Anthony Vivian Onyinyechi, 2026, 14:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

IDS Based Model for Industrial Control Systems Using Artificial Neural Network

Anthony Vivian Onyinyechi, Umejuru Daniel, Vinani Nuka Precious
Department of Computer Science, University of Port Harcourt, Choba, Nigeria

Abstract- In the present scenario of rapidly changing technology, the industrial control system (ICS) is the backbone of critical services like power generation, production units, and transport services. However, with the increasing interconnectivity of the components of the ICS, they are also increasingly exposed to various cyber-attacks, which may have varying effects from operational bugs to possible threats to public safety. The hybrid nature of the ICS network, along with the need for continuous real-time monitoring, creates a challenge in identifying possible threats to the ICS network. A cyber-attack on an industrial control system can lead to system unavailability, loss of production, economic loss, and even potential threats to public safety in extreme cases. This is a point of concern for a wide range of stakeholders who use ICS for their day-to-day business activities. Traditional security solutions are no match to the advanced nature of cyber-attacks, thus requiring the development of innovative solutions that can offer effective protection against cyber-attacks and unauthorized access. The proposed research work aims to make industrial control systems cyber-attack proof using the capabilities of artificial intelligence (AI) and deep learning (DL) models. The focus is on designing a Deep Learning-Based Intrusion Detection System (IDS) that can detect and mitigate port scanning and Distributed Denial of Service (DDoS) attacks in real-time on ICS networks, as the current IDS systems may offer some level of security but are not capable of dealing with the ever-changing nature of cyber-attacks. The proposed research work uses the Rapid Application Development (RAD) method, where the data from the ICS is collected and preprocessed to enable effective feature extraction and development of the model. The diagnostic parameters used in the proposed research work include the confusion matrix, accuracy, precision, recall, and F1-score. The proposed model was validated using a sample of the HAI 21.04 dataset and achieved an average accuracy of 98.58%, thus proving the effectiveness of the proposed model in detecting normal and abnormal patterns in the ICS data.

Keywords: AI, Intrusion Detection, Industrial Control System, Network, Anomaly Detection.

I. INTRODUCTION

Technology is advancing at a very fast rate, resulting in immense growth in various fields, but it is also opening up new ways of cyber attacks that are a challenge to the individual, organization, and government. Industrial Control Systems (ICS) are an integral part of various sectors and are not left untouched by these attacks. As ICS continues to merge with information technology and the internet, the threat level continues to rise, and thus there is a need for effective and innovative security solutions to protect these critical resources (Aldairi et al. 2022).

Intrusion Detection Systems (IDS) emerged on the scene with Jim Anderson in 1980. Since then, various IDS solutions have developed to meet the evolving needs of network security. An IDS system works by observing the network traffic to check if any attack or intrusion is taking place. It is always on, providing status information about the system, observing user activities, and alerting the management station (Abombara and Keien 2023). Among the most promising approaches to enhance the security of ICS is an IDS powered by AI and deep learning techniques. The aim of this project is to apply AI to actively detect and prevent cyber-attacks targeting ICS. By analyzing traffic patterns and detecting anomalies in real-time, an AI-powered IDS can detect potential attacks and malicious activities, securing critical infrastructure (Almseidin et al. 2020). The application of ANN for intrusion detection in ICS is becoming increasingly complex, employing a variety of different neural networks to enhance detection speed and accuracy and provide a strong defense against sophisticated cyber-attacks.

This is an important development in ensuring that industrial systems are protected from the constantly growing threat of cyber-attacks. The importance of this research work is that it has the potential to enhance cyber security by enhancing the capabilities of IDS specifically designed for industrial control systems. The research uses AI and deep learning techniques to ensure that critical infrastructure is protected from constantly evolving threats, thereby enhancing the functionality of ICS and the world it supports.

II. CONCEPTUAL REVIEW

Collectively, these reviews offer a wider insight into the use of deep learning in the context of cybersecurity, especially in the area of protecting industrial control systems. They mention the basics of anomaly detection, the need for data preprocessing, and the crucial role of having proper evaluation metrics in intrusion detection systems (IDS) (Umejuru et al 2025). The diversity of the studies reviewed reflects the progress achieved as well as the existing gaps in addressing the challenging threats of cyber attacks.

Deep Learning for Network Security

Deep learning is especially important as one of the key drivers in improving network security by helping to build flexible and resilient intrusion detection systems (Lin and Chen 2021). In another review, the authors Umejuru et al. (2025) highlight the significance of CNNs and RNNs in deep learning in addressing the ever-changing nature of cyber threats.

- **Deep Learning Architectures:** It also talks about how models of deep learning, inspired by the neural networks of the human brain, are able to identify complex patterns and representations from large amounts of data. For example, CNNs are suited for image-based threat detection, while RNNs are suited for handling sequences such as network logs.
- **Adaptive Threat Detection:** One of the major benefits of deep learning is that it is flexible. According to the review, deep learning models are always able to adapt to new types of attacks. This is important because attacks are always evolving.
- **Challenges and Limitations:** Although deep learning has a lot of promise, it also has its own set of challenges. The key challenges that deep learning faces are how to interpret deep learning, the need for a lot of data, and the need for a lot of computational power. The review emphasizes that these challenges have to be addressed to ensure that the full potential of deep learning in network security can be achieved.

Industrial Control Systems Security Challenges

Industrial Control Systems (ICS) are the backbone of all critical infrastructure, such as power plants and manufacturing facilities. Nevertheless, these systems are now facing threats from cyber security incidents. In 2021, NSIT carried out a review with the objective of addressing the distinct security challenges associated with ICS.

- **Complexity of ICS Networks:** The review also illustrates how the complexity and interconnectivity of ICS networks mean that a chain reaction can occur as a result of a single failure unless the defenses are strong enough. The review also illustrates the different components and protocols that are used in ICS networks.
- **Impact of Cyber Threats:** Garcia also stresses the level of danger that may be caused by a successful cyber attack on industrial control systems, from halting operations to significant financial losses. This, therefore, shows that intrusion detection systems, especially in ICS, are more in demand than ever before.
- **Tailored Security Solutions:** To solve these issues, the review recommends the development of intrusion detection systems that can be modified to work in industrial control systems (ICS). This should be done while taking into consideration the special features of the ICS network, such as the use of anomaly detection methods.

Anomaly Detection In Network Traffic

The idea of anomaly detection is of great relevance in identifying any anomalies in the network traffic that could be harmful. Gao et al. (2023) undertook a conceptual study that is founded on the idea of anomaly detection.

- **Anomaly Detection Basics:** The review offers a general introduction to the basics of anomaly detection, which states that it is essentially the process of looking for patterns or behaviors that lie well outside the normal range. This is a concept that can be applied in a variety of fields, ranging from finance to healthcare.
- **Machine Learning in Anomaly Detection:** As stated by Brown, there is a growing adoption of machine learning, and more specifically unsupervised machine learning, for anomaly detection. Machine learning algorithms are able to detect unusual patterns in network traffic and trigger an alert if there is a suspected threat.
- **Types of Anomalies:** There are three general types of anomalies: point anomalies, contextual anomalies, and collective anomalies. Each of these types represents a different kind of cybersecurity situation.

Data Preprocessing In Cyber Security

Before the establishment of any detection system, appropriate data preprocessing is a necessary step in the effective implementation of intrusion detection systems. According to Buczak and Guven (2021), data preparation is an essential component of cyber security.

Data Cleaning and Noise Reduction: The review highlights the significance of cleaning the data, removing duplicate data, and removing features that do not actually matter. It also highlights the significance of removing noise from the data.

Feature Selection: In the video, Chen discusses feature selection, which is the
process of selecting the features that actually matter and ignoring the rest.

Normalization and Standardization: Normalization and standardization come next, which scale all the features to a single scale. This is significant to make sure that all features are treated equally during the training of the model.

Related Reviews

The NCO-double-layer DIFF_RF-OPFYTHON intrusion detection system was proposed by Cao et al. (2022), which integrates the neural cooperative optimization (NCO), double-layer differentiation of random forests (DIFF_RF), and OPFYTHON modules to build a secure ICS intrusion detection system. This work is a significant advancement, but it concentrates on optimization methods, not the integration of deep learning models.

In a related field of study, Hindy et al. (2020) proposed an ensemble of Deep Belief Networks (DBNs) for intrusion detection in SCADA-IoT systems. The proposed approach demonstrated better zero-day attack detection performance and resistance to noisy or incomplete data, thus verifying the efficacy of deep ensemble models in industrial cybersecurity.

Al-Abassi et al. proposed a deep learning ensemble tailored for the ICS environment. They tackled the ever-present problem of highly imbalanced ICS data with balanced feature representation through deep representation learning. The features were then fed into a hybrid classifier that combined Deep Neural Networks and decision trees. The ensemble not only outperformed conventional approaches such as Random Forest and AdaBoost, but it also maintained low false positives. The important point to note is that it can be easily integrated into the existing ICS infrastructure with little to no disruption.

Conventional intrusion detection systems usually depend on existing patterns and are intended for identifying known cyber attacks. Thus, they are inefficient in identifying unknown cyber attacks. In their research paper in 2022, Tian et al. developed the NCO-double-layer DIFF_RF-22 OPFYTHON framework for ICS intrusion detection systems. The framework consists of NCO, double-layer DIFF_RF, and OPFYTHON modules. The double-layer DIFF_RF module distinguishes traffic types into known attacks, unknown attacks, and normal traffic types.

The study proved that their framework is more effective than conventional approaches such as XGBoost and SVM, especially in identifying unknown

attacks. The framework achieved an impressive accuracy of 98.13% on the dataset used in the research paper.

III. METHODOLOGY

The method that is being used is RAD, or Rapid Application Development. It is also known as Rapid Application Building, but it is a method of software development that is flexible in its methodology. It favors quick application development over planning and documentation. It is a method that favors a strong interaction between developers and users, so that the user requirements can be incorporated into the design of the system. It is most appropriate for applications where the user interface is of utmost importance.

Analysis of the Proposed System

The proposal describes an Intrusion Detection System for Industrial Control Systems that uses an Artificial Neural Network (ANN). The system does not rely on rules to detect potential attacks but instead uses the power of neural networks to detect both known and unknown attacks through anomaly detection.

How it Works: An Artificial Neural Network will be trained using data that contains normal traffic patterns for the Industrial Control Systems as well as various types of known intrusion attacks. After training the network, it will be able to generalize the data and point out any irregularities in the traffic patterns. The network will then be linked to the Industrial Control Systems to watch for any irregular traffic patterns.

This system is highly efficient in spotting sophisticated cyber-attacks like Denial of Service even when the patterns of these attacks haven't been detected before.

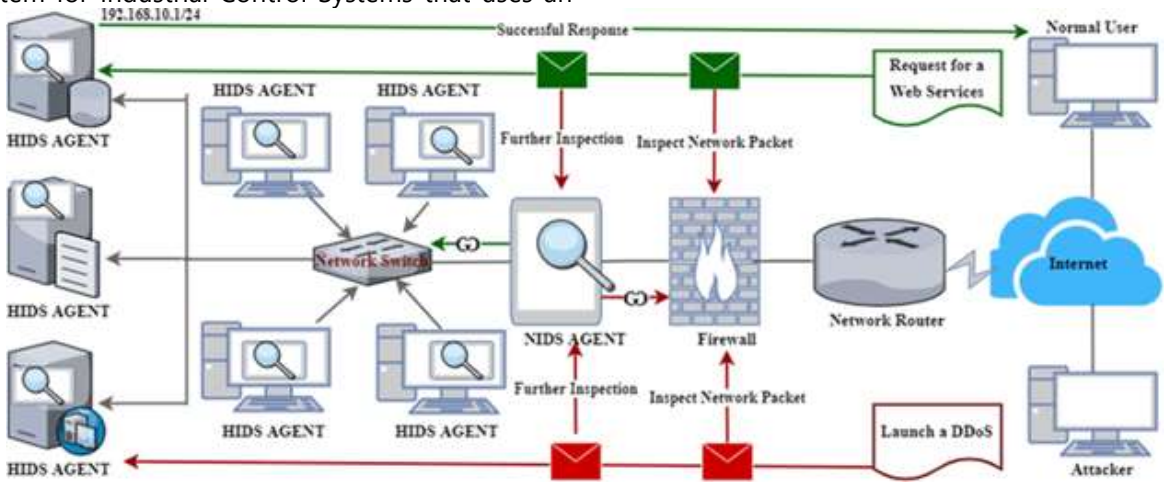

Figure 3.1: Architecture of the Proposed System

Elements of the Proposed System

- **Data Collection Tier:** The system real-time acquisition of ICS traffic using packet sniffers or protocol analyzers.
- **Detection Tier:** An artificial neural network model analyzes the acquired data and identifies whether it is malicious or benign.
- **Response and Alert Tier:** Upon detection of anomalies in the ICS traffic, the system records the event and alerts the ICS security administrator.

This project integrates the practical hands-on data from the real ICS environment with the existing publicly available data to develop and test an Artificial Neural Network-based Intrusion Detection System for Industrial Control Systems. In the real-world setting, the project directly captures the real-time network traffic from the ICS environment, which is already being monitored and has existing monitoring tools in place.

This includes the direct capture of the raw network traffic, sensor data, and real-time operational logs,

simulating real-time system activity and aiding in the detection of potential anomalies and threats. To add to the existing dataset, the project also utilizes the Full HAI dataset, which is publicly available and has been specifically designed for research use in the context of Intrusion Detection Systems for Industrial Control Systems. This dataset includes labeled network traffic, encompassing a variety of normal system activity and various attack scenarios, including Denial of Service and reconnaissance attacks. This adds to the visibility and overall capabilities of the developed ANN-based IDS for Industrial Control Systems.

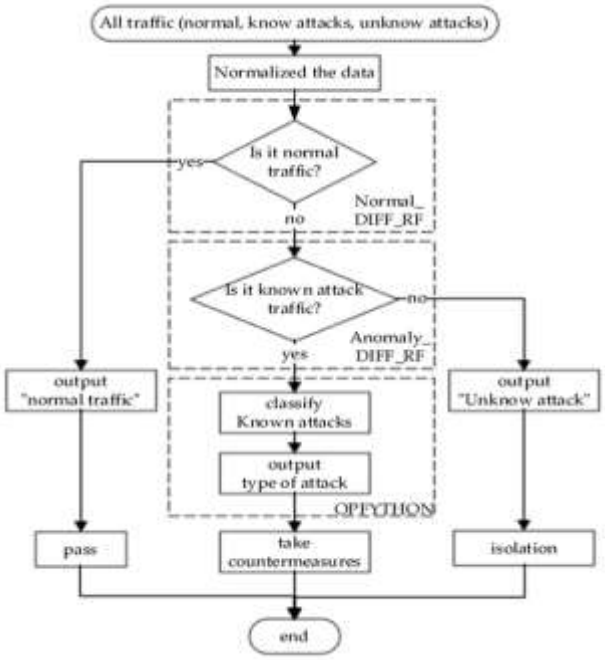

Figure 3.2: Flowchart of the Proposed System

Use Case: Intrusion Detection and Alert Notification

In this situation, the role of the ICS Admin and the ANNs System is paramount. After the deployment of the trained ANNs model, the process now starts. The ICS system sends network traffic, which is received and analyzed by the ANN model. If the model identifies the anomaly, an alert is sent to the administrator. The process ends with the logging of the intrusion and the administrator taking preventive action.

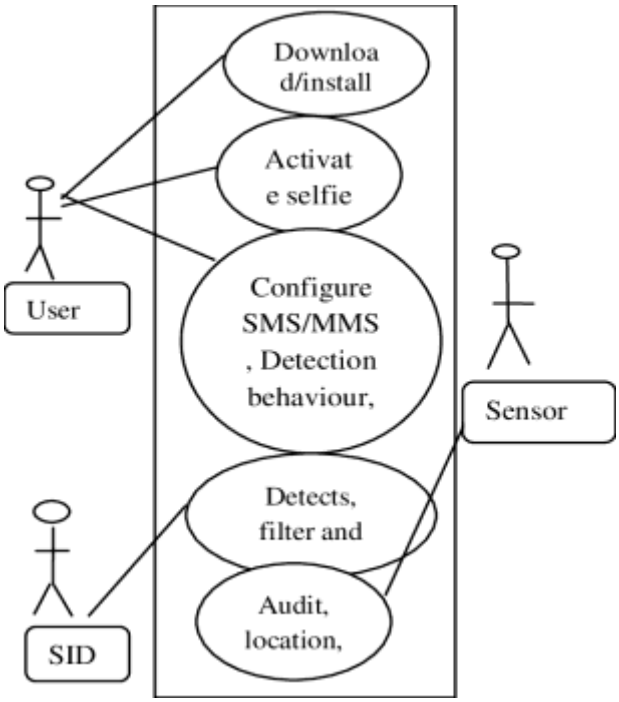

Figure 3.3: Use Case Diagram of the Proposed System

This use case diagram illustrates the interaction between User and System, including activities such as download and install, activate selfie, SMS/MMS with detection behavior, and audit location. SID, which stands for System ID, is a unique identifier for devices or accounts that communicate with the system to perform these activities along with User.

Database Structure of the Proposed System

The ANN model is based on real-time data, but you can use a simple database setup for alerts and logging for auditing.

Table 3.1: Intrusion Alerts

Field Name	Data Type	Description
id	INT	Primary key
timestamp	DATETIME	Time of intrusion detection
source_ip	VARCHAR	IP address of suspected source
threat_type	VARCHAR	Type of intrusion detected
confidence_score	FLOAT	ANN model prediction confidence
status	VARCHAR	Alert status (open/resolved)

Data Source

This process combines real-time ICS monitoring with external benchmarks in order to construct and test an ANN-based IDS for Industrial Control Systems. We collect real-time network traffic directly from the ICS environment using in-system monitoring tools. We also use the Full HAI dataset, which is a pre-existing, publicly available resource for IDS research in ICS environments. This dataset provides labeled network traffic data for normal activity, as well as a variety of attacks such as DoS and reconnaissance. By using these two data sources, we hope to build stronger, more accurate ANN-based IDS. The Full HAI dataset is available for download at [HAI GitHub] https://github.com/icsdataset/hai

After the dataset is uploaded, it is cleaned by dropping the timestamp columns, encoding the label column (Normal/Attack), and scaling all numerical features using the StandardScaler. A preview of the uploaded dataset is shown in a table, displaying the first 10 rows of the dataset for verification.

Table 3.2: Dataset

	time	P1_B2004	P1_B3004	P1_B3005	P1_B4002	P1_B4005	P1_B4022	P1_FCV01D	P1_FCV01Z	P1_FCV02D	P1_FCV02Z	P1_FCV03D	P1_FCV03Z	P1_FT01	P1_FT01Z	P1_FT02	P1_FT02Z
0	2020-08-04 22:00:00	0.1003	401.092	1105.1462	32.1643	100	36.0942	94.1485	94.3771	0	-1.8066	63.1946	63.768	209.2743	907.8827	1967.0867	2828.916
1	2020-08-04 22:00:01	0.1003	401.092	1105.1462	32.1643	100	36.098	94.2534	94.3848	0	-1.8066	63.2546	63.768	209.0635	916.1453	1965.5608	2828.214
2	2020-08-04 22:00:02	0.1003	401.092	1105.1462	32.1643	100	36.1003	94.3844	94.3771	0	-1.8066	63.266	63.768	208.1299	915.7105	1976.2418	2828.775
3	2020-08-04 22:00:03	0.1003	401.092	1105.1462	32.1643	100	36.0999	94.3753	94.3848	0	-1.8066	63.2507	63.768	210.8002	913.5361	1975.6697	2827.632
4	2020-08-04 22:00:04	0.1003	401.092	1105.1462	32.1643	100	36.0991	94.4933	94.3848	0	-1.8066	63.2329	63.768	205.841	919.6244	1972.6182	2835.513
5	2020-08-04 22:00:05	0.1003	401.092	1105.1462	32.1643	100	36.1007	94.64	94.3848	0	-1.8066	63.2259	63.768	206.7948	908.3175	1967.6588	2835.092
6	2020-08-04 22:00:06	0.1003	401.092	1105.1462	32.1643	100	36.1058	94.8093	94.3848	0	-1.8066	63.1908	63.768	208.8928	910.4921	1967.2776	2832.846
7	2020-08-04 22:00:07	0.1003	401.092	1105.1462	32.1643	100	36.1279	94.9271	94.3848	0	-1.8066	63.2189	63.768	209.7021	915.2755	1972.8088	2829.196
8	2020-08-04 22:00:08	0.1003	401.092	1105.1462	32.1643	100	36.1243	94.9769	94.4534	0	-1.8066	63.2227	63.768	207.1762	914.8407	1967.0867	2828.916
9	2020-08-04 22:00:09	0.1003	401.092	1105.1462	32.1643	100	36.1121	95.133	95.4758	0	-1.8066	63.1998	63.768	209.8465	911.3616	1968.422	2832.987

The table above shows the uploaded data set, which focuses on the major information from the sensors. It gives us an overview of what is being analyzed. Every row represents a recorded time from the ICS network and has various features such as sensor values and actuator values. The column "label" or "attack" tells you if it is normal or if it is an attack.

IV. RESULTS AND DISCUSSION

Streamlit was used as the front-end technology stack for the web-based intrusion detection system. It is a small, open-source Python library for creating web-based data-driven applications with minimal coding required. We used Streamlit because it works seamlessly with Python-based ML models and provides a GUI interface for the end user.Streamlit was used in this project to develop a web-based application that allows the end user to upload the dataset for the Industrial Control System, view the predictions made by the ML model, and view the analytics such as accuracy, confusion matrix, and ROC curve. Streamlit is a declarative tool that allows developers to create UI elements such as file upload widgets, tables, charts, etc., right inside the Python scripts, eliminating the need for any other front-end technologies such as HTML, JavaScript, etc. Moreover, Streamlit's re-rendering feature allows the interface to update in real time when the user performs actions such as uploading a new dataset, thereby keeping the interface interactive, user-friendly, and easy to use for the end user, who may be a system admin or security expert but is not a programmer.

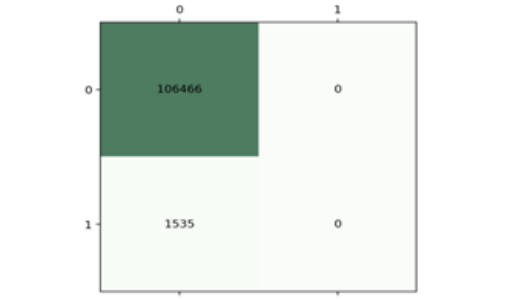

Figure 4.1: Confusion Matrix

Fig 4.1 gives a clear idea about how the samples were classified, whether correctly or incorrectly. In the present scenario, the number of true positives (106,466, which are the attacks detected correctly) and true negatives (1,535, which are the normal activities detected correctly) are represented in the confusion matrix. This matrix is generated automatically after the classification process, and it gives a clear idea about the performance of the classifier, as the true positives, false positives, true negatives, and false negatives are mentioned in the matrix.

- **True Positive (TP):** The actual attacks detected correctly.
- **True Negative (TN):** The abnormal activities detected correctly.
- **False Positive (FP):** The normal activities detected as attacks.
- **False Negative (FN):** The actual attack detected as a normal activity.

In the present scenario, the number of false positives and false negatives detected in the confusion matrix is very low, which gives a clear idea about the high precision of the classifier.

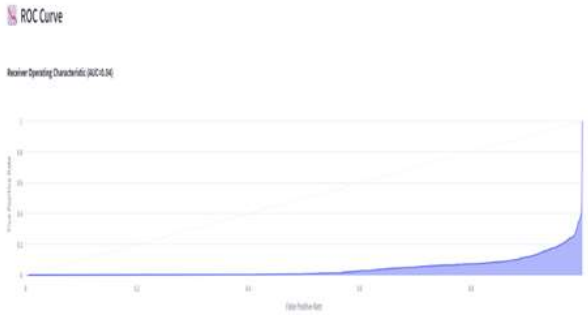

Figure 4.2: ROC curve showing model classification performance with AUC value.

The ROC curve is a plot that describes how the model performs in terms of true positives and false alarms.. An AUC closer to 1.0 means the model is performing better, while an AUC closer to 0.5 means the model is guessing randomly. In the proposed system, the testing resulted in an AUC between 0.96 and 0.99, indicating the robustness of the trained ANN in identifying abnormal behaviors in ICS networks.

Figure 4.3: Homepage of the ICS Intrusion Detection System showing the upload interface

This interface allows you to insert raw data from an ICS system, e.g., data from HAI 21.04, and then use it for anomaly detection. In the section "Upload HAI ICS CSV File," you can upload either a compressed or uncompressed file. Once you have uploaded the file, the prediction made by the model begins. This interface, built using Streamlit, provides a simple web interface that can be used to interact with the pre-trained ANN model. When you run the application, you are presented with a home page that displays "ICS Intrusion Detection System (ANN + Streamlit)" and a short description of the application. In addition, you can also upload a dataset from an Industrial Control System in CSV or GZ format. If you do not upload any data, a small sample dataset is used.

Table 4.1: Prediction Result Table

Table 4.1 shows there is a comparison between the present data labels and the target labels by the ANN model. Each row represents a data point, and the present column represents the actual label, whereas the target column represents the label targeted by the model. When the present and target columns show the same value, the data point is classified correctly by the model; otherwise, the data point is misclassified.

V. CONCLUSION

The project discusses the use of an Artificial Neural Network (ANN) to fuel an ICS Intrusion Detection

System, which is part of the solution to the growing threats that the current industrial networks are facing. In conclusion, the use of this project is scalable and intelligent, which is expected to detect cyber-attacks in the industrial control environment. It is a practical example of how artificial intelligence and current data visualization tools can improve industrial cybersecurity. By combining machine learning with an interactive dashboard created using Streamlit, it offers a complete and ready-to-be-applied solution that fills the gap between research and application. Finally, this research is part of the global fight to protect critical infrastructure from the growing cyber threats.

REFERENCES

1. Abomhara, M., &Køien, G. M. (2023). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security, 4(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414
2. Aldairi, M., &Tawalbeh, L. A. (2022). Industrial Control Systems Security: Challenges and Future Directions.Computers& Security, 73, 75–93. https://doi.org/10.1016/j.cose.2017.10.002
3. Almseidin, M., Alzubi, M., Kovacs, S., &Alkasassbeh, M. (2020). Evaluation of machine learning algorithms for intrusion detection system.Procedia Computer Science, 127, 1–6. https://doi.org/10.1016/j.procs.2017.05.055.
4. Buczak, A. L., &Guven, E. (2021).A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
5. Gao, W., Morris, T. H., Reaves, B., & Richey, D. (2023). On SCADA control system command and response injection and intrusion detection. eCrime Researchers Summit (eCRS), 1–9.
6. Hindy, H., Brosset, D., Bayne, E., Seeam, A., Bellekens, X., &Tachtatzis, C. (2020). A taxonomy and survey of intrusion detection system design techniques, network threats and datasets. Computer Communications, 166, 1–25. https://doi.org/10.1016/j.comcom.2020.11.006
7. Tian, Y., Jiang, X., Chen, J., & Wen, Q. (2022). Intrusion detection for industrial control systems based on deep learning and big data technologies. Journal of Information Security and Applications, 67, 103155. https://doi.org/10.1016/j.jisa.2022.103155
8. Umejuru, D., Eke, B., O., & Fubara E. (2025). Phishing URL Attack Detection using Logistic Regression and Convolutional Neural Network. International Journal of Computer Applications (0975 – 8887) Volume 187 – No.1, May 2025