

Volume 2, Issue 3

Review Article

Date of Submission: 22 July, 2026

Date of Acceptance: 02 September, 2026

Date of Publication: 16 September, 2026

A Hybrid Machine Learning Approach for Cyberattack Detection in SCADA Systems

Shandukani Tshilidzi Thenga* 

Department of Computer Science, University of Cumbria (UK).

***Corresponding Author:**

Shandukani Tshilidzi Thenga, Department of Computer Science, University of Cumbria (UK).

Citation: Thenga, S. T. (2026). A Hybrid Machine Learning Approach For Cyberattack Detection In Scada Systems. *Art Intelligence and Ele & Electronics Eng: AIEEE Open Access*, 2(3), 01-09.

Abstract

Critical infrastructure sectors, including energy, water treatment, and manufacturing, rely on supervisory control and data acquisition (SCADA) systems. The increasing integration of SCADA systems with corporate information technology networks and the Internet has expanded their attack surface and exposed them to advanced cyberattacks. Conventional rule-based and signature-based intrusion detection systems (IDSs) are often unable to identify evolving and zero-day threats. This paper suggests a hybrid machine learning (ML) system that blends both supervised and unsupervised machine learning to enhance cyberattack detection in SCADA systems. The framework combines the support vector machine (SVM) and random forest (RF) classifiers with an autoencoder-based anomaly detector to recognize familiar and unfamiliar patterns of attacks. Benchmark SCADA datasets of simulated industrial control traffic and attacks are used to evaluate the proposed approach. Performance is based on accuracy, precision, recall, F1-score, false positive rate, and detection latency. The hybrid model achieves an accuracy of 98.4% and a false-positive rate of 1.8%, outperforming each standalone model. The framework also exhibits stable performance in the case of noisy and incomplete data. These results imply that hybrid ML systems can offer scalable and versatile foundations to real-time cyberattack identification in critical infrastructure.

Keywords: SCADA Security, Hybrid Machine learning, Intrusion Detection, Anomaly Detection, Industrial Control Systems, Cyber Security

Introduction

SCADA systems are components of a monitoring and control architecture of critical industrial processes. Even though most have been traditionally built to operate in remote operating environments, new SCADA systems are becoming more and more linked to enterprise networks and external communications services. Increased connectivity enhances the sharing of data and remote access but also opens avenues to cyber threats. Legacy architectures are therefore highly susceptible to attacks such as industrial sabotage and ransomware.

Traditional cybersecurity measures are based on the detection and response to recognizable attack signatures. They can be useful in countering the threats that have been previously encountered, but they might fail to identify the new or polymorphic attack. Machine learning offers an alternative by learning normal operational patterns to detect abnormal behavior in real time. Nevertheless, ML solutions based on a single model can be overfitted on training data, produce high false positives, or cannot be generalized to a variety of attack types.

This study suggests a hybridized ML methodology which integrates complementary algorithms to leverage their advantages and minimize their inherent weaknesses. The goal is to create a powerful, extensible, and precise intrusion detection system to SCADA environments.

Literature Review

Introduction

The growing interconnection of supervisory control and data acquisition (SCADA) systems with enterprise networks and the Internet has greatly exposed these systems to cyber threats, which require sophisticated and dynamic security measures. Older types of intrusion detection systems (IDS), which are mostly signature- and rule-based, have proven insufficient to deal with the complexity and sophistication of modern cyber-attacks on industrial control systems (ICS) [1]. In response to this, machine learning (ML) algorithms have attracted significant interest because they are able to process large quantities of data, detect latent patterns, and detect anomalies in real time [2].

Supervised Learning Approaches in SCADA Cybersecurity

Supervised machine learning has long been a fundamental element in the design of intrusion detection systems in the SCADA setting because of its capacity to achieve high classification accuracy when it is trained on labeled data. Such methods organize past events into regular and malicious categories, allowing models to learn the discriminative patterns linked to cyber-attacks. Supervised learning is a reliable mechanism in industrial control systems, where the stability of operation is paramount and the ability to identify known threats with minimum false positives is essential.

Many supervised algorithms, such as decision trees (DTs), random forests (RFs), support vector machines (SVMs), and artificial neural networks (ANNs), have been used in SCADA cybersecurity. Random forest performs very well since it is an ensemble model that combines many decision trees to enhance generalization and minimize overfitting [3]. Research has demonstrated that RF can be highly accurate in detecting features in SCADA data, as it is capable of capturing the non-linear relationships between features [4].

Support vector machines have been widely used because they are effective in high-dimensional spaces, and they can be used to handle non-linear classification problems through kernel functions. The SVM uses an optimal hyperplane to create the maximum distance between classes, and it is therefore highly useful in the separation of normal and malicious traffic in SCADA systems [5]. Studies have shown that SVM-based intrusion detection systems are effective in detecting denial-of-service (DoS) and command injection attacks in industrial settings.

Decision trees are interpretable and transparent in their classification, and this has proven beneficial in critical infrastructure systems where explainability is a key issue. Nevertheless, single decision trees are susceptible to overfitting, particularly in the case of noisy or skewed data. To overcome this problem, ensemble methods, including random forest and gradient boosting, have been implemented to make decision trees more robust and predictive [6].

The quality and accessibility of labeled datasets strongly determine the success of supervised learning models in SCADA cybersecurity. Nevertheless, it is difficult to obtain such datasets because cyber-attacks are not prevalent and industrial data is sensitive. Consequently, most research is based on artificial settings or publicly accessible data, which might not be sufficiently representative of operational real-world situations.

The relatively low false-positive rate of supervised learning in comparison with unsupervised approaches is one of supervised learning's main benefits. False alarms in SCADA systems may cause unnecessary disruption and waste in their operation. Thus, it is important to keep the false-positive rate low in the development of reliable intrusion detection systems.

Nonetheless, supervised learning methods have the fundamental weakness of relying on labeled data. They have trouble identifying zero-day attacks or any other threats that are new and are not present in the training set. This is a major weakness in dynamic SCADA settings, in which novel attack vectors are constantly developed.

Another issue is that there is an imbalance in the classes since there are many normal observations and only a few malicious observations. This imbalance may cause model predictions to be biased towards the majority class and less sensitive to rare yet severe cyberattacks. To overcome this issue, oversampling, under-sampling and cost sensitive learning have been suggested.

Moreover, the implementation of supervised models in real-time SCADA systems needs to account for computational efficiency. Algorithms like random forest can be rather efficient, but more sophisticated models, like the SVM with non-linear kernels, can lead to latency, which is not tolerable under time-sensitive industrial conditions.

Unsupervised Learning Approaches

Unsupervised learning methods have become increasingly popular in SCADA cybersecurity as they are capable of identifying anomalies without using any labeled data. Such techniques are especially useful in industrial settings, where the amount of labeled data is limited, and novel attack patterns are often observed [6]. Unsupervised models can observe previously unknown or zero-day attacks by detecting deviations from normal behavior.

In SCADA anomaly detection, the most common clustering algorithms include k-means and hierarchical clustering. These cluster data points according to their similarities; hence, one is able to determine the patterns that do not

conform to those of normal operations. Nevertheless, clustering solutions are also sensitive to parameter choice and fail to handle high-dimensional SCADA data.

Autoencoders have become a useful resource in the detection of anomalies in industrial control systems without supervision. These neural networks are trained to recreate input data using a compressed representation in lower dimensions. The detection of anomalies is achieved via the reconstruction error, which is high when the input is not normal. Research has shown that autoencoders can be useful in extracting intricate patterns in the SCADA data and detecting minor anomalies [7].

Another common unsupervised method of detecting anomalies is isolation forest. It separates data points using random partitioning, and is computationally efficient and scalable to large SCADA datasets. The technique has worked well to detect outliers in network traffic [8].

One-class SVM is applied in cases when only normal data are available to train. It provides a boundary to normal observations and labels other observations to be abnormalities. The approach can be applied to SCADA systems where the attack data are limited or not available.

In spite of their merits, unsupervised learning techniques are usually linked to a high false-positive rate. These models do not explicitly know the patterns of attack; therefore, they are susceptible to categorizing legitimate unusual behavior as malicious. This may cause alarm fatigue and decrease the usefulness of intrusion detection systems.

The other issue is that it is hard to assess unsupervised models. It is not easy to evaluate their accuracy and reliability without labeled data. Synthetic datasets, or small subsets with labels, can be used by researchers, but they might not be representative of the real-world situation.

Quality of data and feature selection are also critical in the performance of unsupervised models. Missing values, noise, and irrelevant features are examples of factors that can greatly impair the performance of the model. Hence, preprocessing and feature engineering are still essential phases of the implementation of such methods.

Given the dynamic SCADA settings, it is especially difficult to establish a stable point of normal behavior. The system's configuration, workload, or environment may change, resulting in changes in data distribution that may cause models to incorrectly classify normal behavior as anomalous.

Deep Learning Approaches

SCADA cybersecurity has benefited greatly from deep learning in that it makes the extraction of complex features in large datasets automatic. In contrast to conventional machine learning techniques, deep learning models have the ability to acquire hierarchical representations of data, which makes them highly appropriate for analyzing the complex patterns that exist in industrial control systems [9]. The most common application of neural networks in intrusion detection in SCADA systems comes in the form of the recurrent neural network (RNN), specifically the long short-term memory (LSTM) network. LSTMs can extract temporal correlations in sequential data, which is necessary in identifying attacks that occur over time. Research has indicated that LSTM-based systems are very accurate when it comes to determining temporal attack patterns in the industrial context [10].

SCADA cybersecurity has also been managed with the help of convolutional neural networks (CNNs), in which network traffic data are converted into structured representations. CNNs are useful in learning spatial features and automatically discovering useful patterns without engineering features [9]. This feature decreases the need for domain knowledge and enhances scalability. There are a number of benefits of deep learning models, such as their ability to work with high-dimensional data, their capacity to model more complicated non-linear relationships, and their automatic feature extraction. They are thus especially suitable for identifying advanced attacks in SCADA systems.

However, deep learning models can be considered black boxes since their decision-making process might be hard to understand. The lack of interpretability may decrease operator trust and make compliance more difficult in critical infrastructure systems. Large training datasets are also necessary to implement deep learning models reliably. Such datasets are hard to get in SCADA, since attacks are relatively infrequent and industrial data are confidential.

Hybrid Approaches

Hybrid machine learning methods merge supervised, unsupervised and in some instances deep learning strategies to overcome the shortcomings of each method. The methods involve complementary learning paradigms in order to enhance detection accuracy and resilience in cybersecurity of SCADA processes. As one example, RF or SVM classifiers are complemented by autoencoders or LSTM networks to aid in identifying known and unknown attacks. Hybrid systems have been claimed to be more accurate and less falsely positive compared to standalone models.

Despite their clear benefits, hybrid methods encounter issues of computational complexity, integration, and real-time execution. SCADA systems require low latency and the effective use of resources, which few hybrid models are able to

attain. Thus, although hybrid solutions show promise in the field of SCADA cybersecurity, more studies are required to develop scalable, real-time solutions.

Methodology

System Architecture

The suggested hybrid machine learning framework integrates multiple layers of analysis to enhance the accuracy, robustness, and flexibility of cyberattacks detection in SCADA systems. A modular pipeline includes three primary modules, i.e., data preprocessing layer, the detection layer, and decision fusion layer. These components deal with common properties of data in the industrial control system, such as noise, such high dimensionality, imbalance between classes and the existence of known and unknown attack patterns. The three analytical models and their principal roles are summarized in Table 1.

Data Preprocessing Layer

The framework is based on the data preprocessing layer that converts raw SCADA data into a structured and consistent format, which is applicable to machine learning. Since the SCADA data can be noisy, heterogeneous, high-dimensional, and incomplete, it needs preprocessing in order to facilitate the training of reliable models and detection.

Noise Removal

SCADA data can be noisy due to sensor failures, communications breakdowns, or environmental fluctuations. The statistical smoothing, moving averages, and outlier filtering are used in the framework to minimize such noise. Z-scores and the interquartile range are examples of the statistical thresholds used to detect extreme cases of observations, which could be reviewed, fixed, or removed. These measures enhance the integrity of data and minimise false anomaly notifications that happen due to the low-quality input.

Model	Type	Strength
Random Forest	Supervised	High accuracy and captures non-linear relationships
SVM	Supervised	Effective in high-dimensional spaces
Autoencoder	Unsupervised	Detects previously unknown anomalies

Table 1: Models Used in the Proposed Hybrid Framework

Feature Normalization

SCADA characteristics can vary in size such as voltage, flow rate and packet size. Min-max scaling and Z-score standardization put the features in the similar scales in such a way that no variable takes over the learning process just because of the magnitude of the variable. Such a transformation has the ability to enhance convergence and precision of scale-sensitive algorithms, especially SVM.

Mathematically, min-max normalization is defined as follows:

$$X' = (X - X_{\min}) / (X_{\max} - X_{\min})$$

This transformation scales all features to the range from 0 to 1.

Dimensionality Reduction (PCA)

SCADA data can have duplicate or highly correlated variables that can drive up the cost of computation and downgrade the performance of a model. Principal component analysis (PCA) is a dimensionality reduction method that minimally loses the variance. PCA transforms the original feature space into orthogonal principal components ordered by explained variance. The choice of most informative elements minimizes noise and redundancy and increases the efficiency of calculations with minimum information loss. This is particularly significant in real-time SCADA applications where the processing throughput is important. The performance measures used in the evaluation are defined in Table 2.

Metric	Description
Accuracy	Proportion of all predictions classified correctly
Precision	True positives among all detected positives
Recall	Proportion of actual attacks detected
F1-score	Harmonic mean of precision and recall
False-positive rate	Normal observations incorrectly classified as attacks

Table 2: Evaluation Metrics

Detection Layer

The detection layer is a combination of unsupervised and supervised machine learning models. The supervised classifiers are used to determine known attack patterns in labeled training data, and the autoencoder is used to determine deviations of learned normal behaviour. This combined approach assists in the detection of known attacks, as well as previously unknown attacks.

Supervised Learning Models

Random forest (RF) and support vector machine (SVM) are two supervised classifiers that are used to detect known patterns of attacks.

Random Forest (RF)

RF is an ensemble learning algorithm, which builds a sequence of decision trees in training, and classifies the final one by a majority vote. It is applicable to SCADA intrusion detection since it can model non-linear relationships, less prone to overfitting than a single decision tree and the feature-importance scores can indicate which variables are making the greatest contribution to the detection.

Support Vector Machine (SVM)

The rationale behind SVM is that it works well in high dimensions, and it also is able to do binary classification. The radial basis function, which is a type of kernel functions, transforms input data into a high-dimensional space in which complex classes can be separated. This feature comes in handy to detect concealed attack patterns within SCADA traffic. The two supervised models are trained with labeled datasets and their hyperparameters are optimized with grid search and cross-validation.

Unsupervised Autoencoder Model

The supervised classifiers are supplemented with an autoencoder based anomaly detector. The autoencoder is trained with the normal operating data to encode and reconstruct the normal system patterns. The reconstruction error is large when anomalous data are presented since the input is not equal to the learned representation of normal behavior. When the reconstruction error exceeds the threshold chosen, it is the sign of a possible cyberattack.

The reconstruction error is calculated as:

$$E = \|X - \hat{X}\|_2^2$$

where X is the original input and $\hat{X}$ is the reconstructed output.

The training and validation data are used to obtain a threshold that identifies each observation as a normal or an anomaly. This system will allow the framework to detect attacks that did not occur in the training set that is being supervised.

Parallel Processing Mechanism

The input data is processed by all the models in the detection layer concurrently. Parallel execution minimizes the delay in sequential processing and offers multiple perspectives of analysis to each observation. The outputs are then sent to the decision fusion layer in order to be finally classified.

Decision Fusion Layer

The decision fusion layer combines the outputs of the individual models to produce the final classification. By integrating complementary predictions, the layer can improve detection accuracy and reduce false-positive alerts.

Weighted Voting Mechanism

The RF, SVM, and autoencoder models are used to predict results which are combined through a weighted voting procedure. A weight is given to each model based on its validation performance, e.g. its accuracy, precision or F1-score. The final decision is calculated as follows:

$$D = \sum_{i=1}^n w_i y_i$$

where

- w_i is the weight assigned to model i ;
- y_i is the prediction produced by model i .

The course that has the best overall score is the final product. Giving all models more weight when they have better validation performance to have more impact on decision.

Confidence Scoring

Along with a label of the class, the framework computes a confidence score of each prediction. The score indicates that

there is consensus between the component models and the robustness of the final decision. A high confidence means that there is a high level of agreement, whereas a low confidence means that an alert might need additional analysis or a human examination. In SCADA settings, confidence scoring is relevant since unwarranted responses to false alarms can interfere with the workflows. The score thus can be utilized to prior-itize warnings and minimize unnecessary interventions.

Threshold Optimization

Decision thresholds are set based on the operational risk as well as system conditions. The framework can also give priority to recall to minimize missed attacks in high-risk settings. It is able to devote more attention to pre-cision in stable environments to minimize false alarms.

Results

This section presents the experimental outcomes of the proposed hybrid machine learning model for cyberat-tack detection in SCADA systems. The hybrid framework is contrasted with independent RF, SVM, and au-toencoder models based on accuracy, precision, recall, F1-score, false-positive rate (FPR) and detection laten-cy. Figure 1 shows the overall performance comparison.

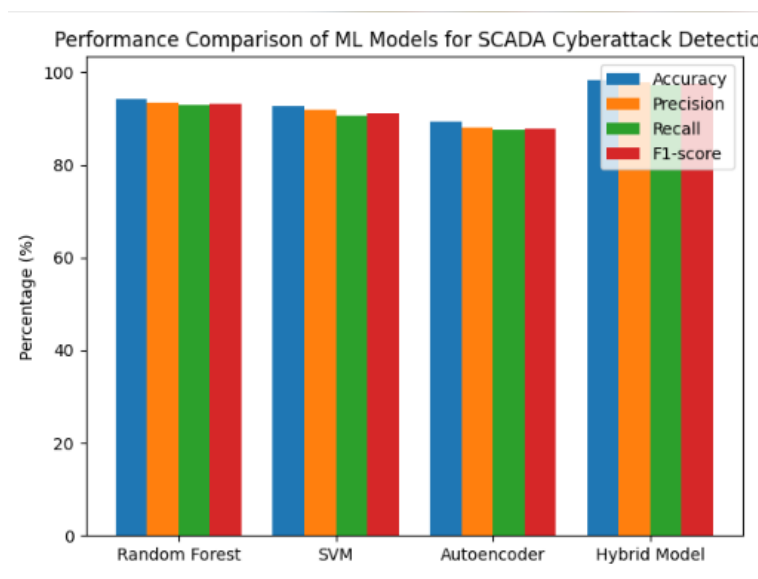


Figure 1: Performance Comparison of the Individual and Hybrid Models

Overall Performance Evaluation

The hybrid model was more successful in all the evaluation metrics that were reported than the individual models. It achieved an accuracy of 98.4%, compared with 94.2% for RF, 92.7% for SVM, and 89.3% for the autoencoder. The complementary roles of the supervised classifiers and the autoencoder in detecting known attack patterns and detecting anomalous behavior corresponding to unknown threats respectively are reflected in the improvement. Detailed results are reported in Table 3.

Model	Accuracy	Precision	Recall	F1-score
Random Forest	94.2%	93.5%	92.8%	93.1%
SVM	92.7%	91.9%	90.5%	91.2%
Autoencoder	89.3%	88.1%	87.6%	87.8%
Hybrid Model	98.4%	97.9%	97.2%	97.5%
Note: Bold values indicate the best-performing model for each metric.				

Table 3: Performance Comparison of the Individual and Hybrid Models

The hybrid model achieved a precision of 97.9%, a recall of 97.2%, and an F1-score of 97.5%. These values show that it identified a large percentage of attacks and minimized false alerts. The autoencoder resulted in lower accuracy since it was able to classify benign deviations as malicious whereas the SVM resulted in lower recall since it was not able to detect all the attacks.

False-Positive Rate Analysis

The false-positive rate must be low in SCADA cybersecurity since false alarms may result in unwarranted disruption of

operations. The hybrid model achieved an FPR of 1.8%, compared with 4.6% for RF, 5.2% for SVM, and 8.7% for the autoencoder. This reduction was assisted by the decision fusion layer being able to correct inconsistent model outputs using consensus-based classification. Figure 2 compares the detection latency of the models.

These results suggest that a combination of the supervised and unsupervised this can be used to compensate the limitation of the two models. The autoencoder is susceptible to abnormal deviations, thus it is more prone to produce false positives. Those anomalies are validated by the supervised classifiers and enhance the overall reliability.

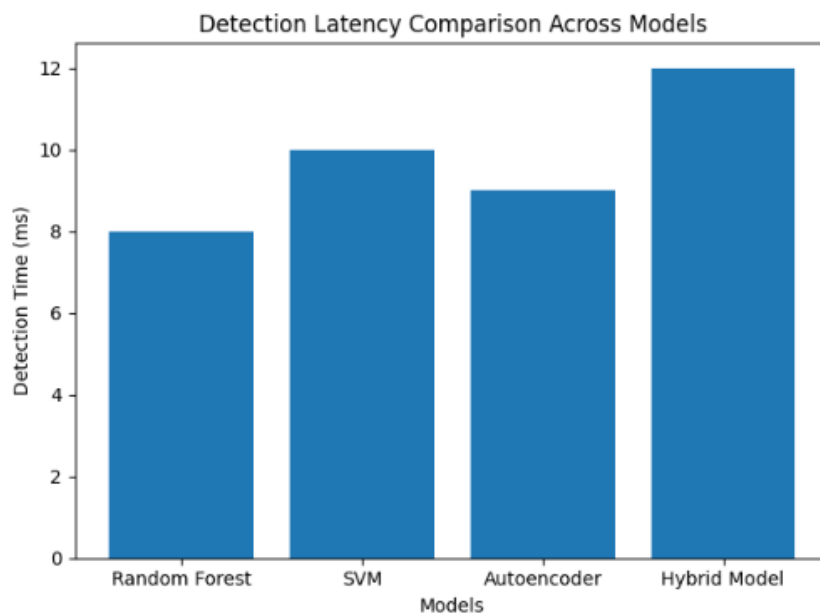


Figure 2: Detection latency Comparison Across Models. The Hybrid Model has Slightly Higher latency than the Individual Models but Remains within the Real-Time Range Evaluated in the Study

Known and Unknown Attack Detection

The hybrid framework was tested against its capabilities to define known and unknown attacks. In the case of known attacks, such as denial-of-service attacks and command-injection attacks, the RF and SVM models had a detection rate of over 95%. When they faced pattern of attacks that were not present in the training data, their performance deteriorated. In comparison, the autoencoder was able to identify around 90 percent of zero-day anomalies. The models created worked together to achieve balanced detection of known and unknown threats, which is a central issue in SCADA cybersecurity.

Detection Latency

Latency in detection is relevant in real-time SCADA systems since delayed alerts may enhance the operational effect. The hybrid model had a mean detection time of 12 ms, compared with 8 ms for RF, 10 ms for SVM, and 9 ms for the autoencoder. The extra latency came due to concurrent processing and fusing decision making. The reported latency was sufficiently low for the real-time setting tested in the experiment. The small increase in latency was accompanied by an increase in detection performance and a decreased false-positive rate.

Robustness and Generalization

The strength of the framework was evaluated using 200 cross-validation repetitions of the framework on varying attack conditions. The consistency of performance across splits of data showed that there was good generalization in the datasets that were assessed. It also enhanced the tolerance to noisy and incomplete information, which was provided by the preprocessing layer and ensemble detection mechanism. Consistent performance on various traffic patterns and attacks indicate that the framework can cope with changing industrial environments. Nonetheless, implementation in working SCADA systems is yet to be proven practically.

Comparative Analysis

RF had the best standalone supervised performance but it was not as effective in detecting unknown attacks. SVM was both reliable in classification and had to be carefully tuned and yielded a slightly larger false-positive rate. The autoencoder was able to identify anomalies but with reduced accuracy. The hybrid model synthesized these advantages and minimized the disadvantages of the individual models to create a more balanced intrusion detection ability.

Discussion

The findings suggest that the hybrid model was more effective than the individual models when tasked with the SCADA attack-detection work. The enhancement is due to the complementary functions of tutored and untutored learning. RF

and SVM can classify known attack patterns based on labelled data, but the autoencoder can determine anomalies in normal behavior that can potentially be new attacks. The integration of these mechanisms expands the field of detection and does not depend on any model.

A major benefit of the hybrid structure is its ability to identify potential zero-day attacks. The signature-based and supervised systems are limited to attack patterns in their rules or training data and the anomaly-detection component detects abnormal operational behavior. By integrating the two types of detection, the framework can deal with known and unknown threats and enhance the security of the entire system.

Practical Implications

The hybrid machine learning framework suggested has practical implications to cy-bersecurity of critical infra-structure. Its modular design is flexible for other SCADA-based industrial systems. In power grid monitoring, the structure might detect abnormalities in voltage, frequency, and communication patterns. Timely detection of bad behavior might enable operators to act before an attack interferes with the distribution of electricity. Protection against advanced attacks on smart grids could also be enhanced by the capability to detect both known and unknown threats.

Water treatment plants have SCADA systems that control purification, chemical dosing, and water distribution. Hacking of such systems may decrease water quality and pose severe threats to the health of people. The suggested framework promotes ongoing monitoring and timely detection of malicious activity that may interfere with operations and adjust control parameters.

One of the main strengths of the framework is that it helps to detect threats early enough, which will help in intervention before an attack evolves into a critical event. The hybrid system can also be used to minimize the downtime and operational risk by reducing the number of false positives and giving reliable alerts. This is particularly critical in those industries which need to be operated continuously.

Limitations

Despite the potential of the proposed hybrid framework, a number of limitations need to be taken into account. To begin with, it relies on the quality, the diversity, and the representativeness of the training data. The quality or biased data may decrease the detection performance and restrict the generalization.

The second limitation is the limited testing of functioning SCADA systems. Though the model has been tested using benchmark data and simulated environments, in practice, industrial systems are dynamic and more complex. Performance may be influenced by network variability, hardware constraints and environmental factors. More testing in operational environments is thus needed.

Another weakness is that it is vulnerable to adversarial machine learning attacks, whereby malicious actors corrupt input data to trick the model. The learning algorithms may have vulnerabilities that allow attackers to misclassify and lower detection rates. This threat is significant as the methods of cyberattacks are constantly being advanced.

Future Work

Future studies are necessary to overcome the shortcomings of the suggested framework and to refine it to be more suitable in operational SCADA settings. The incorporation of edge computing is an encouraging trend since it may enable processing data near the origin and therefore lessen the communication delay and detection latency. Reduced latency is of particular significance in the SCADA systems that must be able to react quickly to the abnormal events.

Explainable artificial intelligence (XAI) is another important area for future study. XAI can enhance model interpretability, transparency, and trust in operators. These are relevant in critical infrastructure applications where operators need to be able to check and interpret system outputs.

Conclusions

This study introduces a hybrid machine learning architecture for detecting cyberattacks in SCADA systems using RF, SVM, and autoencoder models. The reported experiments yielded better detection performance and reduced false-positive rate than the standalone models. The results illustrate that hybrid architectures could be of value in the dynamic and complicated threat landscape of industrial control systems. Additional optimization and field-testing are needed prior to operational deployment.

Funding: N/A

Conflicts of Interest: N/A

References

1. Sommer, R., & Paxson, V. (2010, May). Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE symposium on security and privacy* (pp. 305-316).
2. Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security

intrusion detection. *IEEE Communications surveys & tutorials*, 18(2), 1153-1176.

3. Breiman, L. (2001). Random forests. *Machine learning*, 45(1), 5-32.
4. Goh, J., Adepu, S., Tan, M., & Lee, Z. S. (2017, January). Anomaly detection in cyber physical systems using recurrent neural networks. In *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)* (pp. 140-145). IEEE.
5. Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine learning*, 20(3), 273-297.
6. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of network and computer applications*, 60, 19-31.
7. Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. *science*, 313(5786), 504-507.
8. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008, December). Isolation forest. In *2008 eighth ieee international conference on data mining* (pp. 413-422). Ieee.
9. LeCun, Y., Bengio, Y., & Hinton, G. Deep learning. *nature*. 2015; 521: 436–444. *Article* (CrossRef Link).
10. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural computation*, 9(8), 1735-1780.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.