applied system innovation

MDPI

Article

Unsupervised Learning Approach for Anomaly Detection in Industrial Control Systems

Woo-Hyun Choi and Jongwon Kim *

AI Graduate School, Gwangju Institute of Science and Technology (GIST), Gwangju 61005, Republic of Korea
* Correspondence: jongwon@gist.ac.kr

Abstract: Industrial control systems (ICSs) play a crucial role in managing and monitoring critical processes across various industries, such as manufacturing, energy, and water treatment. The connection of equipment from various manufacturers, complex communication methods, and the need for the continuity of operations in a limited environment make it difficult to detect system anomalies. Traditional approaches that rely on supervised machine learning require time and expertise due to the need for labeled datasets. This study suggests an alternative approach to identifying anomalous behavior within ICSs by means of unsupervised machine learning. The approach employs unsupervised machine learning to identify anomalous behavior within ICSs. This study shows that unsupervised learning algorithms can effectively detect and classify anomalous behavior without the need for pre-labeled data using a composite autoencoder model. Based on a dataset that utilizes HIL-augmented ICSs (HAIs), this study shows that the model is capable of accurately identifying important data characteristics and detecting anomalous patterns related to both value and time. Intentional error data injection experiments could potentially be used to validate the model's robustness in real-time monitoring and industrial process performance optimization. As a result, this approach can improve system reliability and operational efficiency, which can establish a foundation for safe and sustainable ICS operations.

Keywords: industrial control system (ICS); unsupervised learning; SCADA; cyber-physical system; OT (operational technology)

Citation: Choi, W.-H.; Kim, J. Unsupervised Learning Approach for Anomaly Detection in Industrial Control Systems. *Appl. Syst. Innov.* **2024**, *7*, 18. https://doi.org/10.3390/asi7020018

Academic Editor: Felix J. Garcia Clemente

Received: 16 December 2023
Revised: 4 February 2024
Accepted: 15 February 2024
Published: 21 February 2024

1. Introduction

The ICS plays an important role in industrial processes across various sectors, including manufacturing, energy, water treatment, and transportation. It is a critical component of Operational Technology (OT) and works in conjunction with supervisory control and data acquisition (SCADA) systems to manage complex control operations [1–3]. These systems are designed to meet the unique needs of each industry and are highly adaptable. They come equipped with diverse Human–Machine Interfaces (HMIs) that enable operators to efficiently monitor and manage processes. In ICSs, network connectivity plays a critical role in enabling remote monitoring and control [4,5]. It is imperative to prioritize the enhancement in system security and reliability in ICS applications, given the growing number of cybersecurity threats [6].

Nevertheless, it is worth noting that incidents like the 2010 Stuxnet attack on Siemens PLCs at an Iranian nuclear facility have highlighted the potential vulnerabilities of ICSs to cyber threats [7,8]. The attack has brought attention to the need for improved ICS network security to prevent potential cyberattacks on critical infrastructure that could compromise physical systems. The 2015 cyberattack on Ukraine's power grid had a significant socioeconomic impact and severely disrupted the nation's power infrastructure. This incident highlights the importance of implementing robust ICS security measures [9,10]. These events highlight the importance of ICS security not only for IT, but also for national security and societal stability.

As recent cyberattacks have shown, securing ICSs is imperative. However, detecting anomalies in these systems poses several challenges. The ICS is characterized by the use of diverse equipment from multiple vendors, proprietary protocols, and complex communication methods that add to the complexity of securing these systems [11]. The continuous operation of these vital infrastructure management systems further limits access to real-world environments for security research. In addition, the application of security patches or updates to ICSs operating in environments such as production lines and energy infrastructures can be delayed, limiting their practical implementation [12]. Past cyberattacks, such as the Stuxnet event and the Ukrainian power grid attack, underscore the challenge of detecting system anomalies before they cause damage [13]. Anomaly detection in industrial control systems is a significant challenge due to the variety of devices from different vendors, each operating with proprietary protocols and complex communication methods [14]. It is critical to provide timely information to operators to prevent actual damage before it occurs. Our research focused on OPC servers to address these challenges.

Figure 1 shows the conceptual diagram between OT, ICSs, and SCADA. It also shows the OT portion of the Purdue model. The function of an OPC server is to process signals and data from field devices in a standardized manner and convert them into a format that clients can understand. This is accomplished by assigning a unique identifier, or tag, to each piece of data. Tags allow users to identify and retrieve data collected by the OPC server from field devices. These tags typically contain information about the device's location, data type, and value, and are organized in a way that is easy for humans to understand.

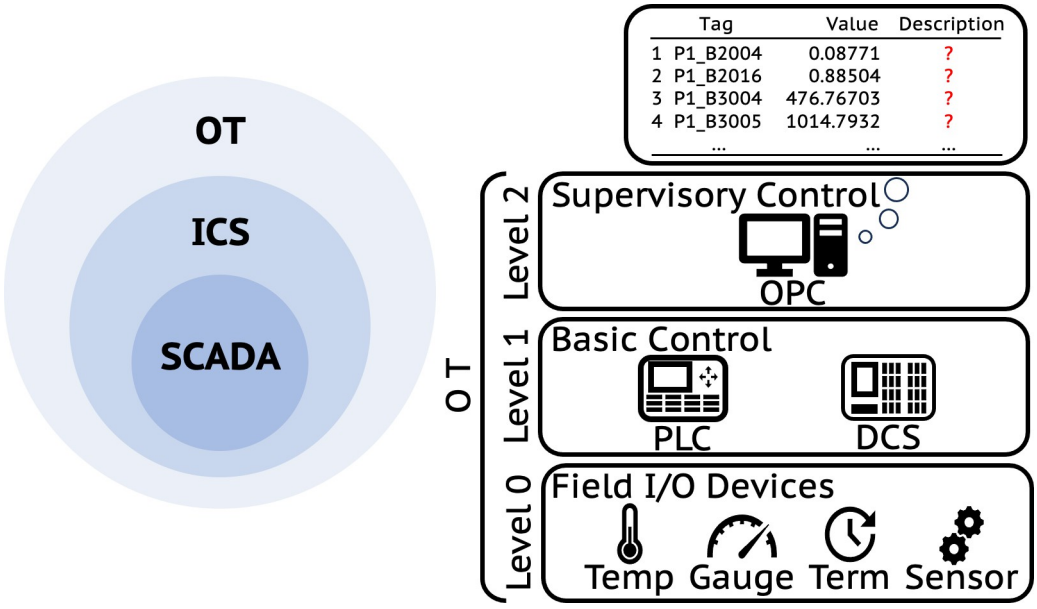

Figure 1. OT, ICS, SCADA concept map with OT part in the Purdue model.

However, in the domain of the ICS, the absence of descriptive annotations for tag values can significantly impede user interaction with the system, making configuration and management tasks more complex. This research aims to solve the problem of detecting anomalies within a complex system composed of different devices, each characterized by its own protocols and communication methods. This research focuses on the use of unsupervised learning techniques as a solution to this problem. Unsupervised learning can identify patterns and structures in data, allowing it to develop predictive models without pre-labeled datasets or extensive prior knowledge of the system's operating paradigm. These features are especially valuable in ICS environments, as they effectively detect emerging security threats that traditional data analytics frameworks may miss. The strategies include an analytical review of data attributes and patterns, the implementation of cluster-

ing techniques to aggregate tags with similar variations, and the incorporation of outlier detection mechanisms.

This study contributes to the field of ICS anomaly detection in the following ways:

- Heterogeneous system anomaly detection: First, we have developed a methodology that can identify anomalies with unique protocols or complex communication methods in systems composed of devices from different vendors. It is highly adaptable to different ICS environments because it does not rely on pre-labeled data or predefined descriptions.
- Leverage restricted network data: We leverage internal data from restricted networks, recognizing the sensitivity and security concerns within ICS networks. Our research focuses on developing techniques that utilize only the internal data accessible within restricted networks. This capability is essential for detecting system changes and anomalies using data that would otherwise be inaccessible for security analysis.
- Proactive anomaly response: Our research aims to facilitate the early detection of anomalous changes within the ICS, providing operators with timely information. This allows for quick and informed responses to potential problems before they can escalate into actual damage, strengthening the proactive defense mechanisms within industrial environments.

This paper is organized as follows. Section 2 reviews existing research on anomaly detection in industrial control systems. Section 3 describes the research methodology used in this study. Section 4 describes the experimental design and results. Section 5 concludes this study with a discussion.

2. Related Work

Anomaly detection has become an important area of research in many fields, including finance, healthcare, manufacturing, and cybersecurity [15]. The main objective of anomaly detection on multivariate time series is to quickly and accurately identify abnormal behavior of a system or process that may indicate a potential threat, failure, or error [16]. This plays an important role in maintaining the stability of the system and avoiding potential risks.

2.1. Anomaly Detection in Industrial Control Systems

Anomaly detection is an important research topic, especially in cybersecurity in the ICS. The ICS is intimately involved in our daily lives and cyberattacks on these systems can cause significant damage [17]. Therefore, technologies that can quickly detect anomalies in the ICS, and thereby prevent potential cyber-attacks, are crucial. AI technologies are becoming an important tool for this, with machine learning and deep learning techniques, in particular, showing promise in detecting anomalies. They can learn complex patterns in data and detect anomalies based on them. They are also effective at detecting anomalies in time series data, considering changes over time [18]. Inoue et al. [19] applied unsupervised machine learning techniques to detect anomalies in a water treatment system. Putchala et al. [20] proposed to apply a deep learning method using gated recurrent units (GRUs) to an intrusion detection system for IoT networks. The method showed a higher detection accuracy than traditional methods. They also proposed a lightweight and multi-layered design to enhance the security of IoT networks. Du et al. [21] proposed an unsupervised machine learning-based detection model based on LSTM-AE and GANs, which can learn complex patterns in time series data to detect anomalies more accurately. In addition, Goh et al. [22] introduced an unsupervised learning approach using RNNs to learn the changes in data patterns over time and use them to detect anomalies. In addition, Mokhtari et al. [23] used random forests to detect anomalous activity in industrial control systems. They showed that this method outperformed other classifier algorithms, which can significantly improve the detection of cyberattacks. Inoue, Putchala, Du, Goh et al. applied various algorithms for anomaly detection in water treatment, IoT networks, and time series data, and Mokhtari et al. utilized random forests to effectively detect anomalous activity in

industrial control systems. These techniques are proving to be highly effective in anomaly detection by learning complex data patterns and considering changes over time.

2.2. Recent Approaches to the Study of Anomaly Detection in Industrial Control System

Anomaly detection is emerging as a very important research topic, especially in industrial control systems. Industrial control systems play a pivotal role in many areas of production, energy management, traffic control, and more, and anomaly detection in these systems can significantly improve safety and efficiency. Recent studies, mentioned in Table 1, focus on improving intrusion detection and anomaly detection, specifically to address security and reliability issues in complex and diverse industrial environments such as ICS.

Table 1. Recent ICS research focused on improving intrusion detection.

Reference	Proposed	Method	Difference to Our Research
Catillo et al. [24]	CPS-GUARD	Based on a single semi-supervised autoencoder and outlier detection techniques	Focus on detection models based on Attack type
Liu et al. [25]	ST-GNN	Dynamic graph modeling approach based on prior knowledge	Focus on anomaly detection after filtering out data noise
Pang et al. [26]	VQ-OCSVM	Network intrusion detection based on hybrid algorithms	Focus on improving network intrusion detection rates
Wolsing et al. [27]	SIMPLE-IID	Intrusion detection based on four simple IIDs (min-max, gradient, steady-time, and histogram)	Focus on improving industrial intrusion detection rates
Park et al. [28]	XGBOOST	Based on alert aggregation intrusion detection system	Focuses on attack detection for this model of IDS by integrating many alerts
Kim et al. [29]	LSTM	Correlation-coefficient-clustering-based performance improvement techniques	Focus on improving detection rates in simulated environments
Xue et al. [30]	Deep SAD	A joint learning approach that integrates regularity representation learning and normalization from a small number of abnormal samples	Focus on improving intrusion detection performance
Gaggero et al. [31]	Neural Network AutoEncoder	Detects cyberattacks on battery electric storage systems (BESSs) in microgrid using neural network-based autoencoders.	Focus on outliers in electrical measurements

They study how to accurately detect anomalous activities or attacks in high-dimensional and complex industrial data using various techniques and methodologies such as graph neural networks, semi-supervised learning, clustering, and mixed algorithms.

However, this research is unique in two important ways.

1. Data-driven tag analysis: The model in this study analyzes operational data from industrial control systems to accurately identify tags of abnormal operation. To do so, we introduce a novel methodology to identify the misbehavior of a particular device by defining its rate of change. This technique enables us to successfully identify complex anomalies that are difficult to detect using traditional methods.
2. Informatization of cluster changes: This research identifies tagged clusters and communicates their changes to control network operators, enabling a rapid response. This process allows security professionals to identify relevant sensors and contribute to the creation of a stable and secure industrial control system environment.

As such, AI-based anomaly detection techniques play an important role in enhancing the security of industrial control systems. Each of these studies presents different methodologies and approaches, which provide a methodology for the more accurate detection of anomalies in different environments. In the future, these studies will continue to evolve and become more prominent as important research topics in cybersecurity.

3. Proposed Method

3.1. Overview of the Proposed Approach

Figure 2 provides an overview of the process proposed in our study. The process for anomaly detection using machine learning in industrial control systems is as follows: Data are collected from multiple sensors and systems in an ICS environment, with a special focus on the HAI (HIL-based augmented ICS) dataset [32] recorded for this purpose. The collected data are analyzed in detail to extract important characteristics and information. This includes dimensionality reduction using Principal Component Analysis (PCA) and data segmentation using K-means clustering. Next, a model is designed and trained using a neural network structure with input, hidden, and output layers. This allows the model to learn patterns from the data. Finally, the model's performance is evaluated on a separate dataset to validate its ability to accurately detect anomalies. When anomalies are detected, the tag name, detection time, and tag value of the anomalous behavior are displayed.

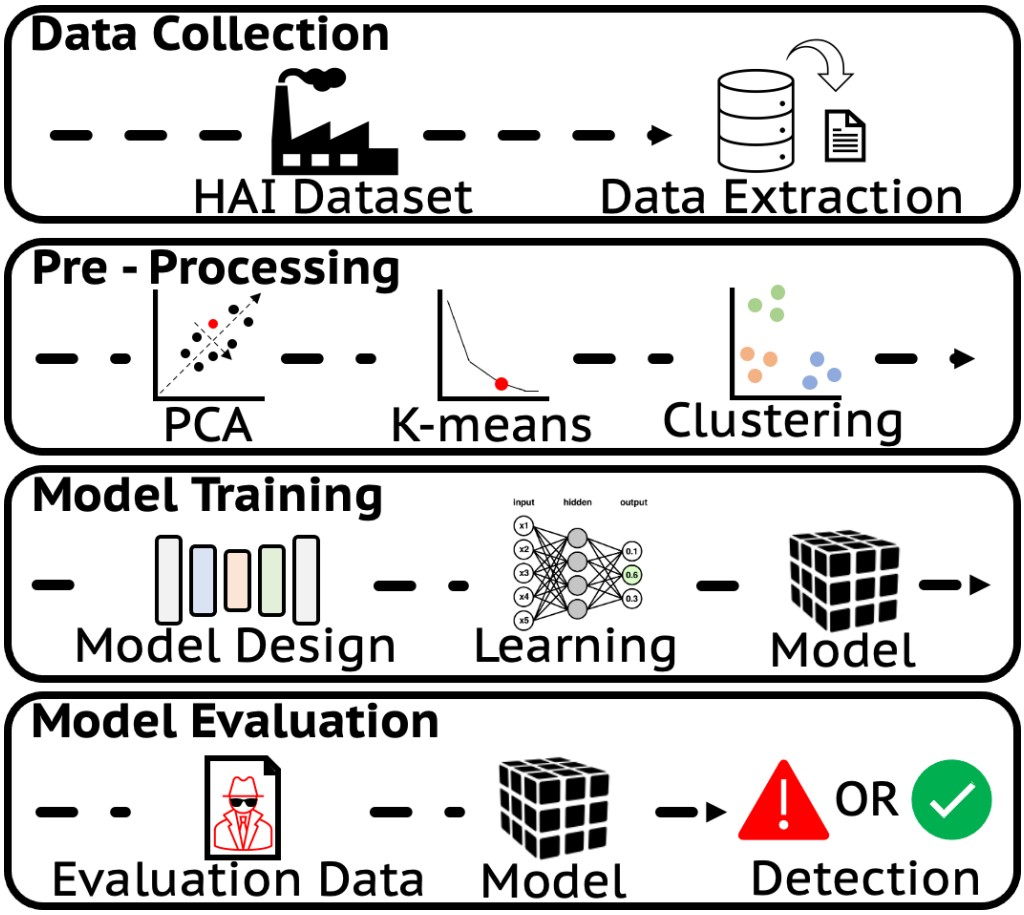

Figure 2. Proposal process overview.

3.2. The Dataset

Our study used an HAI dataset specifically designed for ICS security and augmented with hardware-in-the-loop (HIL) simulations. Figure 3 shows a model that simulates a real industrial environment. This dataset accurately reflects the operation of a real ICS environment, including key components such as the boiler, turbine, water treatment system, and HIL simulation. The boiler operation promotes heat exchange between water at various pressures and temperatures, while the turbine mechanism uses a rotor kit testbed to replicate the operation of a rotating machine. These components are seamlessly integrated through the HIL simulator to ensure they match the speed of the steam generator. The water treatment module emulates hydroelectric power generation by pumping water into an upper reservoir and then discharging it into a lower reservoir.

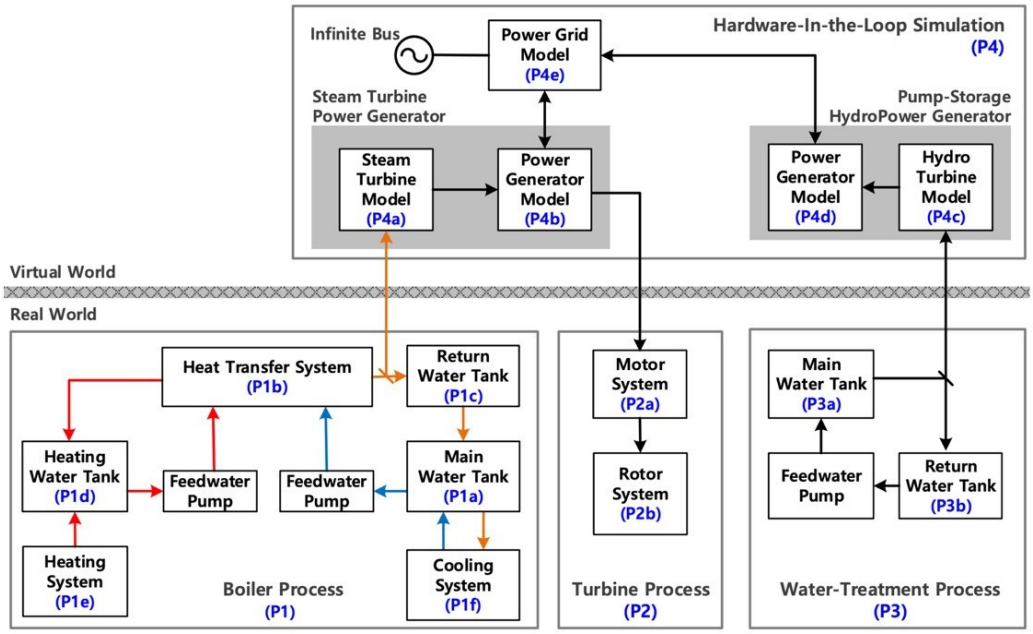

Figure 3. Hardware-in-the-loop (HIL) process flow diagram.

Data were collected from 59 sensors every second for four days, during which 28 artificial attacks were launched against the system, targeting various system points such as control outputs and parameters. For our research, version 22.04 of the HAI dataset consisted of six train\#.csv files, each containing 87 variables (devices). Table 2 is part of the Train1.csv file. We merged these files into a single dataset for model development. We then removed the "attack" column, which was deemed irrelevant to our study, resulting in a dataset of 86 operational variables.

Table 2. Train1.csv, version 22.04 of the HAI dataset.

Timestamp	P1_B2004	P1_B2016	P1_B3004	P1_B3005	...	P4_ST_TT01	Attack
11 July 2021 10:00:00	0.08771	0.88504	476.76703	1014.79321	...	27170	0
11 July 2021 10:00:01	0.08771	0.88619	476.76703	1014.79321	...	27171	0
11 July 2021 10:00:02	0.08771	0.88836	476.76703	1014.79321	...	27170	0
11 July 2021 10:00:03	0.08771	0.89214	476.76703	1014.79321	...	27171	0

3.3. Data Preparation

In this study, we used the HAI dataset to normalize and standardize the data in the initial stage. We also used PCA to select features and reduce dimensionality, and clustering techniques to identify groups of similar objects and identify groups of similar objects, in addition to basic preprocessing tasks. A clustering algorithm is a technique that groups similar data within a dataset based on their characteristics to form clusters. In this study, we removed the 'timestamp' information from the time series dataset before applying the clustering algorithm. To scale the data, we adjusted it to the range [0, 1] using the minimum and maximum values.

3.3.1. Implementing Cluster Segmentation

The K-means algorithm is an unsupervised learning algorithm that groups data into K clusters. It works by minimizing the variance of the distance difference between the given data and each cluster. The sum of squared errors (*SSE*) within each cluster, which is

the sum of the squares of the Euclidean distances between each data point and its cluster center, is expressed by the following formula.

$$SSE = \sum_{i=1}^{k} \sum_{x \in C_i} \| x - \mu_i \|^2$$

where k is the number of clusters. C_i is the set of data points in the ith cluster. x is a data point in cluster C_i. μ_i is the centroid or mean of all the data points in cluster C_i. $\|x - \mu_i\|^2$ is the square of the Euclidean distance between the data point x and the centroid μ_i. Figure 4 shows the number of tags between clusters. To cluster the data, we selected tags that showed similar patterns of behavior. The optimal number of clusters was set at the point where the *SSE* value of K-means dropped sharply, and our study set it at six groups obtained by the optimal value.

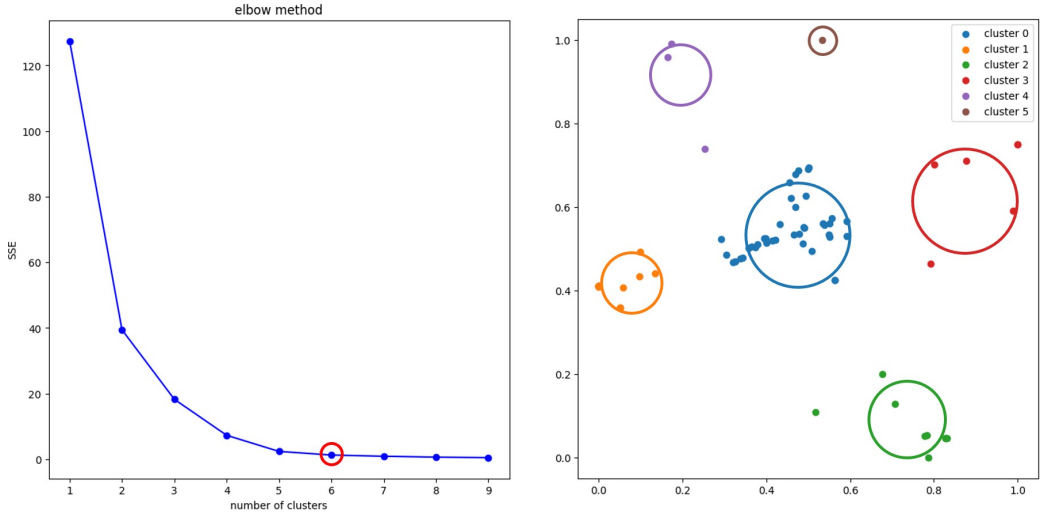

Figure 4. Number of tag clusters.

Table 3 shows the number of tags classified by clustering. Clustering is a technique for grouping data with similar characteristics, which is useful for characterizing and analyzing data. The number of all tags was 86 and was reduced to 3 dimensions using PCA. Data scaling is a common preprocessing step in data analysis that involves adjusting the values in your data to a particular range or scale. This can make variables with different units comparable or prevent variables with larger values from becoming more important during model training.

Table 3. Size of each cluster.

Cluster_Count	Cluster_Size
0	41
1	26
2	9
3	6
4	3
5	1

Cluster 4 is shown in Figure 5. The data were visually grouped based on similar characteristics, with each time series reflecting a distinct pattern or behavior. This allows you to monitor the health and performance of the system.

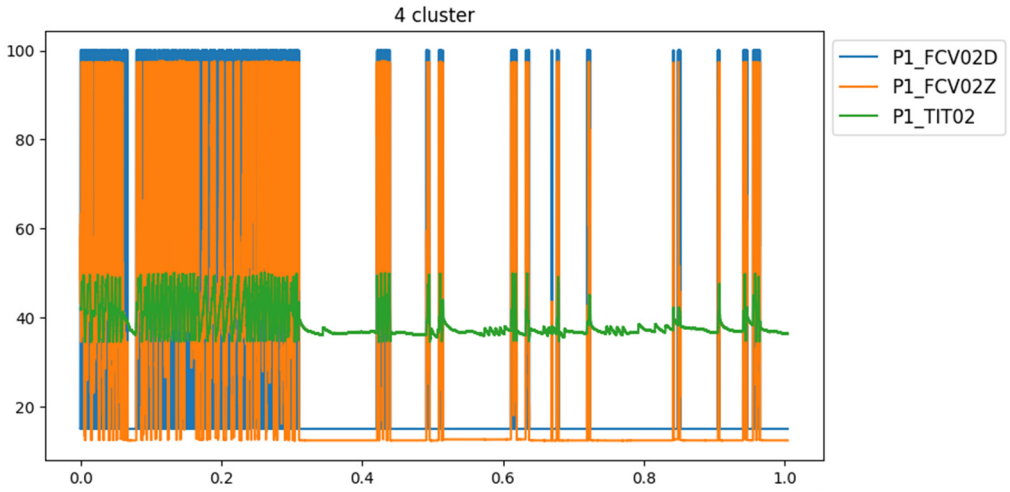

Figure 5. Tags in cluster 4.

3.3.2. Preparation of the Input Data

To process the time series data for use in the composite autoencoder model, the following steps were taken: Firstly, each data point was separated into one-second increments, and a min–max normalization was performed on the data points to adjust all data values to a range between 0 and 1. After completing the normalization process, we divided the entire dataset into 3600 s window sizes and rolled the data based on these windows. We calculated important statistical properties such as the standard deviation, mean, slope, and intercept of the data points in each window. Figure 6 shows the statistical characteristics for "P1_B2004".

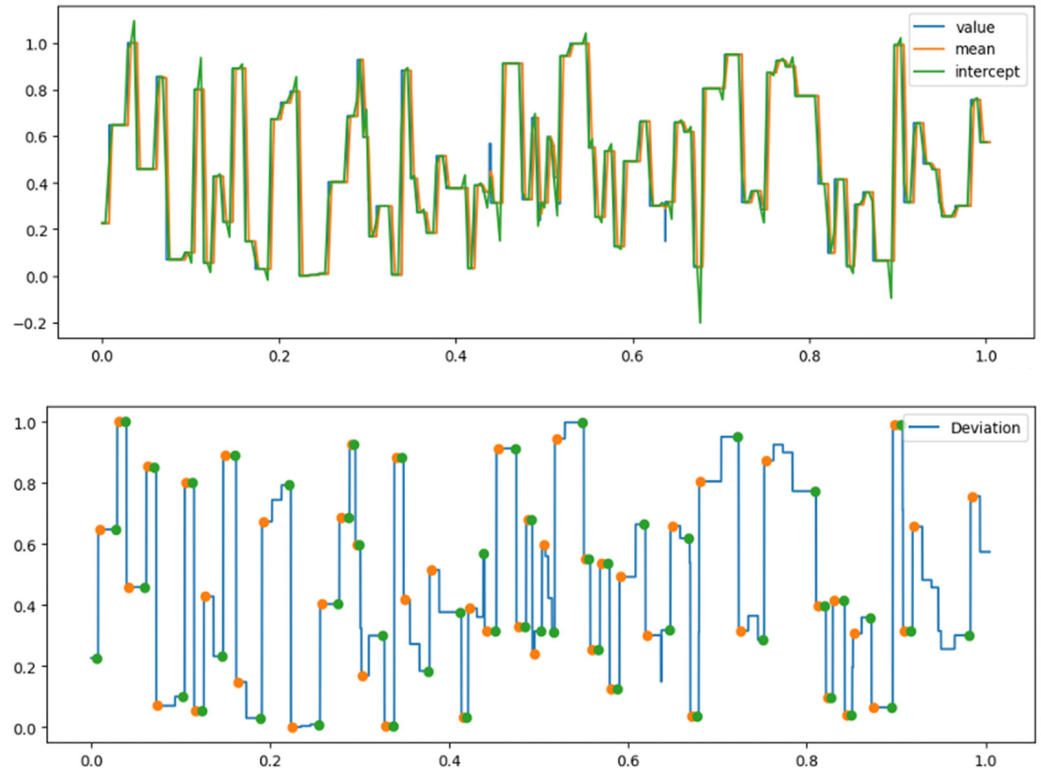

Figure 6. *Cont.*

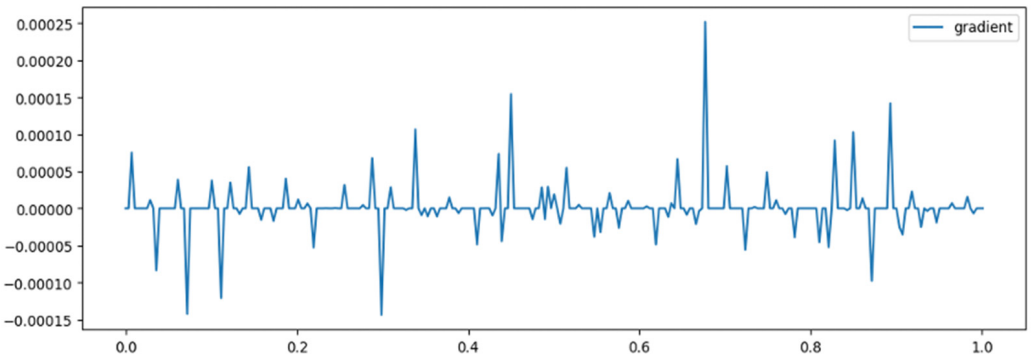

Figure 6. Statistical characteristics of input data.

Finally, to prepare the input data for the autoencoder model, we analyzed the peak values for each tag, broken down into 60 s increments. The normalization process saved the minimum and maximum values calculated for each tag by cluster, providing a reference point for the future ranging and thresholding of each tag. Table 4 displays the values for the statistical properties of collection tags.

Table 4. The values of the statistical property collection tag.

	Value	Mean	Std	Gradient	Intercept	Cluster
0	0.0299	0.0299	0.0000	0.0000	0.0000	1
1	0.0282	0.0291	0.0011	0.0000	0.0000	1
2	0.0293	0.0292	0.0008	0.0000	0.0000	1
3	0.0317	0.0307	0.0023	0.0000	0.0000	1
...	...	...	...	...	...	...

3.3.3. Design the Model Framework

This study applied a composite autoencoder model to detect anomalies in industrial control systems. The composite autoencoder evaluates anomalies by comparing the anomaly score of the output with a pre-generated threshold of the input and classifying it as an anomaly if it exceeds the threshold. The CNN layer filters the input data to activate specific features and then progressively abstracts them to reduce data complexity. The Rectified Linear Unit (ReLU) activation function introduces nonlinearity by setting negative values to zero. This allows the model to learn more complex functions, mitigating the problem of neuron deactivation and improving computational efficiency. Long Short-Term Memory (LSTM) networks, a type of Recurrent Neural Network (RNN), are particularly useful for detecting anomalies in time series data because they can remember long-term dependencies in sequential data. By combining CNNs and LSTM networks, composite autoencoders can identify and highlight important features in the data while encoding and decoding temporal variations. The encoder compresses the input data to extract significant features, and the decoder reconstructs the original data based on these features. Composite autoencoders can effectively detect anomalies, even if they are small or occur consistently over time, by capturing these important features and identifying anomalous patterns. Figure 7 shows the structure of the composite autoencoder used in our study.

- Input layer: In this study, each tag obtained by clustering was used as input data. It was assumed that all tags had no explanation, but they can be processed simultaneously because different data such as temperature, pressure, and flow were clustered.
- Output layer: The output layer of the model was designed to detect abnormal behavior. The output layer reconstructed the input data, compared it to the original data, and generated an abnormal behavior score. At this point, if the abnormal behavior score exceeded a certain threshold, it was considered abnormal and would inform you of the name, value, and time of occurrence of the tag.

- Activation functions and singularities: ReLU was used in the model to increase the nonlinearity of the model and to increase computational efficiency. Loss used the Mean Squared Error and the learning speed of the Adam optimizer was generally set to 0.001.

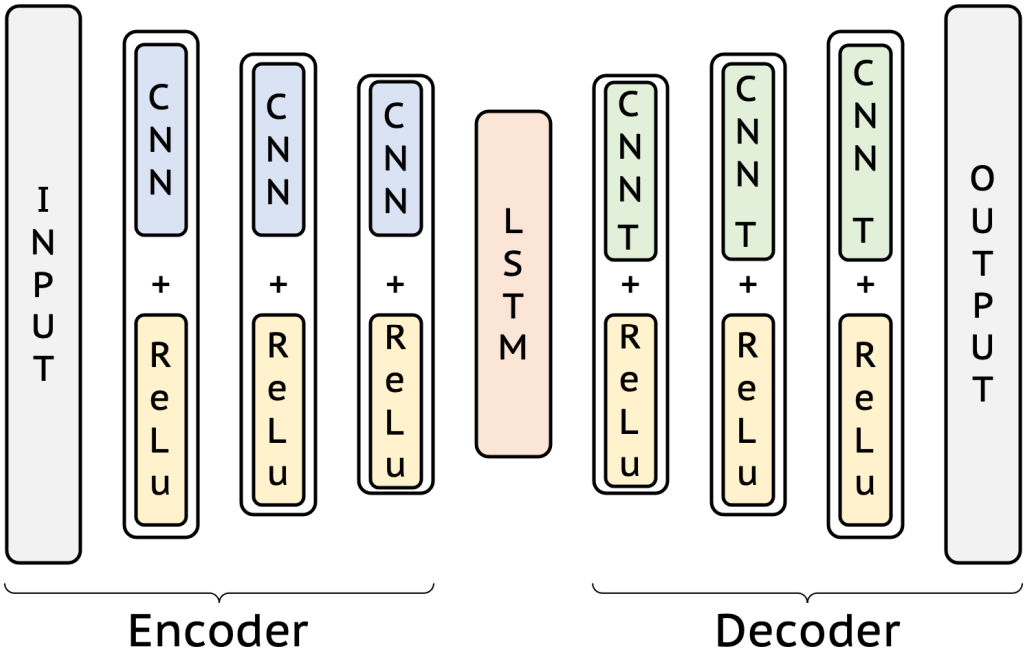

Figure 7. Composite autoencoder architecture.

3.3.4. Tag-Cluster Detection Classification Model

In this study, statistical attribute data were collected and analyzed on a cluster basis for each tag. Any data point that exceeded the threshold was considered anomalous behavior for that tag. Figure 8 shows a boxplot that visually shows the statistical properties of the clusters. If any of the input data, represented by the red dots, exceeded the statistical upper limit defined in the boxplot, anomalous behavior was detected and the corresponding tag was classified as anomalous.

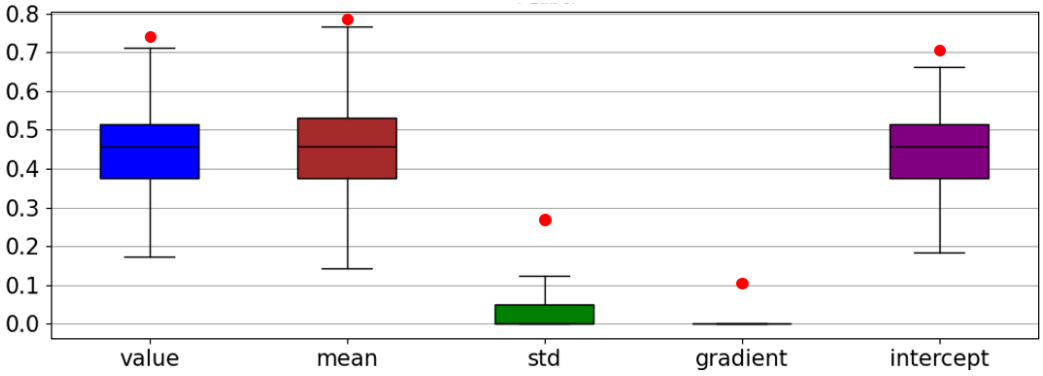

Figure 8. Boxplot for cluster.

As a result, outliers were identified by comparing the thresholds of the reconstructed values from the clustered input values to the output values.

3.4. Evaluation Metrics

One of the main objectives of this study was to systematically evaluate and validate the performance of the model. For this purpose, we used several performance metrics and validation methods.

- Performance metrics: Basically, we used the confusion matrix to calculate the number of true positives, true negatives, false positives, and false negatives. From this, we derived statistical metrics such as accuracy, precision, and recall to evaluate the performance of the model.
- Validation methodology: To increase the reliability of our performance metrics, we modeled the case of a hacking threat by assuming abnormal situations and adding intentional error data. We can evaluate how our anomaly detection model handles these situations.

Performance evaluation and validation are important steps that determine the practicality and reliability of a model. In this study, we performed these steps thoroughly, and we expect the model to perform well in real industrial settings.

Accuracy shows how many samples are correctly classified as a percentage of the total samples.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision shows how many of the predicted positive results are positive as a percentage of the total.

$$Precision = \frac{TP}{TP + FP}$$

Recall shows how many of the true positives are predicted to be positive, as a percentage.

$$Recall = \frac{TP}{TP + FN}$$

The *F*1 *score* is the harmonic mean of *precision* and *recall*. It is a good indicator of the balance between the two.

$$F1Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

4. Experiment and Evaluation

4.1. Classification and Confusion Matrix

Figure 9 is the result of the performance of the classification model. First, it showed high precision for all classes, with cluster 4 attaining a particularly good precision of 0.96. The recall is also high across the board, with cluster 1 attaining the best recall of 0.96. The *F*1 *score*, which is the harmonic mean of precision and recall, shows a balanced value for each class, with values above 0.86. Finally, the overall accuracy is around 0.93, showing that the model correctly classifies most of the total sample. These results indicate that the classification model does a good job of distinguishing between each class, and that it has a high overall performance.

Figure 10 shows that each cluster is clearly distinct. In this study, we performed clustering of the data using unsupervised learning methods. We also performed a validation of the clustering using a test set and found that the results were good, with the data points within each cluster clustered closely together with a clear distinction between the different clusters. These results show that the chosen clustering algorithm has a good grasp of the structure and patterns in the data.

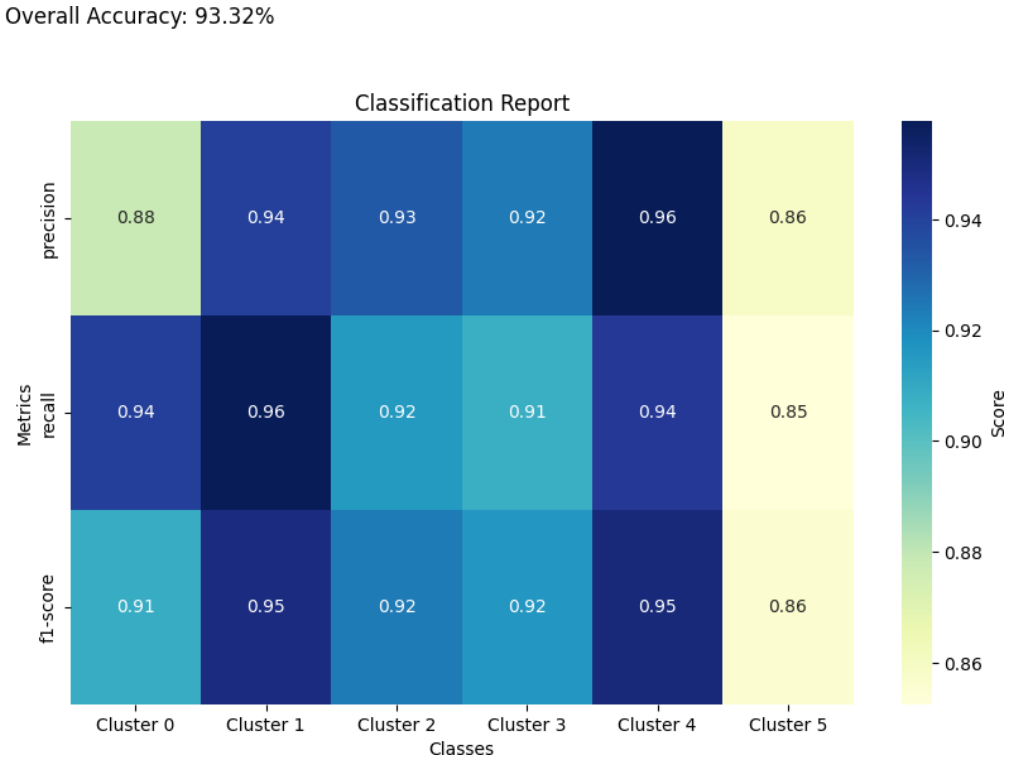

Figure 9. Classification result.

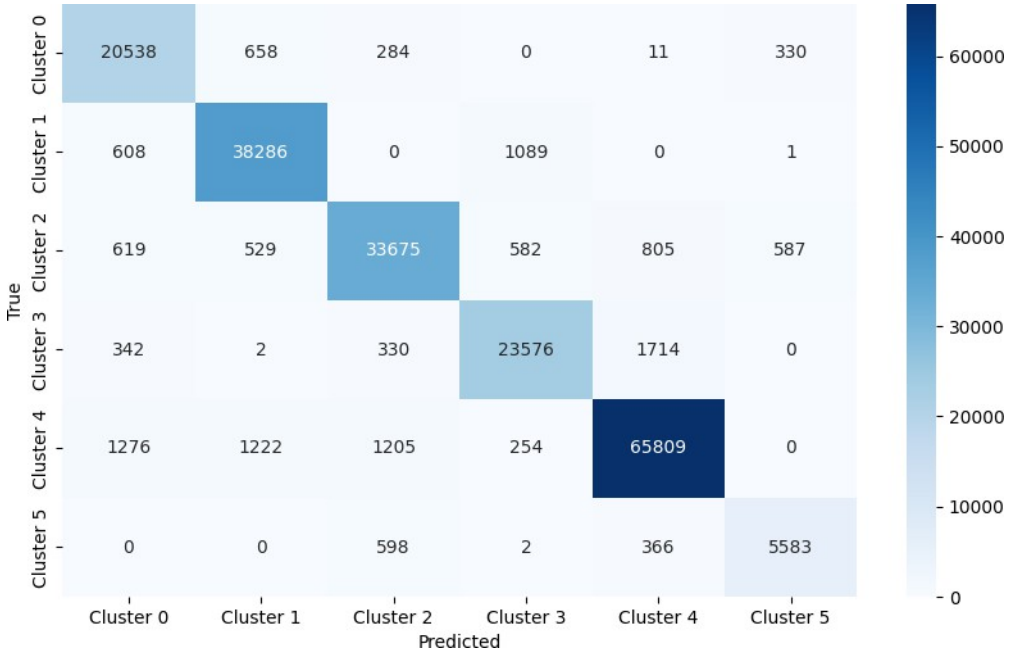

Figure 10. Cluster result.

4.2. Abnormal Behavior Detection Experiment

4.2.1. Single-Variable Abnormal Behavior

As an experiment to mimic sensor failure that may occur in a real operating environment or the abnormal operation of the system, we artificially manipulated data values of 3 s randomly selected from the total data points of 3,600 s to create a data anomaly. The main purpose of the experiment was to see how effective the detection system is in identifying a clear anomaly that occurred in a single variable. Figure 11 shows the detection result when a number of anomalous behaviors were detected in a single variable.

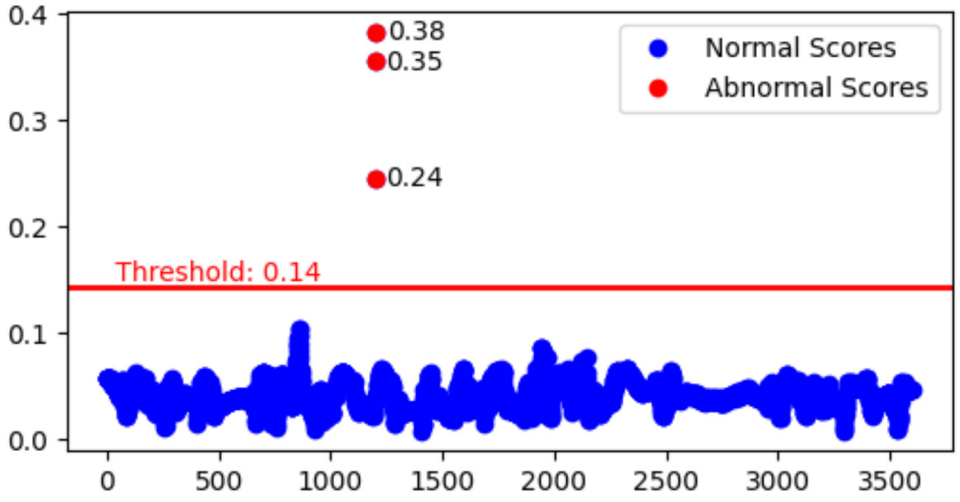

Figure 11. Single-variable detection results.

The abnormal behavior detection algorithm successfully detected a number of abnormal behaviors in a single variable that exceeded the threshold. Table 5 shows that the value of a single variable changes for 3 s, indicating that a single sensor or system can detect abnormal behavior or events.

Table 5. Single-variable detection tag name, timestamp, value.

Tag Name	Timestamp	Value
P1_B3005	11 July 2021 10:19:58	7014.7932
P1_B3005	11 July 2021 10:19:59	10,014.7932
P1_B3005	11 July 2021 10:20:00	11,014.7932

4.2.2. Multivariate-Variable Abnormal Behavior

This experiment focused on evaluating the ability of detection algorithms to detect anomalies occurring simultaneously in multiple variables. We selected two different tags and artificially manipulated one data value in each tag to create an anomaly data state. This experiment assumed a complex anomaly that may occur in different components or centers. The purpose of the experiment was to evaluate how the detection system performs in identifying these multivariate anomalies. Figure 12 shows the results of detecting anomalous behavior in multiple variables.

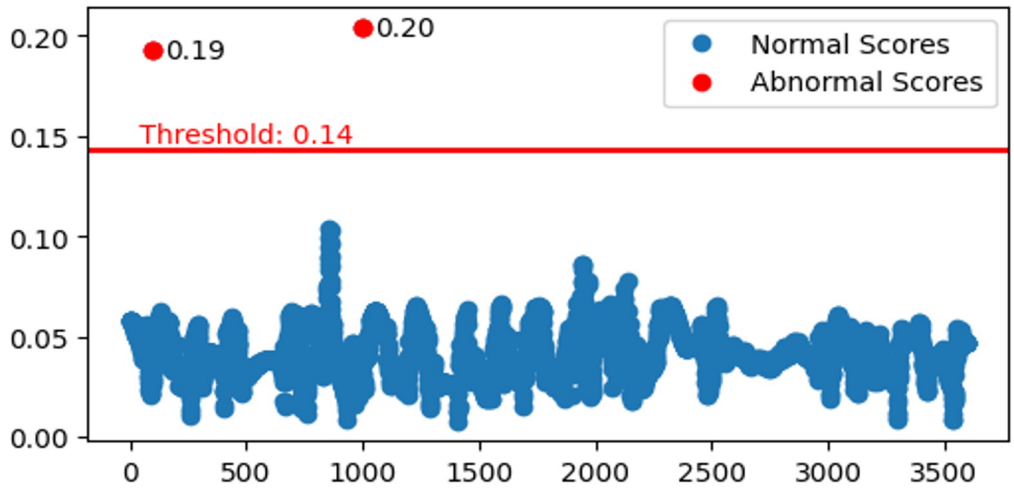

Figure 12. Multivariate-variable detection results.

Values exceeding the threshold were successfully detected in two or more variables. Table 6 shows the results of detecting these values. This demonstrates the ability to detect abnormal behavior or events across multiple sensors.

Table 6. Multivariate-variable detection tag name, timestamp, value.

Tag Name	Timestamp	Value
P1_B2004	11 July 2021 10:01:38	5000.08771
P1_B3004	11 July 2021 10:16:38	5000.36264

4.2.3. One-Variable Abnormal Behavior

The final experiment in our study was designed to verify that the detection system could accurately detect microscopic anomalies. We tested the anomalies by changing only one data value of a single tag, which was assumed to indicate subtle changes in the sensor or small system failures. The key to the experiment was to ensure that the detection algorithm could accurately detect these microscopic changes and generate the appropriate alerts. Figure 13 shows the detection of a single outlier in a variable.

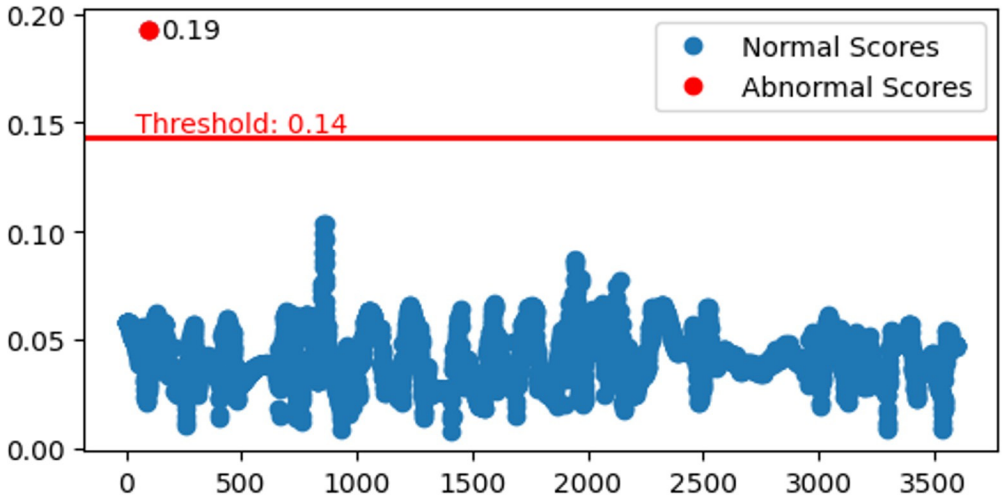

Figure 13. One-variable detection results.

This result shows that the detection model accurately detects small changes in a single variable. Table 7 shows a single value exceeding the threshold in only one variable, demonstrating the ability of our model to proactively and accurately respond to problems before they occur.

Table 7. One-Variable detection tag name, timestamp, value.

Tag Name	Timestamp	Value
P1_B2004	11 July 2021 10:01:38	5000.08771

5. Conclusions

The industrial control system (ICS) is an essential component in the management and control of industrial processes where security and reliability are of utmost importance. Anomaly detection is an essential mechanism for detecting deviations from normal system behavior and identifying potential attacks or system failures. However, generating labeled datasets for supervised machine learning models is a challenging task in ICSs because it requires significant effort and expertise. To address these challenges, this paper presents an unsupervised learning mechanism for anomaly detection in ICSs using instrumentation data. The approach is to use unlabeled datasets to train a machine learning model to detect

anomalous behavior in the system. This approach is preferred because it does not require labeled datasets, making the process more feasible and cost-effective [33]. We have found that a composite autoencoder model that captures the ability to detect anomalous behavior in the ICS and identifies unusual patterns in the data is most effective.

In future work, we plan to investigate identifying attack types based on real-world measurement data. We believe that identifying attack types that occur in real systems and quickly detecting threats is best suited for anomaly detection in ICSs. It is also important to quickly identify and mitigate potential threats to prevent potential outages. To this end, we would like to explore different techniques and models that can effectively identify different types of attacks in ICSs.

Author Contributions: W.-H.C. designed the algorithm, performed the simulations, and prepared the manuscript as the first author. J.K. led the project and research and advised on the whole process of manuscript preparation. All authors discussed the simulation results and approved the publication. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No. 2019-0-01842, Artificial Intelligence Graduate School Program (GIST)).

Data Availability Statement: Publicly available datasets were analyzed in this study. This data can be found here: [https://github.com/icsdataset/hai] (accessed on 25 April 2022).

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

References

1. Fausto, A.; Gaggero, G.B.; Patrone, F.; Girdinio, P.; Marchese, M. Toward the integration of cyber and physical security monitoring systems for critical infrastructures. *Sensors* **2021**, *21*, 6970. [CrossRef] [PubMed]
2. Wang, Z.; Song, H.; Watkins, D.W.; Ong, K.G.; Xue, P.; Yang, Q.; Shi, X. Cyber-physical systems for water sustainability: Challenges and opportunities. *IEEE Commun. Mag.* **2015**, *53*, 216–222. [CrossRef]
3. Stouffer, K.; Falco, J.; Scarfone, K. Guide to industrial control systems (ICS) security. *NIST Spec. Publ.* **2011**, *800*, 16.
4. Tuptuk, N.; Hailes, S. Security of smart manufacturing systems. *J. Manuf. Syst.* **2018**, *47*, 93–106. [CrossRef]
5. Nachreiner, F.; Nickel, P.; Meyer, I. Human factors in process control systems: The design of human–machine interfaces. *Saf. Sci.* **2006**, *44*, 5–26. [CrossRef]
6. Ralston, P.A.; Graham, J.H.; Hieb, J.L. Cyber security risk assessment for SCADA and DCS networks. *ISA Trans.* **2007**, *46*, 583–594. [CrossRef] [PubMed]
7. de Brito, I.B.; de Sousa, R.T., Jr. Development of an open-source testbed based on the modbus protocol for cybersecurity analysis of nuclear power plants. *Appl. Sci.* **2022**, *12*, 7942. [CrossRef]
8. Evancich, N.; Li, J. Attacks on industrial control systems. In *Cyber-Security of SCADA and Other Industrial Control Systems*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 95–110.
9. Jin, M.; Lavaei, J.; Johansson, K.H. Power grid AC-based state estimation: Vulnerability analysis against cyber attacks. *IEEE Trans. Autom. Control* **2018**, *64*, 1784–1799. [CrossRef]
10. Rajkumar, V.S.; Ştefanov, A.; Presekal, A.; Palensky, P.; Torres, J.L.R. Cyber attacks on power grids: Causes and propagation of cascading failures. *IEEE Access* **2023**, *11*, 103154–103176. [CrossRef]
11. Cheminod, M.; Durante, L.; Valenzano, A. Review of security issues in industrial networks. *IEEE Trans. Ind. Inform.* **2012**, *9*, 277–293. [CrossRef]
12. Dzung, D.; Naedele, M.; Von Hoff, T.P.; Crevatin, M. Security for industrial communication systems. *Proc. IEEE* **2005**, *93*, 1152–1177. [CrossRef]
13. Lindsay, J.R. Stuxnet and the limits of cyber warfare. *Secur. Stud.* **2013**, *22*, 365–404. [CrossRef]
14. Hao, W.; Yang, T.; Yang, Q. Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber-physical systems. *IEEE Trans. Autom. Sci. Eng.* **2021**, *20*, 32–46. [CrossRef]
15. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
16. Audibert, J.; Michiardi, P.; Guyard, F.; Marti, S.; Zuluaga, M.A. Usad: Unsupervised anomaly detection on multivariate time series. In Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, Virtual, 6–10 July 2020; pp. 3395–3404.
17. Zhu, B.; Joseph, A.; Sastry, S. A taxonomy of cyber attacks on SCADA systems. In Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 9–22 October 2011; pp. 380–388.

18. Kim, B.; Alawami, M.A.; Kim, E.; Oh, S.; Park, J.; Kim, H. A comparative study of time series anomaly detection models for industrial control systems. *Sensors* **2023**, *23*, 1310. [CrossRef] [PubMed]
19. Inoue, J.; Yamagata, Y.; Chen, Y.; Poskitt, C.M.; Sun, J. Anomaly detection for a water treatment system using unsupervised machine learning. In Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW), New Orleans, LA, USA, 18–21 November 2017; pp. 1058–1065.
20. Putchala, M.K. Deep Learning Approach for Intrusion Detection System (ids) in the Internet of Things (iot) Network Using Gated Recurrent Neural Networks (gru). Master's Thesis, Wright State University, Dayton, OH, USA, 2017.
21. Du, Y.; Huang, Y.; Wan, G.; He, P. Deep Learning-Based Cyber–Physical Feature Fusion for Anomaly Detection in Industrial Control Systems. *Mathematics* **2022**, *10*, 4373. [CrossRef]
22. Goh, J.; Adepu, S.; Tan, M.; Lee, Z.S. Anomaly detection in cyber-physical systems using recurrent neural networks. In Proceedings of the 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, 12–14 January 2017; pp. 140–145.
23. Mokhtari, S.; Abbaspour, A.; Yen, K.K.; Sargolzaei, A. A machine learning approach for anomaly detection in industrial control systems based on measurement data. *Electronics* **2021**, *10*, 407. [CrossRef]
24. Catillo, M.; Pecchia, A.; Villano, U. A Deep Learning Method for Lightweight and Cross-Device IoT Botnet Detection. *Appl. Sci.* **2023**, *13*, 837. [CrossRef]
25. Liu, J.; Wang, X.; Xie, F.; Wu, S.; Li, D. Condition monitoring of wind turbines with the implementation of spatio-temporal graph neural network. *Eng. Appl. Artif. Intell.* **2023**, *121*, 106000. [CrossRef]
26. Pang, J.; Pu, X.; Li, C. A hybrid algorithm incorporating vector quantization and one-class support vector machine for industrial anomaly detection. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8786–8796. [CrossRef]
27. Wolsing, K.; Thiemt, L.; Sloun, C.V.; Wagner, E.; Wehrle, K.; Henze, M. Can industrial intrusion detection be simple? In Proceedings of the European Symposium on Research in Computer Security, Copenhagen, Denmark, 26–30 September 2022; pp. 574–594.
28. Park, H.; Choi, Y.J. Frequency-Based Representation of Massive Alerts and Combination of Indicators by Heterogeneous Intrusion Detection Systems for Anomaly Detection. *Sensors* **2022**, *22*, 4417. [CrossRef] [PubMed]
29. Kim, J.; Shin, J.; Park, K.W.; Seo, J.T. Improving Method of Anomaly Detection Performance for Industrial IoT Environment. *Comput. Mater. Contin.* **2022**, *72*, 5377–5394. [CrossRef]
30. Xue, F.; Yan, W. Multivariate time series anomaly detection with few positive samples. In Proceedings of the 2022 International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 18–23 July 2022; pp. 1–7.
31. Gaggero, G.B.; Caviglia, R.; Armellin, A.; Rossi, M.; Girdinio, P.; Marchese, M. Detecting cyberattacks on electrical storage systems through neural network based anomaly detection algorithm. *Sensors* **2022**, *22*, 3933. [CrossRef] [PubMed]
32. Shin, H.K.; Lee, W.; Yun, J.H.; Kim, H. HAI 1.0: HIL-Based Augmented ICS Security Dataset. In Proceedings of the 13th USENIX Conference on Cyber Security Experimentation and Test, Berkeley, CA, USA, 10 August 2020; USENIX Association: Berkeley, CA, USA, 2020.
33. Maseer, Z.K.; Yusof, R.; Bahaman, N.; Mostafa, S.A.; Foozy, C.F.M. Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. *IEEE Access* **2021**, *9*, 22351–22370. [CrossRef]