engineering proceedings

MDPI

Proceeding Paper

Improving Industrial Control System Cybersecurity with Time-Series Prediction Models †

Velizar Varbanov * and Tatiana Atanasova

Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Acad. G. Bonchev Str., Bl.2, 1113 Sofia, Bulgaria; tatiana.atanasova@iict.bas.bg

* Correspondence: velizar.varbanov@iict.bas.bg

† Presented at the 11th International Conference on Time Series and Forecasting, Canaria, Spain, 16–18 July 2025.

Abstract

Traditional security detection methods struggle to identify zero-day attacks in Industrial Control Systems (ICSs), particularly within critical infrastructures (CIs) integrated with the Industrial Internet of Things (IIoT). These attacks exploit unknown vulnerabilities, leveraging the complexity of physical and digital system interconnections, making them difficult to detect. The integration of legacy ICS networks with modern computing and networking technologies has expanded the attack surface, increasing susceptibility to cyber threats. Anomaly detection systems play a crucial role in safeguarding these infrastructures by identifying deviations from normal operations. This study investigates the effectiveness of deep learning-based anomaly detection models in revealing operational anomalies that could indicate potential cyber-attacks. We implemented and evaluated a hybrid deep learning architecture combining Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to analyze ICS telemetry data. The CNN-LSTM model excels in identifying time-dependent anomalies and enables near real-time detection of cyber-attacks, significantly improving security monitoring capabilities for IIoT-integrated critical infrastructures.

Keywords: Industrial Control Systems (ICSs); time-series anomaly detection; deep learning; cybersecurity; Convolutional Neural Networks (CNNs); Long Short-Term Memory (LSTM)

check for updates

Academic Editors: Olga Valenzuela, Fernando Rojas, Luis Javier Herrera, Hector Pomares and Ignacio Rojas

Published: 22 July 2025

Citation: Varbanov, V.; Atanasova, T. Improving Industrial Control System Cybersecurity with Time-Series Prediction Models. *Eng. Proc.* **2025**, *101*, 4. https://doi.org/10.3390/engproc2025101004

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The cybersecurity of critical infrastructures (CIs) is a national security concern due to their essential role in economic stability and public safety according to the European Union Agency for Cybersecurity (ENISA) [1]. The exponential growth of cyber-attacks targeting these infrastructures [2] highlights the urgent need for innovative protection measures. Threat actors, whether politically or financially motivated, increasingly exploit zero-day vulnerabilities, making these attacks particularly difficult to detect and mitigate.

Traditional Intrusion Detection Systems (IDSs), such as signature-based and misuse-based approaches, rely on predefined attack signatures and known threat patterns. While effective for recognizing previously identified threats, these systems struggle against zero-day attacks that mimic normal operational behaviour or exploit unknown weaknesses. In contrast, anomaly detection methods offer a more robust solution by identifying deviations from normal system behaviour, thereby detecting previously unseen cyber threats. Moreover, security strategies designed for information technology (IT) environments may not fully meet the needs of Industrial Control Systems (ICSs). While IT security prioritizes

data confidentiality, ICS security emphasizes real-time availability and system integrity to ensure uninterrupted industrial operations. The growing convergence of IT and operational technology (OT) systems has further blurred the distinction between these domains, expanding the attack surface for cyber threats.

Over the past few decades, ICSs have evolved to integrate modern Industrial Internet of Things (IIoT) technologies, enhancing efficiency and operational control. However, this interconnectivity has also eliminated the effectiveness of traditional isolation-based security measures, exposing industrial environments to remote cyber threats. Adversaries targeting ICS systems can have physical consequences, such as manipulating actuators to disrupt production or cause equipment malfunctions, posing severe risks to infrastructure stability.

Currently, ICSs face significant threats from state-linked actors, which continue to prioritize operational technology (OT) as a critical target. Cyber–physical attack operations and preparations suggest that threat actors are increasingly adopting living-off-the-land (LotL) tactics, techniques, and procedures to exploit OT systems. These tactics leverage native tools and legitimate software within ICS environments to remain undetected.

Hacktivist groups have also increased their operational tempo, with a growing likelihood of state-sponsored threat actors co-opting or masquerading as hacktivists to conduct nuisance operations under the guise of plausible deniability. This shift further complicates attribution and response strategies. Collateral damage from ransomware attacks on information technology systems remains one of the most significant risks to operational availability. Developments in the cybercriminal ecosystem indicate a rising threat of extortion operations targeting OT systems, potentially causing widespread disruption. Given these evolving threats, there is an increasing demand for advanced cybersecurity solutions tailored to ICS environments.

Traditional security approaches often fail to address the unique challenges of ICS environments, necessitating advanced detection mechanisms such as machine learning-based [3,4] anomaly detection. This study explores the use of deep learning-based anomaly detection models to safeguard ICSs against cyber threats. Our approach leverages machine learning techniques to identify anomalies, ensuring the integrity and reliability of industrial processes.

This study focuses on anomaly detection in ICSs using the Secure Water Treatment (SWaT) dataset, a widely recognized benchmark dataset for ICS security research. We explore various deep learning techniques to detect cyber threats.

Following the introduction in Section 1, the rest of this paper is structured as follows: In Section 2, the related works are briefly discussed. Then, in Section 3, the Secure Water Treatment (SWaT) dataset is overviewed. The methodology of experiments is presented in Section 4, along with results, and Section 5 discusses the results obtained. Finally, in Section 6, the conclusions of this study are presented, and some directions for future research are proposed.

2. Related Work

Anomaly detection in ICSs has gained significant attention in recent years. A relevant study on ICS security was conducted in "A Dataset to Support Research in the Design of Secure Water Treatment Systems" by Goh et al. [5]. The research introduced the Secure Water Treatment (SWaT) testbed, a scaled-down version of a real-world industrial water treatment plant, where data was collected under both normal and attack conditions. The study emphasized the importance of datasets that include both network traffic and physical properties to design effective defence mechanisms against cyber–physical threats. Our work builds upon such datasets by incorporating advanced machine learning techniques to detect anomalies in ICS environments. Additionally, a study by Tameem

et al. [6] investigated ICS and SCADA threats using honeypot data analysis and Security Information and Event Management (SIEM) solutions. The research identified several types of attacks, including brute-force login attempts, reconnaissance activities, vulnerability scanning, and unauthorized access attempts targeting various industrial protocols. Our study complements this by analysing anomaly detection methods for similar attack types in ICS environments, with a focus on detecting deviations in operational data rather than analysing attack traffic collected from honeypots.

Further, research by Wang et al. [7] highlights the importance of cybersecurity awareness in ICS risk assessment. The study introduced a cybersecurity awareness framework based on the MP2DR2 risk control matrix, emphasizing how human factors and training influence security incident response. This aligns with our study's approach, as human error remains a critical factor in ICS cybersecurity. While our focus is on detecting anomalies in operational data, cybersecurity awareness training could complement our proposed anomaly detection models by reducing attack vectors caused by misconfigurations and insider threats.

A recent study by Mahmud et al. [8] proposed an Isolation Forest-based anomaly detection model for ICS security. The study demonstrated the effectiveness of Isolation Forest in mitigating cyber threats by identifying anomalous system behaviours without requiring labelled attack data. Our research expands on this approach by comparing the performance of Isolation Forest with other deep learning models, such as CNNs and LSTMs, to assess their relative advantages in detecting sophisticated attacks within ICS environments. Additionally, research by Pinto et al. [9] investigates the effectiveness of unsupervised anomaly detection models for ICSs, particularly in detecting operational anomalies that could indicate cyber-attacks. Their study evaluated Isolation Forest (IF), Local Outlier Factor (LOF), One-Class SVM (OCSVM), and Autoencoders, highlighting the VAE-LSTM model's capability to identify cyber-attacks within seconds in high-frequency datasets. This aligns with our study's approach, which incorporates deep learning-based anomaly detection techniques for ICS security. Our study further extends this work by evaluating hybrid supervised–unsupervised models to enhance anomaly detection accuracy while ensuring minimal false positives.

A study in [10] implemented a Lightweight Long Short-Term Memory Variational Autoencoder (LSTM-VAE) and reported detecting 82% of anomalies present in the SWaT dataset. The authors applied the Kolmogorov–Smirnov (K–S) test to compare the probability distributions of training and testing data, leading to the elimination of 15 features—AIT201, AIT202, AIT203, P201, AIT401, AIT402, AIT501, AIT502, AIT503, AIT504, FIT504, PIT501, PIT502, and PIT503—even though some of these were involved in attack scenarios, such as attack 38, which targeted AIT401 and AIT502. This suggests that the model could detect anomalies based on dependencies among other physical devices rather than direct manipulation of excluded features. Similarly, in [11], an LSTM neural network was employed, where 22 features representing sensors and actuators were removed due to zero variance, K–S test results exceeding 0.25, or inconsistencies in training and testing distributions. In that case, the model successfully detected 23 out of 28 cyber-attacks, excluding those that lacked physical impact or were ineffective. Additionally, the study incorporated a 120 s time window for feature extraction using Fourier Transformation, which resulted in attack detection occurring at least two minutes after the initial breach.

Another approach in [12] utilized an LSTM Autoencoder for anomaly detection in ICSs, integrating a statistical feature extraction method for both industrial network data and external network traffic. This method demonstrated promising results in attack detection by leveraging network activity patterns. However, the effectiveness of deep learning-based models heavily depends on the quality of extracted features from raw data.

3. Materials and Methods

3.1. The Secure Water Treatment (SWaT) Dataset

The Secure Water Treatment (SWaT) dataset is a publicly available benchmark dataset developed for cybersecurity research in industrial environments. It provides a realistic testbed for evaluating anomaly detection techniques in Industrial Control Systems (ICSs) by simulating normal operations and various cyber-attacks on a fully operational water treatment system. The dataset consists of 11 days of continuous operational data, including

- 7 days of normal operation;
- 4 days with simulated cyber-attacks.

The dataset includes sensor and actuator readings, covering different attack scenarios, network traffic, and physical process data. The attacks range from data injection to command manipulation and denial-of-service (DoS) attacks. This dataset is widely used in anomaly detection research, providing a controlled environment to evaluate machine learning models for cybersecurity in ICSs.

3.2. Attack Scenarios in SWaT Dataset

One of the notable attack scenarios in the dataset involves

- Spoofing sensor values (LIT301) to trigger an underflow condition.
- Attack duration: 07:13:27 to 07:17:47 (row 9598-9857).
- Normal operation used for model training: 04:33:27 to 06:48:27 (row 1-8097).

The attack forces the water treatment system into an undesirable operational state, potentially leading to equipment failure or service disruption. Since ICS systems operate under strict physical constraints, even minor sensor manipulations can have significant cascading effects on overall system integrity. The dataset allows researchers to evaluate anomaly detection models by analysing deviations in physical process data.

4. Methodology

4.1. Data Preparation for Machine Learning

Effective use of deep learning models requires robust data preprocessing steps:

1. Handling Missing Values: Any missing or infinite values in the dataset were removed to maintain data integrity.
2. Feature Selection: The dataset contains multiple sensor readings; for anomaly detection, key features such as LIT301, AIT301, and AIT302 were selected based on domain knowledge.
3. Normalization: All numerical features were standardized using mean (1) and standard deviation normalization to ensure uniform scaling across different measurements.

$$x' = \frac{x - \mu}{max(x) - min(x)} \quad (1)$$

4. Time-Series Windowing: A sliding time window approach was used to structure the data into sequences for model training, capturing short-term dependencies in ICS operations.
5. Data Splitting: The dataset was split into training (70%) and testing (30%) sets to evaluate model performance effectively.

4.2. Implementing Machine Learning Algorithms

This study employs a hybrid CNN-LSTM model to capture both spatial and temporal relationships in ICS data. The model structure includes the following:

- Convolutional Layer: Extracts key features from time-series input.
- MaxPooling Layer: Reduces dimensionality to focus on critical patterns (2).

$$F_{max(x)} = max\{x_i\}_{i=0}^{n} \quad (2)$$

- LSTM Layer: Captures sequential dependencies in sensor readings.
- Dense Output Layer: Produces anomaly predictions.

Model parameters were set as follows: batch size = 256, training epochs = 5, optimizer = Adam, loss function = Mean Squared Error (MSE) (3).

$$MSE = \Sigma(y_i - p_i)^2/n \quad (3)$$

where y_i is the i-th observed value, p_i is the corresponding predicted value for y_i, and n is the number of observations. The Σ indicates that a summation is performed over all values of i.

4.3. Model Architecture Summary

The CNN-LSTM model implemented in this study combines spatial feature extraction and temporal pattern recognition, making it well-suited for time-series anomaly detection in ICSs. The model architecture consists of four key layers, each serving a specific function in processing sensor data for anomaly detection. Table 1 summarizes the model's architecture. The Conv1D layer applies 1D convolutional filters to the time-series sensor data, allowing the model to learn local dependencies across sensor readings. This helps in recognizing subtle fluctuations in ICS signals, which are often indicative of anomalies.

Table 1. Model's architecture.

Layer Name	Type	Output Shape	Parameters
Conv1D	Convolutional Layer	(None, 720, 256)	4096
MaxPooling1D	Pooling Layer	(None, 180, 256)	0
LSTM	Recurrent Layer	(None, 64)	82,176
Dense	Fully Connected	(None, 72)	4680

To enhance computational efficiency, the MaxPooling1D layer reduces the size of the extracted feature maps. This downsampling process preserves important information while significantly lowering the computational complexity of the model.

The LSTM layer plays a crucial role in capturing temporal dependencies in the sensor data. Unlike traditional feedforward networks that treat each input independently, LSTM maintains historical context, enabling the model to detect anomalies that evolve over time rather than isolated spikes.

Finally, the Dense layer generates a 72-step forecast, predicting future sensor values based on learned patterns. This step is critical for anticipating anomalies before they impact ICS operations, allowing for early threat detection.

By combining a CNN for spatial feature extraction and LSTM for sequential pattern recognition, this architecture effectively identifies irregular patterns in time-series ICS data, making it well-suited for real-time anomaly detection in industrial environments.

4.4. Model Training

The model was trained using supervised learning, with normal operational data used as baseline sequences. Training was performed using the TensorFlow/Keras framework, leveraging GPU acceleration where available. The model learns the normal behaviour of ICS sensors and attempts to flag deviations.

4.5. Model Evaluation

To further validate the model's anomaly detection capability, predictions were visualized against actual sensor values over time. The evaluation involved analysing time-series sequences of sensor data, comparing predicted vs. actual values, and assessing the model's accuracy in forecasting sensor anomalies.

By iterating over validation data samples, predictions were generated and plotted against real ICS readings. This visualization technique helps in

- Assessing how well the model forecasts sensor behaviour over multiple time steps.
- Identifying whether the model can detect deviations corresponding to anomalous activity.
- Validating the model's real-time anomaly detection effectiveness.

Several tests were performed for different time intervals in the dataset with past_history = 720 and future_target = 72. The code iterates through three batches of validation data, where each batch contains a sequence of past sensor values, the true future values, and the model's predicted future values. The following Figures 1 and 2 illustrate the test results, highlighting the model's ability to predict.

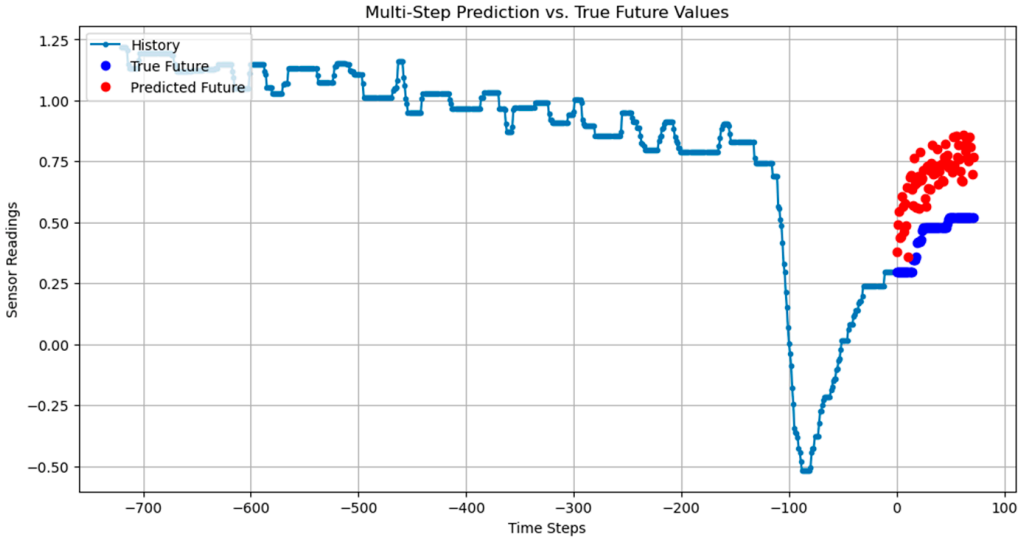


Figure 1. The multi-step plot visualizes the comparison, allowing an assessment of how accurately the CNN-LSTM model forecasts time-series sensor data and detects anomalies. Since the dataset uses time-series windowing, the duration of each batch depends on the configured time steps (history length of 720 and future target of 72), meaning each sequence represents 720 past time steps used to predict the next 72 time steps.

While Figures 1 and 2 show some differences between the true (blue) and predicted (red) values, particularly during abrupt changes, the model accurately follows the general trend. The transient discrepancies may result from sudden system dynamics that are harder to predict. Despite this, the model effectively identifies most anomalies.

To assess model performance, the following evaluation metrics were computed:

1. Accuracy: Measures the percentage of correct classifications.
2. Precision: Evaluates the proportion of true anomalies correctly classified.
3. Recall: Measures how many actual anomalies were identified.
4. F1-score: A balance between precision and recall, providing an overall performance measure.

The following results were obtained (Table 2).

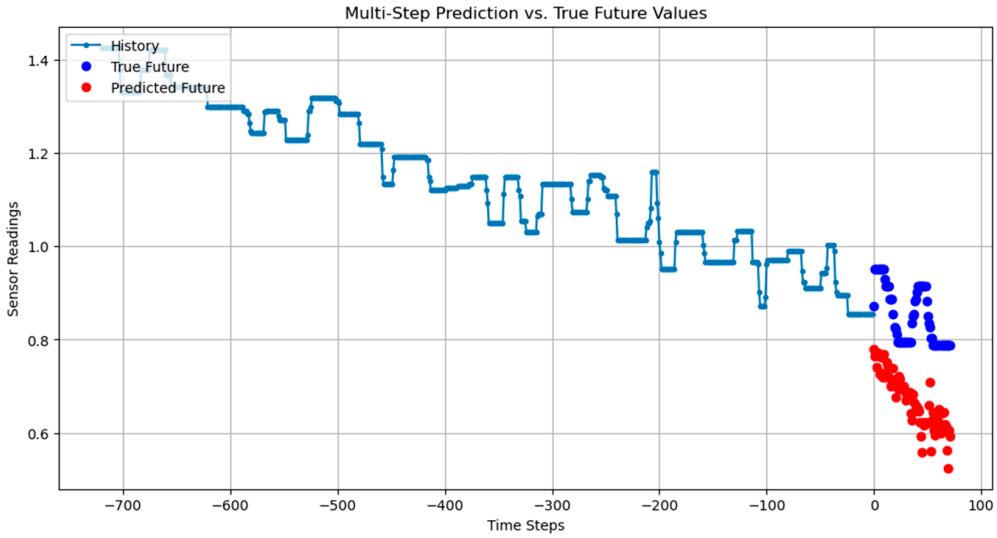


Figure 2. Predictions for different time intervals in the dataset.

Table 2. Prediction results using the CNN-LSTM model.

Metric	Score
Accuracy	0.9356
Precision	0.9389
Recall	0.9931
F1-score	0.9652

These metrics indicate that the model can effectively make predictions of abnormal time-series sensor data with high precision and recall, making it a viable tool for real-time ICS anomaly detection.

5. Discussion

The results of this study demonstrate the promising potential of machine learning for anomaly detection in ICS environments. However, the complexity of ICS data, particularly in IIoT-integrated systems, poses challenges in evaluating model performance due to the absence of labelled attack data. The evaluation process primarily relies on assessing the model's ability to capture anomalies based on deviations from expected system behaviour. Given that data distributions in CI environments are often non-normal, this adds complexity to anomaly detection, especially when analysing time-series sensor data.

The results demonstrate that the CNN-LSTM model effectively captures time-series anomalies, outperforming traditional detection methods in identifying deviations in ICS sensor data. However, while the model shows high precision and recall, the evolving nature of cyber threats necessitates human oversight to interpret complex anomalies and minimize false positives. The need for cybersecurity analysts remains critical, as automated systems alone may struggle with nuanced attack scenarios, persistent threats, and evolving adversarial techniques.

The importance of preserving temporal dependencies in ICS anomaly detection is evident in cases where sensor values evolve based on prior system states. For instance, the activation of an actuator at time t may depend on preceding sensor readings at $t - 1$, reinforcing the necessity of models that effectively capture these relationships. While anomaly detection models such as Local Outlier Factor (LOF) and Isolation Forest (IF) can manage non-normal data distributions, approaches like Vanilla Autoencoders and Variational Autoencoders (VAEs) may struggle to capture such temporal dependencies effectively. Our results confirm that deep learning models integrating LSTM

layers significantly enhance anomaly detection by accounting for sequential patterns in time-series data.

The process of evaluating anomalies must consider the limitations of predefined attack labels, which are often based solely on the start and end timestamps of known cyber incidents. Some attacks may begin without immediate operational impact, while others may have residual effects even after they cease. Refining anomaly detection models to adapt to delayed or persistent attack consequences will be crucial for improving cybersecurity defences.

Despite the model's high accuracy, precision, and recall, its effectiveness is limited when addressing complex and evolving cyber threats. The reliance on labelled normal operation data for training, challenges in detecting previously unseen attack types, and the need for low-latency performance in real-time environments highlight key limitations. To overcome these, future work will focus on integrating unsupervised learning techniques, collecting real-world attack data, and analysing multimodal sources such as network traffic and sensor data. Crucially, a human-in-the-loop approach is essential—cybersecurity professionals play a vital role in interpreting anomalies, reducing false positives, and refining detection strategies, ensuring robust and adaptive threat mitigation in industrial control systems.

Integrating network traffic data with sensor-based anomaly detection in future work could further enhance cybersecurity resilience in ICSs. While the CNN-LSTM model effectively identifies time-series anomalies, the evolving nature of cyber threats necessitates human oversight.

6. Conclusions and Future Work

This study highlights the potential of machine learning for ICS anomaly detection. This paper makes the following key contributions:

We propose a hybrid CNN-LSTM deep learning model tailored for ICS anomaly detection, capable of capturing both spatial and temporal dependencies in telemetry data.

Our model achieves a high detection performance (F1-score 96.52%) on the SWaT dataset, outperforming traditional models such as Isolation Forest and Local Outlier Factor (LOF).

We provide a comparative analysis of existing machine learning-based ICS detection models, highlighting the gaps such as lack of temporal modelling, and explain how our approach addresses these shortcomings.

We discuss the limitations and provide directions for integrating network traffic analysis and human-in-the-loop systems for enhanced threat detection.

While the results demonstrate the promise of this approach, relying solely on anomaly detection based on physical system data is not sufficient. To gain a more holistic view of security, it is crucial to incorporate network information. Future research will focus on

- Integrating network traffic data with physical system data to develop multimodal approaches capable of detecting anomalies from different sources.
- Implementing ICS honeypots to gather real-world attack data, enhancing the robustness of anomaly detection models.
- Improving real-time detection capabilities.
- Exploring hybrid models combining supervised and unsupervised learning.
- Testing on additional industrial datasets for validation.

By combining data from different sources, we aim to extract complementary features and capture intricate dependencies between modalities. Sensor data can highlight anomalies in physical operations, such as unauthorized access or tampering, whereas network traffic data can reveal digital threats like distributed denial-of-service (DDoS) attacks, malware communications, or data exfiltration attempts. This integration is critical as it

provides a comprehensive view of both physical and digital activities, greatly improving the detection of complex cyber threats that might not be identified if each type of data were examined separately.

Additionally, enhancing the model's ability to detect subtle anomalies is essential, as modern attack vectors are increasingly designed to mimic normal behaviour to evade detection. Future work will also focus on developing hybrid models that improve sensitivity to such sophisticated threats. By integrating machine learning techniques into ICS security frameworks, organizations can better protect critical infrastructure from emerging cyber threats.

Our approach differentiates itself by leveraging sensor and actuator data specific to cyber–physical systems (CPSs) rather than solely relying on network traffic. Additionally, we emphasize the importance of generalization by ensuring our model is robust across various attack types, addressing the challenge that models performing well on one dataset may not generalize effectively to others. Strengthening the model's adaptability is key to enhancing its applicability in real-world ICS environments.

Author Contributions: Conceptualization, V.V. and T.A.; methodology, V.V. and T.A.; software, V.V.; validation, V.V. and T.A.; resources, V.V.; writing—original draft preparation, V.V.; writing—review and editing, V.V. and T.A.; visualization, V.V.; supervision, T.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the National Science Fund of Bulgaria under contract No. КП-06-Н85/16.

Data Availability Statement: The Secure Water Treatment (SWaT) dataset used in this study is publicly available and can be found at: https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/ (accessed on 26 February 2025). No additional datasets were generated or analyzed during the current study.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. National Cyber Security Strategies. Available online: https://resilience.enisa.europa.eu/enisas-ncss-project/ (accessed on 26 February 2025).
2. Cybersecurity Incident Reporting and Analysis System (CIRAS). Available online: https://ciras.enisa.europa.eu/ (accessed on 26 February 2025).
3. Varbanov, V. Advancing Cyber Threat Intelligence through Machine Learning Algorithms. In Proceedings of the Cognitive Models and Artificial Intelligence Conference, İstanbul, Türkiye, 25–26 May 2024. [CrossRef]
4. Varbanov, V.; Atanasova, T. Leveraging Machine Learning for Threat Hunting in Network Security. In Proceedings of the 38th annual European Simulation and Modelling Conference (ESM'2024), EUROSIS-ETI, University of the Basque Country, San Sebastian, Spain, 23–25 October 2024.
5. Goh, J.; Adepu, S.; Junejo, K.N.; Mathur, A. A Dataset to Support Research in the Design of Secure Water Treatment Systems. In *Critical Information Infrastructures Security*; Havarneanu, G., Setola, R., Nassopoulos, H., Wolthusen, S., Eds.; CRITIS 2016; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10242. [CrossRef]
6. Tameem, U.Z.; Mahnoor, L.H.; Syed, M.A.U.H. Investigating Threats to ICS and SCADA Systems Via Honeypot Data Analysis and SIEM. *Int. J. Innov. Sci. Technol.* **2024**, *6*, 189–197.
7. Wang, K.; Guo, X.; Yang, D. Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks. *Electronics* **2022**, *11*, 1659. [CrossRef]
8. Mahmud, M.S.; Islam, M.A.; Rahman, M.M.; Chakraborty, D.; Kabir, S.; Shufian, A.; Sheikh, P.P. Enhancing Industrial Control System Security: An Isolation Forest-Based Anomaly Detection Model for Mitigating Cyber Threats. *J. Eng. Res. Rep.* **2024**, *26*, 161–173. [CrossRef]
9. Pinto, A.; Herrera, L.C.; Donoso, Y.; Gutierrez, J.A. Enhancing Critical Infrastructure Security: Unsupervised Learning Approaches for Anomaly Detection. *Int. J. Comput. Intell. Syst.* **2024**, *17*, 236. [CrossRef]
10. Fährmann, D.; Damer, N.; Kirchbuchner, F.; Kuijper, A. Lightweight Long Short-Term Memory Variational Auto-Encoder for Multivariate Time Series Anomaly Detection in Industrial Control Systems. *Sensors* **2022**, *22*, 2886. [CrossRef] [PubMed]

11. Umer, M.A.; Junejo, K.N.; Jilani, M.T.; Mathur, A.P. Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. *Int. J. Crit. Infrastruct. Protect.* **2022**, *38*, 100516. [CrossRef]
12. Khan, I.A.; Keshk, M.; Pi, D.; Khan, N.; Hussain, Y.; Soliman, H. Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems. *Ad. Hoc. Netw.* **2022**, *134*, 102930. [CrossRef]

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.