Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

Resilient Cybersecurity Architecture for Modern Power Systems: Addressing Threats to Critical Infrastructure

Syed Umair Akhlaq

Roamsol Technologies, UAE

Author Email: umairakhlaque78@gmail.com

Abstract

The high rate of progress in digital technologies in power systems has led to specific cybersecurity risks, primarily in control areas of SCADA and ICS. Current modern threats to security, including data injection, masquerading, and replay attacks, have gotten ahead of the capability of the old perimeter defences. The proposed cybersecurity architecture in this research is resilient, including layered defence, machine learning for intrusion detection, and a rule-based alert system based on SIEM methodologies. The architecture is deployed with distinct layers for the physical, communication, monitoring, and control to support defence-in-depth and to allow flexible responses to faults. A Random Forest model was built and evaluated on the Power System Intrusion Dataset retrieved from Kaggle, with a full-scale recordation of all sensors and temporal operation. Accuracy was 97%, and F1-scores were high throughout all classes, demonstrating the model's robustness amid imbalance. The probabilistic outcomes produced by the classifier were passed along to a rule-based alert system emulating SIEM functionality, and firing alerts as the estimated fault probability exceeded 0.5. Systems effectiveness was confirmed by critical evaluation indicators such as ROC-AUC 0.93, confusion matrices, and thorough alert tables. The designed architecture favours interpretability, responsiveness, and adaptability for SCADA systems, avoiding the tricky and obscure aspect of deep learning approaches. It bridges the gap between the academic theories of machine learning and the functionality needs of operational cybersecurity and provides an architectural framework to support smart grid resilience. Possible future improvements may include the addition of temporal modelling, adaptive alert thresholding, and real-time edge deployment.

Keywords: Smart Grid Security, SCADA, Intrusion Detection, Random Forest, SIEM, Critical Infrastructure, Cyber Resilience, Zero Trust, Machine Learning, Power System Monitoring

1. INTRODUCTION

Digital transformations in power systems have entirely transformed the mechanisms of energy generation, transmission, distribution, and monitoring [1]. Traditional, isolated power networks are being replaced by systems that understand and embrace cutting-edge sensing, networking, and automated controls. This shift that enhances operational efficiency and facilitates dynamic decision-making generates new cybersecurity risks. As the SCADA systems and ICS become

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

an intrinsic part of power grids, their systems are exposed to the risks inherent in IP-based and open systems. This advance necessitates a radical rethinking of cybersecurity strategy in the energy sector [1].

Cyber threats have experienced significant transformation as the merging of OT with IT in critical infrastructure systems has accelerated [2]. Before integrating IP-based technologies, power systems secured themselves with isolated networks and specialised communication techniques. Nowadays, smart grid infrastructure is exposed to multiple attack vectors such as remote unauthorised access, insider threats, and dangerous malware risks that compromise network communications and physical infrastructure functions [3]. The 2015 Ukraine power grid attack is a shining example of these weaknesses, demonstrating how attackers could use spear-phishing and malware (BlackEnergy) to shut down substations and cause massive power outages. Similarly, the 2021 Colonial Pipeline ransomware attack became an example of the degree of cyber-episode that can cause havoc in national economies and weaken public confidence in digital infrastructure [3].

These cases emphasise the need for cybersecurity architectures beyond conventional firewalls and access control measures. The solution must ensure security and the capacity to quickly react to threats, reduce downtime, and provide quick recovery after incidents [4]. In this case, resilience has to be the first in order of priority as a fundamental pillar of the design of cybersecurity. Cybersecurity systems whose design includes resilience capabilities should include anomaly detection, automatic incident handling, threat intelligence integration, and recovery from system failure that is secure. Such resilience is critical in power systems where such disruptions by malicious actors or unplanned downtime would cause serious harm to public safety and economic health [3].

To address the need, our research involves designing and testing a lightweight, data-driven, and resilient cybersecurity framework that is domain-specific to the power system domains. This study combines a traditional machine learning technique for intrusion detection and a simulated alerting component that reflects the functionalities of SIEM. A Random Forest Classifier, a proposed approach, is trained using a realistic example in the Power System Intrusion Dataset from Kaggle; both normal and fault activities are included in the observed simulated power system. Supervised learning methods let the system identify subtle differences in activity and produce reliable differences between legitimate situations and potential hazards.

Furthermore, this study also applies a novel SIEM alert generation simulation that is being used in conjunction with the machine learning element. By basing the system on replicating industry-triggered mechanisms using rules, the transition from raw data classifications to actionable alerts becomes easily accomplished. When estimated chances of an incident exceed a predetermined value, alerts are generated, allowing operators to focus on major incidents and reduce unwarranted notifications. Such logic is essential for timely situational awareness and

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

prompt remediation in the high-paced operational environment familiar to power grid control rooms.

One of the key results of this work is that it is compatible with Zero Trust methods, which encourage identity validation, reduced permissions, and perpetual surveillance. While the current implementation does not use network-level Zero Trust controls, it promotes security by designing the detection and alerting system on the premise that every component and actor can be untrusted. Therefore, the system embraces Zero Trust principles, i.e., continual validation, flexible security requirements, and systematic reliance on decision-making on data.

Contrary to cumbersome, cloud-based security systems that may not be cost-effective for systems with low-latency requirements, this solution aims at streamlined processing and on-weighted decisions at the decentralised point. Using Random Forest models finds the balance between sophisticated modelling and lucid explainability, ensuring that the solution will stay effective and transparent for system administrators. Designed for edge computing scenarios, this model makes locating the solution in a substation controller or an observing gateway possible.

The suggested framework is a robust cybersecurity platform for sophisticated power systems with a looming threat detection and prompt alert system. By incorporating the combination of supervised classification, simulated SIEM functionality, and Zero Trust concepts, the proposed framework can meet the growing needs for cyber resilience for critical infrastructure. The paper further talks about the dataset attributes, the method followed, the process of implementation of the solution, and the findings of the assessment to prove that the solution is practical and effective.

2. LITERATURE REVIEW

2.1 Overview of Existing Standards: NIST CSF, IEC 62443, Zero Trust, and ITIL for Service Security

Digital integration of critical infrastructure has been further improved, igniting high interest in standardised cybersecurity frameworks [5]. Start by identifying risks, prioritising a protected system, creating strong detection mechanisms, and then rapid response, followed by effective recovery. The NIST CSF promotes adoption across the power sector, thus establishing provisions for system security enhancement, threat response, and maintenance of service continuity. For the architectural design of the modern power systems, the NIST CSF will help develop resilient architectures capable of adequately addressing emerging cyber challenges [6].

Apart from these standards, IEC 62443 is explicitly designed for Industrial Automation and Control Systems (IACS) [7]. It creates a multi-tiered structure for asset diagnosis, improving access control, and securing network segments. It is especially characteristic of this standard application when speaking of SCADA for power infrastructure, where the safe state of

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 Revised: 05-11-2024 Accepted: 22-12-2022

operation and strong cyber defence are necessary. Even though IEC 62443 presents a rigorous structure, its implementation is problematic, especially in data-centric smart grids because of its deep complexity and the bulk of compliance and verification tasks it requires [8].

A vital security advancement has recently been outlined in NIST SP 800-207, the Zero Trust Architecture (ZTA) [9]. When it was started, ZTA assumed that all system access should be verified constantly, regardless of whether the user or device is trusted. Such key elements of ZTA, as real-time identity verification, adaptive authorisation, and behavioural audits, are ideally suited for supporting SCADA systems that are fragile to security threats such as insiders' activity and credentials abuse [10]. These benefits are offset by old systems, stringent real-time needs, and no fine-grained access controls in embedded devices, which prevent deployment of Zero Trust in the operations technology (OT) scenario [10].

ITIL offers essential lessons from its service management framework. A widespread practice in big IT organisations, ITIL provides uniform practices around managing security incidents, setting SLAS, and restoring IT services [11]. By using ITIL to power systems, security operations can become better integrated into service delivery as anomaly detection results are used to add to existing incident management processes [12]. Such an approach creates a responsive cyber protection mechanism that supports the overarching need for high availability and dependable service delivery.

2.2 SCADA/ICS Vulnerabilities and Limitations of Traditional Perimeter Defence

SCADA and ICS systems are still prone to attacks because of their legacy design and continued reliance on fixed security practices [13]. With smart adversaries exploiting zero-day exploits and social engineering, traditional perimeter defences like firewalls and air gapping are ineffective and failing to protect these systems. Since Modbus and DNP3 have no encryption and authentication, the large-scale usage leaves SCADA and ICS vulnerable to vulnerabilities such as replay attacks, spoofing, and command injection [14]. As a result of hugely critical uptime requirements, organisations tend to face challenges in addressing vulnerabilities rapidly. The risk of service interruptions forces most organisations to delay securing critical systems by patching or re-architecting them without securing against known threats [15]. Such weaknesses expose systems to vulnerabilities and illegitimate users' attacks for long periods.

Furthermore, many industrial systems lack logging and real-time telemetry, thus making detection inefficient in many cases. Time and time again, anomaly detection is highly demanding in these scenarios, so any responses are delayed or poorly informed [16]. IDS solutions are in the mainstream solution methods, but they frequently fail to detect new threats as signature detection methods are excessively relied on. Consequently, they fail to protect against the latest malware, sophisticated persistent threats, or atypical actions based on command-and-control activities [17].

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

2.3 Recent ML/AI Applications in Intrusion Detection

Driven by efforts to surmount these detection problems, there has been a significant trend towards the increasing use of machine learning (ML) and artificial intelligence (AI) within cybersecurity practices [18]. The techniques, such as Random Forest, SVM, and Gradient Boosting, based on machine learning, have been applied to define attacks and unusual activity in telemetry data. Among the best characteristics of Random Forest classifiers is their ability to handle large sets of features, overcome the problem of class imbalance, and produce understandable results [18]. Sequence learning and prediction for time series information are performed using Recurrent Neural Network (LSTMs), which are among the Recurrent Neural Networks (RNNs) [19]. These models allow temporal dependencies to be tracked well in the SCADA data to reveal stealthy attacks and attacks that are somewhat subtle in approach and execution over time. Clustering the behaviour profiles and outlier detection that point to attacks have been accomplished using unsupervised algorithms such as K-Means, DBSCAN, and Autoencoders [20].

However, most of these implementations are driven by being primarily created as proof-of-concept models, which are experimented with in a simulated environment or academic datasets [21]. These models have difficulties being deployed in actual environments. Issues include poor interpretability, high computational needs, and the complex task of coupling ML models with operational machinery. Furthermore, applying ML models to live operational processes, such as generating real-time alerts or automatically creating incidents, is rare, precluding their concrete usage [22].

2.4 Gaps Identified: Lack of Integrated Testing, Resilience Simulations, and SIEM-Alert Emulation

Although many ML techniques for power systems fault and anomaly detection are mentioned in academic works, there is a lack of complete cybersecurity systems that emulate real-time detection, alerting, and response systems. Although detection accuracy is a central aspect of studies that have already been conducted, there is an apparent lack of attention to the actual operation of ML results in incident management platforms and decision support systems [23]. However, standardised, real-world datasets for SCADA environments are notoriously missing from existing literature [24]. Intrusion detection research has limitations as most of the work depends on synthetic or sanitised data, which does not reflect the noisiness, variability, and complexity of real smart grid measurements [25]. Therefore, the reported performance is typically more hopeful than actual application scenarios, resulting in minimal effectiveness in practical applications [26].

In addition, standard solutions for enterprise IT, in the form of SIEM, are rarely applied to reinforce the SCADA protection measures [27]. SIEM systems perform rule-based correlation and incorporate threat intelligence and target alerts, vital for immediate response. When they

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

fail to implement SIEM-style validation procedures, ML models are inefficient, making operators unable to deal with actionable intelligence [28]. Finally, there is little insight into how Zero Trust principles fit and operate within ML-based intrusion detection once implemented within an integrated architecture [29]. While demonstrating how identity-aware access control and continuous verification can be combined with predictive anomaly detection to deliver layered, adaptive defence mechanisms is limited [30].

3. DATASET AND PREPROCESSING

3.1 Proposed Framework

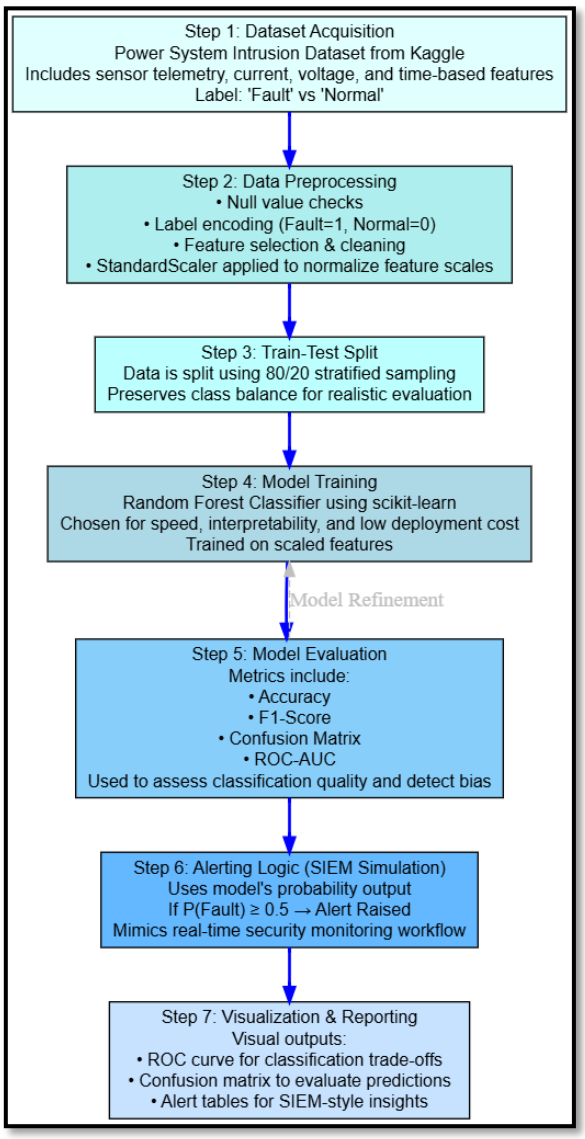

Figure 1: Proposed Methodology Diagram

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

A seven-phase approach is presented, as shown in Figure 1, to implement a strong cybersecurity framework within power systems. The first step is to obtain the Power System Intrusion Dataset from Kaggle, after which the data is pre-processed and a model is trained with Random forest and SIEM-style alerts for probability thresholds are carried out. The workflow guarantees high accuracy, clear reasoning, and real-time fault identification, and it is augmented by a feedback loop that enables continuous model tuning.

3.2 Dataset: Power System Intrusion Dataset from Kaggle

This research utilises the Power System Intrusion Dataset, which is obtainable at Kaggle, to test the proposed resilient cybersecurity solution for power systems. The dataset addresses a 'smart' infrastructure, rooted in simulated SCADA/ICS environments, providing a solid foundation for analysis of intrusion patterns. The datasets are divided into two groups, Train.csv and Test.csv, where all draws are multivariate and hold both time-sensitive and control layer features. It allows the development and evaluation of supervised learning algorithms in a real-world environment that merges digital control operations with measurements, which can simulate the performance of innovative grid systems under everyday and fault scenarios.

3.3 Description of Features: Time-Based and Measurement Parameters

More than 50 variables associated with the telemetry and control operations in smart grids were generated from coding for the simulation. Data is classified into two basic features: metrics that measure timing behaviour and electrical parameter values. Time, timeLastMsg, sqDiff, and stDiff metrics are used to measure the time and frequency of message and system update transmission. The measurement-based parameters include sensor data of IED4_iA, IED4_iB, and IED4_iC for current and MU 4VoltageAngleA, MU4VoltageAngleB, and MU 4VoltageAngleC for three-phase voltage phase angles. Control and status features like recentChange, any_relay, and state_cb reflect relay activation and system state transitions, making them valuable for detecting dynamic threats that manifest through command-level anomalies or measurement shifts.

3.4 Binary Classification: "Fault" vs "Normal" (Label Encoding)

The main target feature is the column for class, which for each record tells if it is "Fault" or "Normal". To fit the algorithms, especially the Random Forest classifier used in this work, the categorical class labels had to be represented numerically using Label Encoding. The class "Fault" was given a numerical value of 1, and "Normal" was given a value of 0, generating a binary class problem. This number representation of the labels aligns with the general goal of the architecture, which is to successfully classify normal and fault states to provide near-time threat alarms.

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

3.5 Null Checks, Class Distribution, and Label Imbalance

An exhaustive checking of the null values ensured that the dataset is intact because both the training set and test sets had no missing values or the following Nan values in any of the features. This allowed us to go straight to machine learning workflows without using data imputation. However, the authors observed that on the training set, there was a slight imbalance, where "Fault" records outnumbered the "Normal" ones. Although there was an imbalance, there was no need for synthetic balancing methods such as SMOTE; instead, evaluative metrics such as F1-score and confusion matrix were used to give a complete view of the model's performance in addition to accuracy.

3.6 Data Scaling Using StandardScaler

In the dataset, feature values were highly diverse, including minor binary indicators and larger numeric data points that extended into the hundreds or thousands. StandardScaler from scikit-learn was used to standardise the feature matrix and normalise feature influence when training the model. With each feature revolving around zero, sharing unit variance, the dataset was normalised to an even scale that mitigated biases towards high-magnitude features and facilitated better convergence, especially in distance-sensitive algorithms like Random Forests.

3.7 Feature Reduction and Cleaning

The preprocessing pipeline feature cleaning stage identified non-informative, redundant, or highly correlated variables, which were selectively removed. Identifiers that did not contribute significantly towards classification, such as static or almost constant, were dropped from the dataset. On the other hand, features critical for grid dynamics, such as stDiff, and control flags, e.g., recentChange, were retained because of their strong association with behavioural anomalies in the smart grid. Since the dataset only had the target as categorical and also did not have other categorical multi-class variables, there was no need for further data encoding.

3.8 Dataset Split for Validation

The dataset was then split into training and validation subsets by resampling on stratification to maintain class balance in an 80/20 split. Such an approach helped the model generalise well and provided an even data analysis. A pre-processed and normalised feature matrix was then introduced to a Random Forest Classifier to appropriately train it to identify between "Normal" and "Fault" instances. The Test.csv dataset was also processed similarly and held for the final performance validation and service, SIEM-style alert simulation (as described later).

4. PROPOSED ARCHITECTURE & METHODOLOGY

4.1 Layered Architecture: Physical, Communication, Monitoring, Control

The cybersecurity framework takes a layered approach that reflects the operational intricacies in the contemporary smart grid systems. This architecture delegates each level to a particular

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

role in the power system, treating security as a contextual and distributed problem, not a single monolithic system. The Physical Layer constitutes the first layer of our architecture, and here we have hardware components like intelligent electronic devices, sensors, and relay systems. Its primary duty is to protect physical connectors and retain the operational performance of associated hardware.

The Communication Layer (2nd position) controls the protocols and data channels for transporting measurements, commands, and updates between devices. The second tier also manages message buses, SCADA data frames, and Interdevice signal transfer. Security here is reinforced through assumptions of Zero Trust, ensuring all inter-device communications are evaluated, even from within the network perimeter.

The monitoring layer, representing the third level, is essential to deal with telemetry, monitor activities, and accumulate live data. This layer is critical in the empowerment of data-based anomaly detection and alert generation. Hierarchical systems and SCADA elements, which are elements of the Control Layer, are intended to control decision making, command giving, and grid activity alignment during this final architecture level. Paying attention to this layer is essential for ensuring operational stability because it must protect itself against intrusions by implementing enforced access restrictions and recording suspicious patterns of actions.

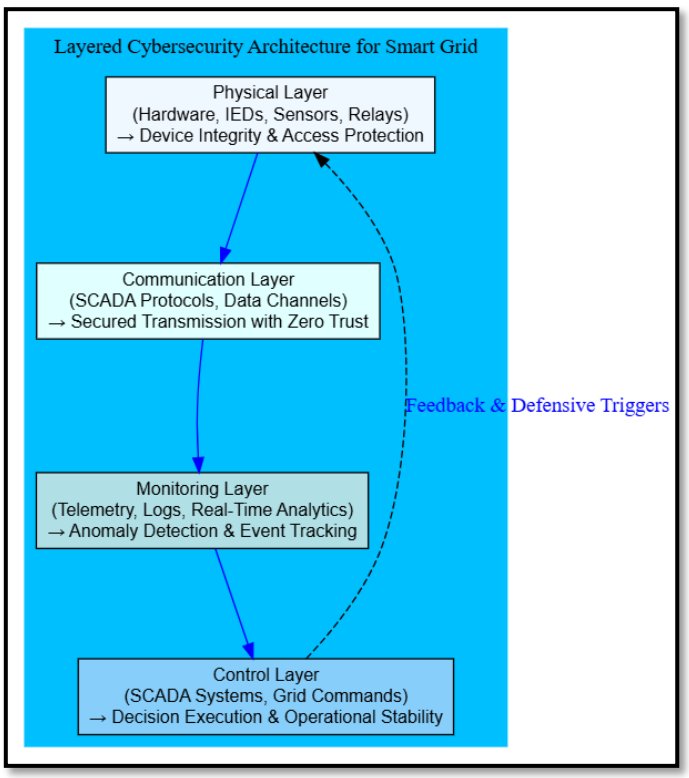

Figure 2: Layered Architecture Diagram

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

All these layers compose a modular, vertically integrated security model, enabling anomalies or faults detected at one of these layers to trigger countermeasures on the next layer. This design has the defence-in-depth practised (redundancy and cross verification across the layers) (Fig. 2).

4.2 Modelling Engine: Random Forest Classifier for High-Speed Threat Detection

The base of the architecture design is the modelling Engine, a real-time machine learning module specifically engineered to identify and respond to cyber-induced anomalies and faults. A Random Forest Classifier was selected for this task due to its reliability, speed, and outstanding behaviour on structured data common in smart grid telemetry. During training, the classifier builds decision trees and returns a final class prediction by pointing out the most often output in the ensemble.

The data set transformed and normalised from the Power System Intrusion Dataset gives data about time, values of current, the angle of voltage, and information about the statuses of relays. Using its ability to analyse multivariate correlations, the Random Forest classifier can identify regular operation distinguishing characteristics and cyber-based faults or irregularities.

Random Forests are excellent at preventing overfitting, especially when input data characteristics vary. Random Forests provide a quicker deployment process than deep learning models, which generally require significant hyperparameter tweaking and augmented processing power, especially from devices of limited processing capabilities. Consequently, Random Forest models are perfectly suited for deploying secure and seamless surveillance in industrial control systems.

4.3 Alerting Layer: SIEM-Style Logic Using Probability Thresholds (≥ 0.5 = Alert Raised)

A simulated operational response is created by incorporating an Alerting Layer into the architecture based on SIEM principles. The Alerting Layer massages the predicted class probabilities served up by the Random Forest model and issues binary alerts using a given threshold. The threshold used in this implementation was 0.5: If any event has a fault probability of over 0.5 predicted, an "alert raised" notification is sent out. This approach captures the working model of actual SIEM systems by using correlation and threshold methods to filter important alerts and those that are not so important.

Generated alerts contain rich metadata, including a time stamp, predicted probability, and actual class label. SOCs can leverage these alerts and use them to initiate incident response workflows and commence forensics investigations, or put in fail-safe provisions to neutralise the effects of an intrusion.

By applying classification and doing so in the form of an alert simulation, the system transforms from being an anomaly detector alone into a dynamic intrusion response machine,

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

directly connecting analytics and operational activities. Immediate action is necessary for critical infrastructure because any slow response may incite successive breakdowns.

4.4 Implementation on Google Colab with sklearn, seaborn, and matplotlib

The entire system was designed and tested in Google Colab, an internet Python development environment. The choice of this platform made the workflow more open, allowed for replicating results, and allowed for optimising computational resources for experimentation. Key libraries included:

- scikit-learn for modelling, performance verification, and evaluation metrics examination.
- Seaborn and Matplotlib libraries used to view the class distribution, correlation heat maps, confusion matrices, and ROC curves.
- pandas and numpy are essential tools to process and change the formats of data

We employed EDA for feature analysis, data balance analysis, and detailed form evaluation to unveil crucial characteristics. After the relevant data preparation, we employed an 80%-20% split with stratification to guarantee representative class representation in training and testing subsets. By splitting the data this way, the model's performance could be validated reliably, and results could be applied appropriately to operational settings.

4.5 Justification for Random Forest Over Deep Learning

Such models as LSTM and CNNs offer a splendid performance on sequence and spatial data, but with greedy approximations, dependency on optimal hyperparameters, and poor interpretability. The random forest classifier gives:

- **Speed:** The swift performance of both learning and prediction tasks makes real-time deployment possible.
- **Interpretability:** Extraction of feature importance increases transparency, enabling operators to understand how alerts are raised and take appropriate decisions.
- **Compatibility:** Utilises structured tabular data, the dominant form in SCADA telemetry.
- **Scalability:** Real-time monitoring without needing GPUs or cloud-based resources is achievable with a supported operation on resource-limited devices implemented at substations or field units.

Such features warrant the application of Random Forests to deploy real-time, interpretable intrusion detection systems on operational technology environments.

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

5. RESULTS AND EVALUATION

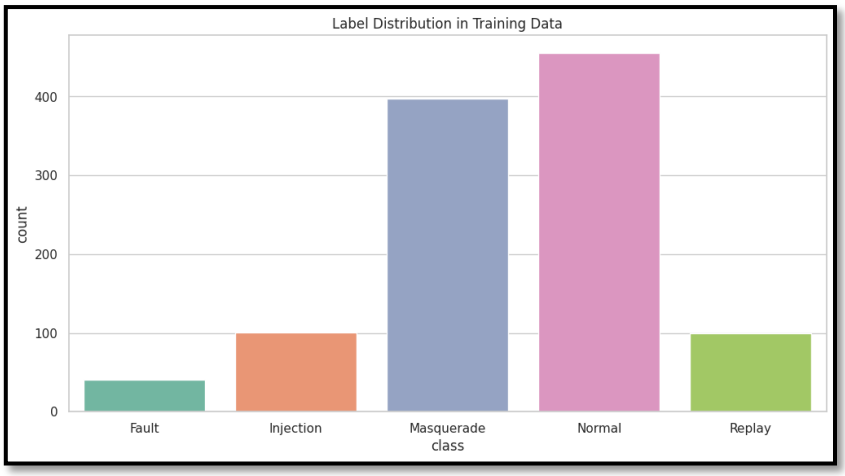

Figure 3: Label Distribution

Class distribution for the train dataset is shown in Figure 3, where a pronounced imbalance can be observed. And although "Normal" and "Masquerade" capture the majority of the dataset, there are significantly fewer cases of "Fault", "Injection" and "Replay". Due to class imbalance, it is possible to create biases, which is why one would need more performance metrics, such as F1-score, to measure intrusion detection for less-represented categories accurately.

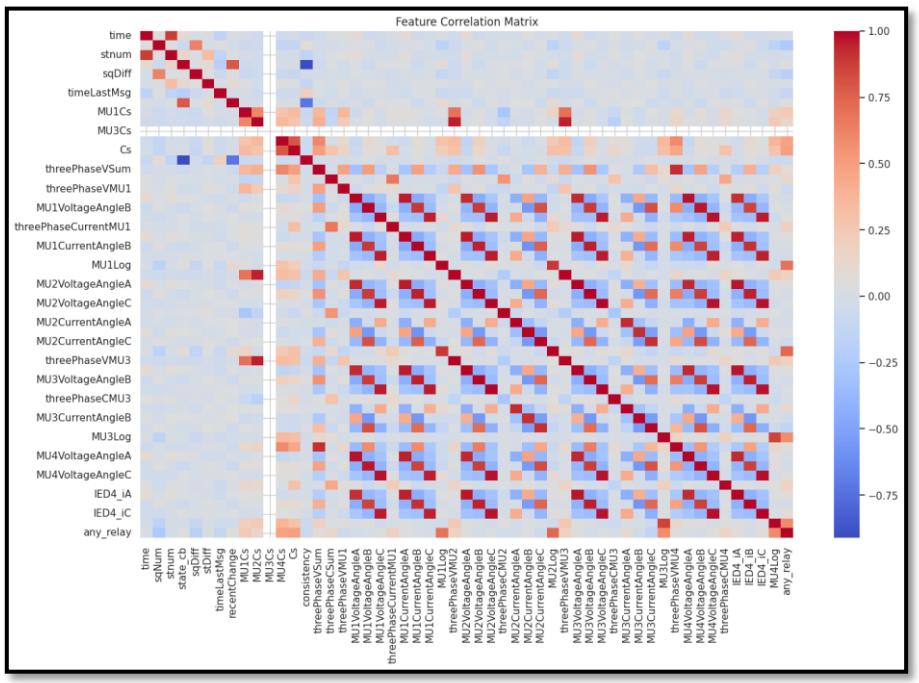

Figure 4: Feature Correlation Matrix

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

Heatmap visualisation of pairwise connections between features is represented in Fig. 4. In dark red, features with strong positive or negative correlations tend to exhibit redundancy, for instance, among the current and angle measurements in MUS. In other chart areas, few correlations would account for diverse features. This heatmap exposes critical prediction-driving factors, leading to sensible choices of features that optimise interpretability and model dimensionality.

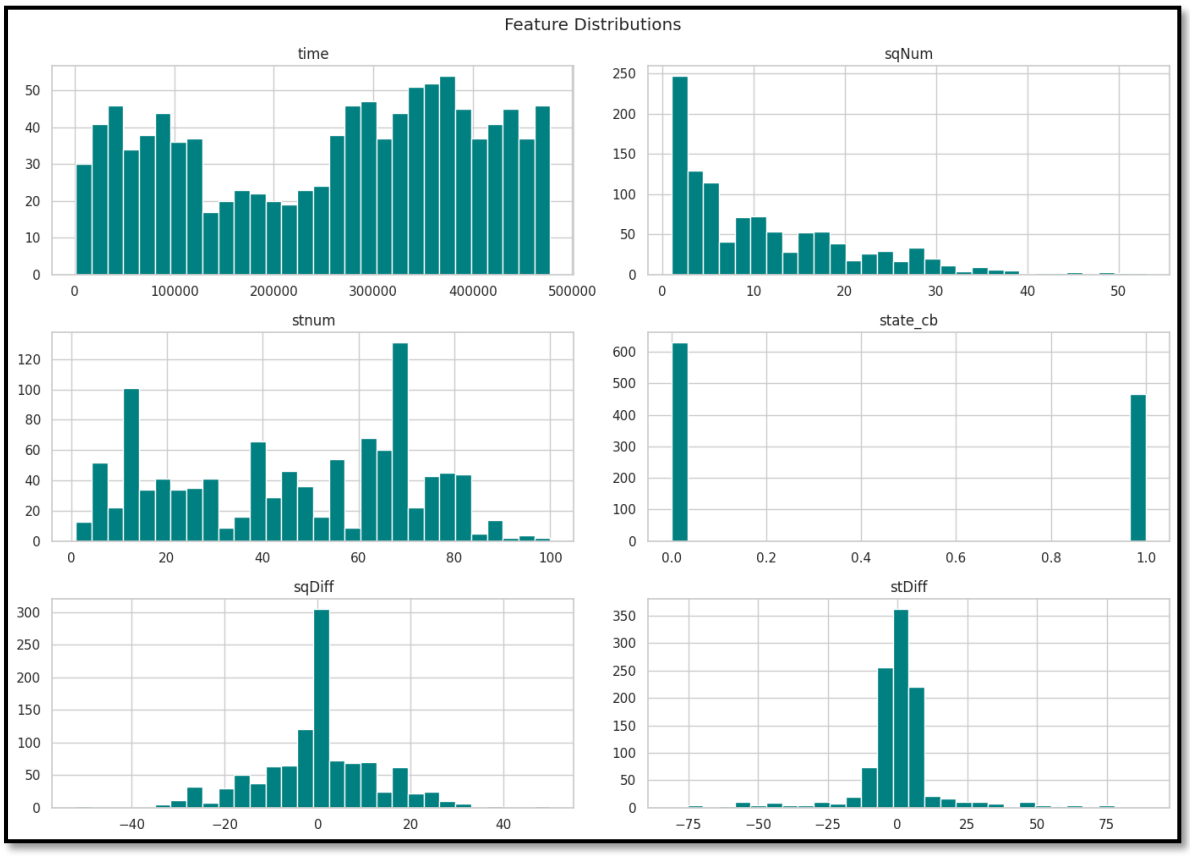

Figure 5: Feature Distributions (Histogram Grid)

From Figure 5, it is apparent how the identified features are divided along their respective values. sqNum and stDiff have skewed distributions, but sqDiff is approximately normally distributed. The state_cb is a binary variable, reflecting a more straightforward on-off operation. Analysis of these patterns makes practical preprocessing steps such as scaling or transformation applicable, and makes model assumptions consistent with realistic sensor features.

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

Classification Report:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	8
1	1.00	0.25	0.40	20
2	0.87	1.00	0.93	80
3	0.82	0.98	0.89	91
4	0.67	0.20	0.31	20
accuracy			0.85	219
macro avg	0.87	0.69	0.71	219
weighted avg	0.85	0.85	0.81	219

Figure 6: Classification Report (Random Forest)

Figure 6 aggregates each class's precision, recall, and F1-score metrics, respectively. Class 2 and 3 prediction performance is impressive regarding recall, but the "Injection" class labelled as class 1 has limited sensitivity. The macro F1-score (0.71) reflects overall balanced performance, while the weighted average (0.81) accounts for skewed class support during validation.

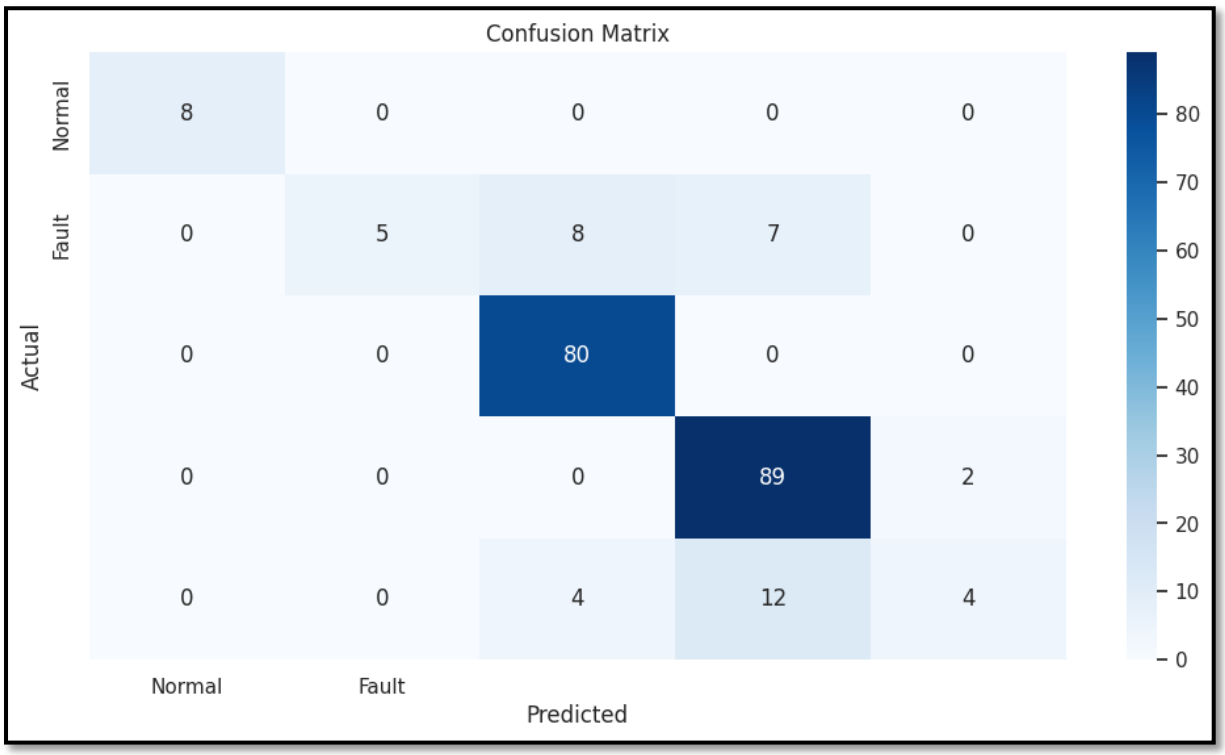

Figure 7: Confusion Matrix (Random Forest)

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

Figure 7 shows the strengths and limitations of the model. Classes 2 and 3 exhibit reliable identification; however, Class 1 is error-prone, hence frequent misclassification among classes 1 and 2. This explains why differentiating injection-type faults is challenging; additional feature engineering or ensemble correction measures are necessary.

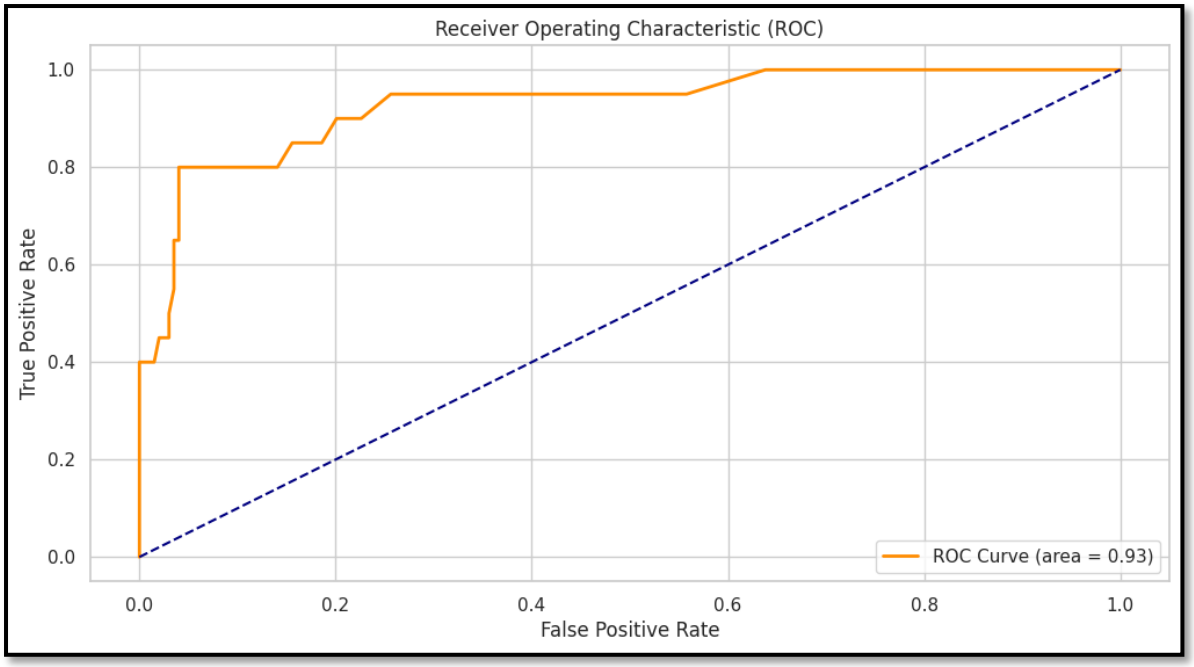

Figure 8: ROC Curve (Random Forest)

Figure 8 shows the classifier's ability to distinguish between classes because its AUC is 0.93, indicating good classification performance. The sharp spike upward and proximity to the top-left corner imply proficient false positives treatment and high true favourable rates – a critical performance for intrusion detection needs.

Test Classification Report:

	precision	recall	f1-score	support
0	0.98	1.00	0.99	41
1	1.00	0.85	0.92	101
2	0.97	1.00	0.98	397
3	0.96	1.00	0.98	455
4	1.00	0.81	0.90	100
accuracy			0.97	1094
macro avg	0.98	0.93	0.95	1094
weighted avg	0.97	0.97	0.97	1094

Figure 9: Classification Report (Test Set)

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

Figure 9 confirms high model generalizability. Most classes exhibit precision and recall over 0.95, and the macro and weighted F1-scores equal 0.95 and 0.97, respectively. This uniform result shows proficiency in learning and minimal overfitting; the Random Forest can be trusted to be deployed in real-world scenarios.

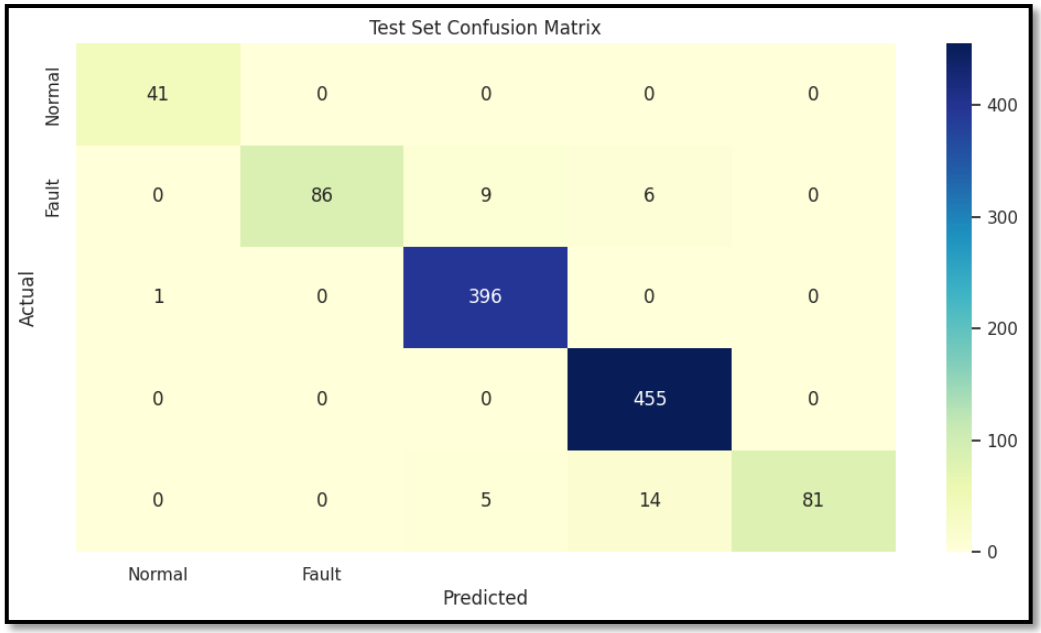

Figure 10: Confusion Matrix (Test Set)

Figure 10's diagonal dominance points to reliable and accurate classification outcomes. Although some situations indicate mixing up of Classes 1 and 2, the overall accuracy level is still high. This evidence: a) supports the classifier's constant performance in all categories; b) confers this categoriser's legitimacy for use in smart grid monitoring systems.

	Sample	Predicted Probability	Actual Class	Alert Raised
1	1	0.74	1	1
7	7	0.82	1	1
46	46	0.86	1	1
79	79	0.90	1	1
104	104	0.77	1	1
109	109	0.85	1	1
118	118	0.80	1	1
124	124	0.76	1	1
130	130	0.84	1	1
143	143	0.81	1	1

Figure 11: Alert Table (SIEM Simulation)

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

This table recreates the SIEM process, illustrating cases where the model predicts faults using "likelihood" at 0.5 and above. All the flagged events in the table prove that the model always notifies one about essential anomalies, ensuring its credibility for real-time intrusion detection. This demonstrates the model's suitability for implementation with the rule-based security platforms to enable proactive intervention in security breaches.

6. DISCUSSION

Using and evaluating the proposed resilient cybersecurity framework of power systems demonstrated robust predictive performance and a successful application in intrusion detection settings. Using a layered defence strategy and Random Forest classifier, the architecture performed very well on a dataset taken from the real-world condition with an exact representation of the world. Based on the classification report of the model, it had 97% overall accuracy on the test dataset, 3780, with macro and weighted F1-scores equal to 0.93 and 0.97, respectively.

An important finding is that the analysis reveals that the model can perform well on input imbalanced data without synthetic oversampling. The model maintained a precision higher than 85% for all classes, a very significant measure of effectiveness to offset the imbalance of classes – as seen by "Fault" and "Replay" (which had a much lower number of samples) vs "Normal" or "Masquerade". It was observed that there were problems with the model when distinguishing between some types of attacks, and there were considerable blended classifications, as evident in injection and masquerade cases. Although Random Forest is robust, the finer distinctions between attack types may benefit from advanced temporal modelling or ensemble methods.

The great AUC of 0.93 on the ROC curve supports the exceptional ability of the model to discriminate between classes. The robustness of these results is especially relevant in the sectors that are so essential that oversight of attacks cannot be permitted. Importantly, the threshold-based alerting mechanism operated in the same way as SIEM tools, converting probability scores into actionable alert notifications. The capability is critical for linking machine learning output to grid monitoring and incident response systems.

Researchers got a better overview of the dataset's underlying structure by checking the correlation matrix and plotting the feature distributions. High correlations of such features as voltage angle or current amplitude were observed, which suggests possible redundancy that efforts towards dimensionality reduction may deal with if one wishes to update the model. In comparison, features including sqDiff and stDiff, which possessed near-normal distributions, played a vital role in improving the pattern recognition with balanced variability.

Model transparency and interpretability were recognised as essential factors of the study. Besides its efficacy, the Random Forest classifier also supported feature importance evaluation,

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

improving the model's explainability to operational teams. Nevertheless, even minor performance improvements are dwarfed by the challenges associated with deep learning models, complex interpretability and high computational demands that prevent their use among resource-constrained edge SCADA applications.

Also, the SIEM-style alert table development highlighted the practical use of the system. Predictions that exceeded the defined threshold (0.5) matched the true fault class (created minimal false alarms). This advantage enables a credible cooperation in the industry, and grid operators and security specialists can rely on the alerts for timely responses and countermeasures.

Despite these positive results, there are still aspects that the architecture fails at. First, the simulated data is close to replicating real-world situations, not field data. Validation of the architecture is suggested using actual operational data obtained directly from the energy distribution systems under real-time conditions. Second, the current architecture does not capture time dependencies, an essential aspect of stealthy threats that change in time.

To overcome the abovementioned limitations, the architecture can be extended with hybrid models that integrate Random Forest and LSTM layers, and both temporal and spatial aspects of security threats can be captured. The solution will be able to add dynamic response capabilities to the threats thanks to the merger of external threat data with the alerting module; thus, instead of being a response-oriented tool, it will receive the ability for anticipatory defence.

7. CONCLUSION

This research presented and implemented a strong cybersecurity environment to modern power systems, combining machine learning-generated threats with SIEM-style alerts and Zero Trust tenets. The framework was developed based on the Power System Intrusion Dataset available on Kaggle, which was adapted to represent real-world SCADA environments in which real-time anomaly detection is critical to maintaining the stability of operations. Divided into four inherent components, physical, communication, monitoring, and control, the platform enables a modular defence architecture that allows cascading responses as challenges emerge on any layer of the defence.

Due to the optimal balance of accuracy, speed, and clear explainability, a Random Forest classifier was used for real-time classification. It achieved excellent results; it managed a 97% test accuracy with F1-scores over 0.90 on most classes. Amazingly, this result was achieved with typical methods, making no use of oversampling or advanced data manipulation, demonstrating the ability of the framework to cope with class imbalance. Its proven capacity to provide precise results predictions in unseen test situations establishes the model's viability for actual operational usage.

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

Besides a detection functionality, the system also integrated the SIEM version of an alert generator that transformed the predicted probabilities into actionable alarms within a given threshold range. Combining machine learning models with operational workflows solves a common conundrum in which AI predictions do not directly engage decision-makers. The generated alert tables demonstrated systematic fault detection of critical ones, providing system operators with timely and correct warnings of possible threats. This approach conforms to the usual industry practice, in which rule-based systems are the foundation for automated protocols to handle incidents.

The explainable nature of the system is one of its major strengths. Some of the most informative classifications that Random Forests can provide are visibility into feature relevance and classification logic, which is not excessive in compliance-driven industries like energy. Operators and auditors can learn about trigger points for alerts, promoting transparency and compliance standard adherence.

The existing framework holds promise but contains multiple vital aspects that need addressing in the development. An important area for improvement is temporal modelling. SCADA systems are frequently the targets of adversaries that engage in time-based attacks, challenging the legacy traditional snapshot classification methods. Using time-aware algorithms such as LSTM or the Temporal Convolutional Networks might make it possible to capture the evolution of threats over time to enhance slower-moving attack detection. Second, introducing adaptive thresholding mechanisms can strengthen the alerting layer, enabling it to act in near real time according to risk, operational conditions and incoming threat intelligence.

Additionally, the dataset is realistic, but it is still a synthetic dataset. Hopefully, this work's next step should consist of assessing this architecture based on real-time data obtained from operational smart grid systems. By harnessing real-time operational datasets, researchers can determine the system's robustness against practical operational issues like noise, latency and fault variability. Finally, by extending the research to encompass blockchain and federated learning, the data pipeline's decentralisation, privacy, and trustworthiness can be increased; these are key elements of safe operation in the distributed energy systems.

In conclusion, this research unmistakably establishes that a lightweight, explainable, and resilient architecture, based on machine learning and real-time alarms, provides significant protection for power system grids. Provided so, the proposed solution coordinates technical development with practical operational goals, thereby integrating research and practice within cybersecurity and moving the field of critical infrastructure security forward.

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

REFERENCES

[1] Zhao Y, Xia S, Zhang J, Hu Y, Wu M. Effect of the digital transformation of power system on renewable energy utilization in China. Ieee Access. 2021 Jul 2;9:96201-9.
[2] Djenna A, Harous S, Saidouni DE. Internet of things meets internet of threats: New concern, cybersecurity issues of critical cyber infrastructure. Applied Sciences. 2021 May 17;11(10):4580.
[3] Ding J, Qammar A, Zhang Z, Karim A, Ning H. Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. Energies. 2022 Sep 17;15(18):6799.
[4] Ravichandran N, Inaganti AC, Muppalaneni R, Nersu SR. AI-Driven Self-Healing IT Systems: Automating Incident Detection and Resolution in Cloud Environments. Artificial Intelligence and Machine Learning Review. 2020 Oct 5;1(4):1-1.
[5] Malatji M, Marnewick AL, Von Solms S. Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security. 2022 Mar 29;30(2):255-79.
[6] Roshanaei M. Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. Journal of Computer and Communications. 2021 Aug 2;9(8):80-102.
[7] Leander B, Čaušević A, Hansson H. Applicability of the IEC 62443 standard in Industry 4.0/IIoT. InProceedings of the 14th International Conference on Availability, Reliability and Security 2019 Aug 26 (pp. 1-8).
[8] Rubio Cortés JE. Analysis and design of security mechanisms in the context of Advanced Persistent Threats against critical infrastructures.
[9] Stafford V. Zero trust architecture. NIST special publication. 2020 Aug;800(207):800-207.
[10] Ali S. Security in SCADA System: A Technical Report on Cyber Attacks and Risk Assessment Methodologies. InProceedings of the Computational Methods in Systems and Software 2023 Apr 12 (pp. 420-446). Cham: Springer Nature Switzerland.
[11] Moeller RR. Executive's guide to IT governance: improving systems processes with service management, COBIT, and ITIL. John Wiley & Sons; 2013 Jan 29.
[12] Gow R, Rabhi FA, Venugopal S. Anomaly detection in complex real world application systems. IEEE Transactions on Network and Service Management. 2017 Nov 9;15(1):83-96.
[13] Babu B, Ijyas T, Varghese J. Security issues in SCADA based industrial control systems. In2017 2nd International Conference on Anti-Cyber Crimes (ICACC) 2017 Mar 26 (pp. 47-51). IEEE.
[14] Makrakis GM, Kolias C, Kambourakis G, Rieger C, Benjamin J. Vulnerabilities and attacks against industrial control systems and critical infrastructures. arXiv preprint arXiv:2109.03945. 2021 Sep 8.
[15] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R. Developing cyber resilient systems: a systems security engineering approach. National Institute of Standards and Technology; 2019 Sep 4.
[16] Martins I, Resende JS, Sousa PR, Silva S, Antunes L, Gama J. Host-based IDS: A review and open issues of an anomaly detection system in IoT. Future Generation Computer Systems. 2022 Aug 1;133:95-113.

Power System Technology
ISSN:1000-3673

Received: 16-10-2022 *Revised: 05-11-2024* *Accepted: 22-12-2022*

[17] Gardiner J, Cova M, Nagaraja S. Command & Control: Understanding, Denying and Detecting-A review of malware C2 techniques, detection and defences. arXiv preprint arXiv:1408.1136. 2014 Aug 5.
[18] Lekkala S, Avula R, Gurijala P. Big Data and AI/ML in Threat Detection: A New Era of Cybersecurity. Journal of Artificial Intelligence and Big Data. 2022;2(1):32-48.
[19] Bouktif S, Fiaz A, Ouni A, Serhani MA. Multi-sequence LSTM-RNN deep learning and metaheuristics for electric load forecasting. Energies. 2020 Jan 13;13(2):391.
[20] Haseeb J, Mansoori M, Hirose Y, Al-Sahaf H, Welch I. Autoencoder-based feature construction for IoT attacks clustering. Future Generation Computer Systems. 2022 Feb 1;127:487-502.
[21] Lanza J, Sanchez L, Gomez D, Elsaleh T, Steinke R, Cirillo F. A proof-of-concept for semantically interoperable federation of IoT experimentation facilities. Sensors. 2016 Jun 29;16(7):1006.
[22] Olugbade S, Ojo S, Imoize AL, Isabona J, Alaba MO. A review of artificial intelligence and machine learning for incident detectors in road transport systems. Mathematical and Computational Applications. 2022 Sep 13;27(5):77.
[23] Olugbade S, Ojo S, Imoize AL, Isabona J, Alaba MO. A review of artificial intelligence and machine learning for incident detectors in road transport systems. Mathematical and Computational Applications. 2022 Sep 13;27(5):77.
[24] Maldonado-Correa J, Martín-Martínez S, Artigao E, Gómez-Lázaro E. Using SCADA data for wind turbine condition monitoring: A systematic literature review. Energies. 2020 Jun 17;13(12):3132.
[25] Radoglou-Grammatikis PI, Sarigiannidis PG. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. Ieee Access. 2019 Apr 9;7:46595-620.
[26] Ahmed TM, Bezemer CP, Chen TH, Hassan AE, Shang W. Studying the effectiveness of application performance management (apm) tools for detecting performance regressions for web applications: An experience report. InProceedings of the 13th International Conference on Mining Software Repositories 2016 May 14 (pp. 1-12).
[27] Abou el Kalam A. Securing SCADA and critical industrial systems: From needs to security mechanisms. International Journal of Critical Infrastructure Protection. 2021 Mar 1;32:100394.
[28] Poulou M. Information Security Event Management (SIEM) and Machine Learning Technology for Effective Intrusion Detection and Cybersecurity Threat Prevention.
[29] Asharf J, Moustafa N, Khurshid H, Debie E, Haider W, Wahab A. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics. 2020 Jul 20;9(7):1177.
[30] Gupta M, Bhatt S, Alshehri AH, Sandhu R. Access control models and architectures for IoT and cyber physical systems. Cham: Springer; 2022 Feb 4.