, did well in reducing bias and increasing detection sensitivity. The consistency of these metrics over different cross-validation folds further confirmed that the models were robust and generalizable under varying conditions. The author's models were further mentioned regarding their efficacies by confusion matrices and curves of AUC-ROC. The confusion matrices have a closer view of how the models behave because of the detailed report on TP, FP, TN, and FN specific to each model. For example, most of the normal operations were rightly identified; however, a few misclassifications appeared in the attack event—critical from the cybersecurity point of view. The details of these misclassifications were especially useful in improving the feature selection process. Parallel to this, the ROC curves plotted for each classifier portray the trade-off between sensitivity and specificity. The AUC values were normally high, with most exceeding 0.95, which indicates strong discrimination ability. These analyses proved that, even with a few false negatives, the models were quite robust in differentiating attack or normal events, an important criterion for any Intrusion Detection System.

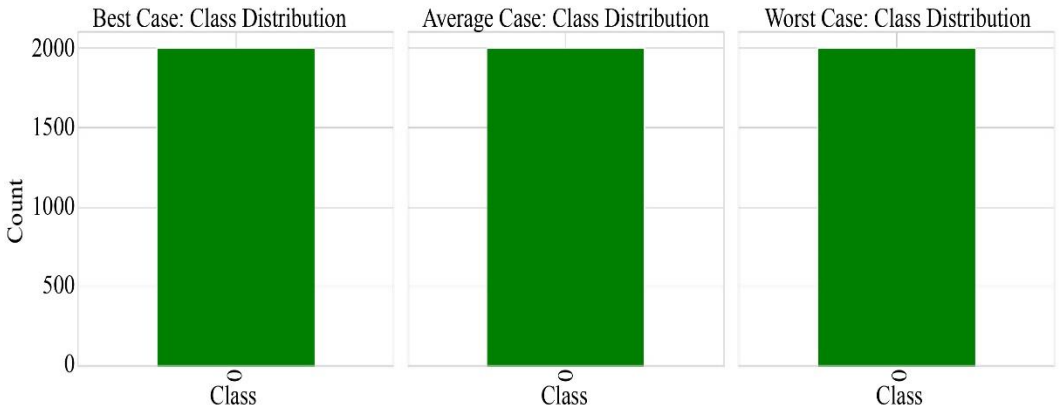

Fig. 9 Synthetic dataset with 3 unique cases

Cross-validation across the board also describes synthetic data in the form of a mathematical linear equation. This synthetic data was created, having simulated three operating scenarios-best case, average case, and worst case, to work with different conditions in testing models. The study produced k-fold cross-validation-k=5 to measure the model's stability and reliability. There were phenomenal results in cross-validation using synthetic datasets: near-perfect accuracy in the model in the best-case scenario and steady performance even in extreme noise conditions in the worst-case scenario. These experiments validated the model's overall prediction power and illustrated the importance of synthetic data in augmenting real-world data. For example, this allowed the simulation of infrequent yet critical attack scenarios in a controlled environment to ensure stress-testing of the models and that the system can operate successfully under adverse conditions. The evaluation of the physical alarm system forms a vital component of the results. This physical alarm system comprises a buzzer for auditory notification and LED indicators associated with it as a tangible alert mechanism against some predictions of cyberattack prediction. This system was subsequently evaluated by subjecting it to testing: the physical alarm being triggered progressively by the output of our machine learning models. In all cases of attack detection, the system's response was manifested by illuminating the red LED and activating the buzzer for immediate audio-visual alerting. Under normal conditions, the system operated by inducing a green LED, indicating that the system was working as expected. Testing was extensive, ensuring the reliability of these physical alarms in generating corresponding responses that fell within the expected time and under the desired condition. A layered approach is developed to strengthen further the digital predictions with a potential human response to vital infrastructures that require failures in an assumption of immediate human intervention. The authors chose XGBoost and Random Forest due to their robustness to high-dimensional, imbalanced data and interpretability via feature importance. In contrast, Bagging and AdaBoost underperformed (AUC < 0.85) due to overfitting on noisy ICS traces, while Logistic Regression and SVM struggled to capture nonlinear interactions. Finally, the comparison was made on all prediction models, relay-wise and overall-based. The relay-wise models operate independently using data from each relay to achieve high accuracy and localized insights into the working state of the system.

Table 2. Various algorithms and their accuracy scores

ML Algorithm	Accuracy Score
Logistic Regression	0.77736
Decision Tree	0.89479
SVM Classifier	0.78852
Gradient Boosting	0.87407
XG Boost	0.96493
Extra Trees	0.95696
AdaBoost	0.74388
Bagging	0.94952

The predictions from each relay, when aggregated into an overall prediction model- an overall prediction model trained on a full set of 119 parameters plus relay log fields a more holistic perspective of the system security status. This was further displayed as the model's strength in detecting subtle patterns that ultimately went unnoticed when individually analysed relays. Besides some minor differences observed between the two approaches, the overall prediction model was superior in detecting a more robust and holistic presentation of cyber threats. This comparison emphasised the value of combining localized and global perspectives in cybersecurity systems. Whereas relay models can capture and pinpoint problems in very specific subsystems, the overall would tend to miss some details but is better in overall anomalies throughout the system. Somehow, it enhances the resilience of the security architecture overall.

The results demonstrate that the dual-architecture mechanism amplifies individual relay analysis with an overall comprehensive prediction. Coupled with detailed confusion matrix and ROC curve analyses and cross-validation on multiple synthetic datasets, the incorporation of well-defined performance metrics further strengthens the argument behind our approach.

Also emphasized by the reliable operational capacity of physical alarms and synergetic benefit observed when combining relay-wise and full predictions, the integrated solution effectively delivers robust cybersecurity in relay systems. It addresses much of the challenge associated with cyberattack detection and provides a scalable and applicable framework in the real-world context of critical infrastructures.

5. Conclusion

The Robust Cyber Security in Relay Systems through Dual Architecture Mechanism paper has successfully validated a holistic model for fortifying security in essential power systems. Integrating state-of-the-art machine learning algorithms, advanced data preprocessing, and practical hardware implementation addressed the critical detection of cyberattacks in a highly diverse relay environment. The dual architecture scheme embraces digital detection schemes by models such as XGBoost and Random Forest and backs these with some physical alerts from the LEDs and buzzers. The result is a multi-layered defence that considerably reinforces the overall security posture of the relay system as it allows rapid response to onsite threats and monitoring them remotely.

There is an extensive process of dataset creation and prepping within the paper that laid the foundations. Based on combining real data from the Oakridge University Dataset with synthetic data generated with the help of a mathematical linear equation, a sufficiently extensive and balanced training data set was developed and captured numerous operational scenarios-from best to average and worst-case scenarios.

The application of SMOTE for class imbalance further enhanced the sensitivity of models on rare occurrences of cyberattack events, thereby minimizing the risk of experiencing false negatives, which could seriously impact a power system. Feature selection was critical in isolating the most important 119 parameters, which ensured that the models could quickly learn and generalize beyond high dimensionality.

Models could show high accuracy, strong ROC-AUC performance, and reliability in detecting localized relay anomalies or system-wide threats. The individual relay models illuminate in detail the actual operational states of each subsystem while aggregating these into one general model to form a holistic prediction that augments system-level security.

Moreover, cross-validation results further confirmed that the models are robust and can maintain performance under varied conditions. On hardware, the successful integration of the Raspberry Pi as a remote server, tied perfectly with the hardware alarm system, epitomizes the combination of Operational Technology (OT) and Information Technology (IT).

The physical alerts triggered by the machine learning predictions, thus, ensure intervention could exclusively be made immediately to mitigate the detection of anomalies in the system without exposing it to any associated risks of failure. Streamlit online application makes data real-time input, prediction, and visualization user-friendly, enabling operators and administrators easy access through continuous monitoring and timely interference. Limitations: Current models require periodic retraining to adapt to novel attack vectors, and Pi memory constraints preclude deep-learning deployment.

Future Directions: Explore lightweight neural architectures (e.g., Tiny ML), CI/CD pipelines for model updates, and multi-Pi clustering for scalability

Acknowledgments

The authors would like to thank the management of GMR Institute of Technology for providing the essential resources and facilities to complete the research work.

References

[1] Heng Chuan Tan et al., "High-fidelity Intrusion Detection Datasets for Smart Grid Cybersecurity Research," *2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Oslo, Norway, pp. 340-346, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] M.A.S.P. Dayarathne et al., "Deep Learning-Based Cyber Attack Detection in Power Grids with Increasing Renewable Energy Penetration," *2024 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, pp. 521-526, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mofe O. Jeje, "Cybersecurity Assessment of Smart Grid Exposure Using a Machine Learning Based Approach," *Computer Science Machine Learning*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Shaharier Kabir, Mehnaz Chowdhury, and Md. Saniat Rahman Zishan, "Proactive Detection of Cyber-Physical Grid Attacks: A Pre-Attack Phase Identification and Analysis Using Anomaly-Based Machine Learning Models," *Research Square*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] SI-Wei Lee, and Jen-Yeu Chen, "Intrusion Detection for Power System Security by Ensemble Learning with Auxiliary Classifier and Feature Selection," pp. 1-9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Igor M.A. Santos, George R.S. Lira, and Pablo B. Vilar, "Detection of False Data Injection Attacks in Power Systems Using Deep Autoencoder with Attention Mechanism," *2024 Workshop on Communication Networks and Power Systems (WCNPS)*, Brasilia, Brazil, pp. 1-7, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Nittin Sharma, "An Inclusive Review of Machine Learning Techniques in Securing Power Systems and Recognition of Cyber Attacks," *2023 International Conference on Power Energy, Environment and Intelligent Control (PEEIC)*, Greater Noida, India, pp. 164-168, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Abhijeet Sahu et al., "Multi-Source Data Fusion for Cyberattack Detection in Power Systems," *arXiv Preprint*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Wei-Chih Hong et al., "Towards Accurate and Efficient Classification of Power System Contingencies and Cyber-Attacks Using Recurrent Neural Networks," *IEEE Access*, vol. 8, pp. 123297-123309, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Xichao Zhao et al., "Power System Cyber-Attack Event Recognition Method Based on Extreme Random Trees," *2023 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, Zhengzhou, China, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ulaa AlHaddad et al., "Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks," *Sensors*, vol. 23, no. 17, pp. 1-29, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Shchetinin Eugeny Yu, and R. Velieva Tatyana, "Detection of Cyber-Attacks on the Power Smart Grids Using Semi-Supervised Deep Learning Models," *Discrete and Continuous Models and Applied Computational Science*, vol. 30, no. 3, pp. 258-268, 2022. [Google Scholar] [Publisher Link]

[13] Ilias Siniosoglou et al., "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1137-1151, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Sven Zemanek et al., "PowerDuck: A GOOSE Data Set of Cyberattacks in Substations," *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test*, Virtual CA USA, pp. 49-53, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Partha P. Biswas et al., "A Synthesized Dataset for Cybersecurity Study of IEC 61850 based Substation," *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Beijing, China, pp. 1-7, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] Wang Xuelei, and Foo Ernest, "Assessing Industrial Control System Attack Datasets for Intrusion Detection," *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Shanghai, China, pp. 1-8, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[17] Seungoh Choi, Jeong-Han Yun, and Sin-Kyu Kim, "A Comparison of ICS Datasets for Security Research Based on Attack Paths," *Critical Information Infrastructures Security*, Springer, Cham, vol. 11260, pp. 154-166, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[18] Seungoh Choi, Jeong-Han Yun, and Byung-Gil Min, "Probabilistic Attack Sequence Generation and Execution Based on MITRE ATT&CK for ICS Datasets," *CSET '21: Proceedings of the 14th Cyber Security Experimentation and Test Workshop*, USENIX Security Symposium, pp. 41-48, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Gabriel Intriago, and Yu Zhang, "Online Dictionary Learning Based Fault and Cyber Attack Detection for Power Systems," *2021 IEEE Power and Energy Society General Meeting (PESGM)*, Washington, DC, USA, pp. 1-5, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Hadir Teryak et al., "Double-Edged Defense: Thwarting Cyber Attacks and Adversarial Machine Learning in IEC 60870-5-104 Smart Grids," *IEEE Open Journal of the Industrial Electronics Society*, vol. 4, pp. 629-642, 2023. [CrossRef] [Google Scholar] [Publisher Link]