Data, Information and Computing Science
A. Nayyar et al. (Eds.)

doi:10.3233/ATDE250012

An Intrusion Detection System for Multiclass Classification Across Multiple Datasets in Industrial IoT Using Machine Learning and Neural Networks Integrated with Edge Computing

Tamara ZHUKABAYEVA[a] Zulfiqar AHMAD[b,*] Nurdaulet KARABAYEV[a], Dilaram BAUMURATOVA[a] and Mushtaq ALI[b]
[a] *Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan*
[b] *Department of Computer Science and Information Technology, Hazara University, Mansehra 21300, Pakistan*

Abstract. With the rapid expansion of industrial IoT (IIoT), maintaining robust cybersecurity is essential for the smooth operation of industrial processes. Industrial environments require adaptive solutions to effectively mitigate evolving cyber threats and protect sensitive operations. This research aims to improve the cybersecurity of industrial IoT environments. The research intends to design and implement an adaptive and real-time intrusion detection system with edge computing integration that improves the reliability of the operations in industrial IoT. We incorporated machine learning approaches to classify cyber threats using XGBoost and Deep Neural Networks (DNN). A comparative analysis of results obtained from two datasets shows that the XGBoost model was slightly more accurate than the DNN model, with an accuracy of 79% for dataset D1 and approximately 99.42% for data set D2. This analysis also clearly demonstrates the usefulness of these machine learning approaches and the need to select a model depending on the requirements for detecting particular attacks. Confusion matrix analysis shows that both models have several advantages in terms of recognizing different types of cyber threats.

Keywords. Intrusion detection system, industrial IoT, machine learning, neural network, cybersecurity.

1. Introduction

Industrial Internet of Things (IIoT) is the application of Internet-connected devices and sensors in industries to drive improvements in efficiency and effectiveness. Industrial IoT targets industries include manufacturing, energy, logistics, and smart city industries where big data is gathered from machines, tools, and equipment [1]. For example, in smart grids, IIoT helps the utilities to manage the consumption of electricity as well as distribution in smart cities like Amsterdam by conducting research on the smart meters

* Corresponding Authors: Zulfiqar Ahmad (zulfiqarahmad@hu.edu.pk)

and sensors [2]. Edge Computing is an IT solution that distributes computation processes and keeps locally data processing and storage to reduce latency and bandwidth [3]. In the case of IIoT, edge computing is beneficial as it facilitates decision-making on the real-time data collected at the operational sites of industries [4]. These features include the ability to respond quickly to data sources, data security, and the need to rely less on the central cloud data centers [3]. For example, in a manufacturing plant, far-end devices can obtain data on the running equipment and identify errors that, if corrected locally, do not need to be sent to the cloud system. Some of the participant firms that integrate edge computing in their IIoT systems include Siemens and Honeywell to strengthen production, equipment control, and minimize disruptions [5], [6].

Intrusion attacks in IIoT are highly dangerous to critical industrial sectors like manufacturing industries, power stations, and transportation networks [7]. These attacks can begin with simple hacking, data theft, or more complex attacks that affect operations, compromise safety, and result in major economic losses and include distributed denial of service (DDoS) and advanced persistent threats (APTs) [8], [9], [10], [11]. As the number of connected IIoT devices grows, conventional security measures fail to cope, thus the importance of intrusion detection systems (IDS). Among these trends, machine learning (ML) and neural networks (NNs) are regarded as the most suitable trends in modern IDS development owing to their flexibility and adaptiveness [12], [13], [14].

There are rising security challenges prevalent in IIoT systems. With the industries and other sectors extending their devices and sensors to run critical operations, the instances of cybercrime such as data breaches, DDoS, and malware have increased, which is a threat to important services and has incurred huge financial and machinery losses. Most of the current security measures are inadequate in addressing the challenges posed by IIoT systems in terms of the increasing data intricacy and the volume of data. This study aims at filling these gaps through the development of a more intelligent and efficient IDS that incorporates the application of machine learning and neural networks. Edge computing is necessary to achieve fast feedback and reduce response time and latency in data processing closer to IIoT devices to begin and mitigate the attack. Through this, the study targets multiclass classification on several datasets so that the developed IDS will be able to detect various types of attacks, making it relevant for different industries. The main findings of this research work are as follows:

- We proposed a framework that is tailored to the problem of intrusion detection in IIoT networks.
- We incorporated machine learning and neural networks models in the proposed framework to improve the efficacy of intrusion detection, which enables the multiclass classification of the different types of attacks.
- The proposed study utilizes edge computing principles in that it processes data close to the source, decreasing latencies and bandwidth consumption and increasing the possibility of real-time analysis and faster detection of intrusions.
- The system is designed to handle multiple datasets and classify a wide range of intrusion types, improving the flexibility and applicability of the IDS across different IIoT environments.
- By combining machine learning, neural networks, and edge computing, the system offers real-time detection and proactive prevention of security threats in IIoT systems.

The remaining part of the paper is highlighted as follows: Section II provides related work. Section III describes the proposed framework. Section IV delivers experiments, results, and discussion, while Section V concludes the article.

2. Related Work

We reviewed the existing studies in respect of IIoT, edge computing and intrusion detection systems.

Industry 4.0, or the IIoT, presents manufacturing enterprises with significant opportunities and risks in terms of financial performance [1], [15]. In [1] conducted a literature review and an expert interview to explore the recent innovation in emerging technologies for manufacturing change and the necessary requirements and strategies that manufacturing firms in emerging economies have to adopt to realize this transformation. The research constructed a comprehensive understanding of factors related to IIoT and discovered research directions to enhance the IIoT transition agenda. Many industries incorporate cloud resources and its services to get the related advantages [15]. Almost all the industrial applications incorporate many power-sensitive devices that produce a massive amount of data. This data is referred to as IIoT data and encompasses multi-dimensional information within its pool. Such a massive database is required to be processed carefully to provide fundamental solutions that could revive the system and enhance its performance [1], [15].

The IIoT can be considered a major research subfield of the IoT [9]. The study in [9] includes a review of the literature related to IIoT security, with an emphasis on the years 2017-2023. The authors outline IIoT security threats and categorize them according to the layer through which attackers launch these threats. The authors also describe the security requirements that are violated by these attacks. They discuss how the IIoT can utilize new technologies like AI and edge/fog computing to tackle security issues and improve IIoT security.

IDS are designed to prevent some of the worst kinds of intrusions. IDS works in real time to scan the environment to identify intrusion [16]. It is worth pointing out that the openness of the connection of the devices in the IoT invites cyber incidents [17]. The study in [17] presents a novel next-generation cyber-attack prediction framework for IoT systems. The framework employs the multi-class support vector machine (SVM) and improved CHAID decision tree machine learning techniques. IoT traffic is then analyzed for different types of attacks using a multi-class support vector machine. The SVM model is then tuned using the CHAID decision tree that identifies the most important attributes for the classification of attacks. The effectiveness of the proposed framework was tested on the real dataset of IoT traffic. The results show that the attacks can be classified correctly by using the proposed framework. The framework may identify which attributes are most important for attack classification to improve the precision of the SVM model. The proposed technique deals with network traffic parameters that may be indicators of cyber threats in IoT networks and affected network nodes. The study presented in [18] proposes a robust deep learning model referred as AttackNet for the detection and classification of botnet attacks in IIoT. The model is evaluated using the latest dataset and standard performance evaluation metrics, demonstrating its ability to protect IIoT networks with a testing accuracy of 99.75%, a loss of 0.0063, precision and recall score of 99.75% and 99.74% respectively. Their presented model demonstrates superior accuracy, particularly within the N_BaIoT dataset [18].

3. Edge-Integrated IDS Framework for Multiclass Intrusion Detection in IIoT

The proposed framework as described in figure 1, offers a rich framework for the prevention of intrusion attacks. The framework is to ensure an IIoT environment that works with two datasets, one containing normal network traffic and device behavior and the other containing attack scenarios. These datasets mimic intrusion attacks, including DDoS, unauthorized access, and malware, which are applied to the IIoT environment. The process starts with data gathering from several IIoT devices, where both legitimate and anomalous behavior is observed. Before the actual evaluation of analyzed data, some steps are performed, known as pre-processing, and the most important of them is the data cleaning and normalization as well as feature extraction. Preprocessing is beneficial in getting the data ready for the various machine learning and NN models that follow. The proposed framework uses machine learning and neural networks for intrusion detection. In the machine learning pipeline, we used XGBoost model because of its effectiveness in dealing with the structured data and its effectiveness in identifying complicated patterns that point to cyber threats. In parallel, in the neural network pipeline, a Deep Neural Network (DNN) is applied to further unveil complex correlations in the data for the model to identify complex and new forms of attacks. Edge computing is incorporated into the suggested framework for performing data processing near the data generation point or within the IIoT devices and local edge nodes. This significantly reduces latency, enhances response time, and addresses the issue of bandwidth that would be needed if big data was to be sent to a central cloud. Because all the computations are done locally, the system is capable of providing an immediate reaction to potential threats that are crucial for the protection of critical industrial procedures. In the last step of the proposed IIIoT protection system, data-driven decision making is done, where results from machine learning and the neural network models are used to determine the best course of action to protect the IIoT environment. This makes it possible for the system to change and learn from new threats with a corresponding optimization of the system operational performance by taking immediate action on the detected anomalies. The combined application of edge computing improves the system's capacity to deliver timely, efficient, and flexible intrusion detection across various IIoT deployments.

3.1 Algorithm for IDS with Multiclass Classification Across Multiple Datasets in Industrial IoT

Algorithm 1 gives the steps for deploying IDS in an IIoT setting by using machine learning and artificial neural networks employed in edge computing. The first process of the algorithm is to collect data from the IIoT devices and to preprocess the data for removing inconsistencies, normalizing, and making it ready for analysis. The raw data collected is preprocessed, and then the data are forwarded to edge nodes for real-time processing. The framework utilizes two models: XGBoost and Deep Neural Network (DNN). In real-time mode, the actual data is input through both the models. Depending on what the final detection reveals, the system generates responses; it can be an alert or countermeasure against the threat. It also enables frequent evaluation of the models to provide a reaction to the new threats, and, as a result, the algorithm is also scalable and robust enough to protect important IIoT systems.

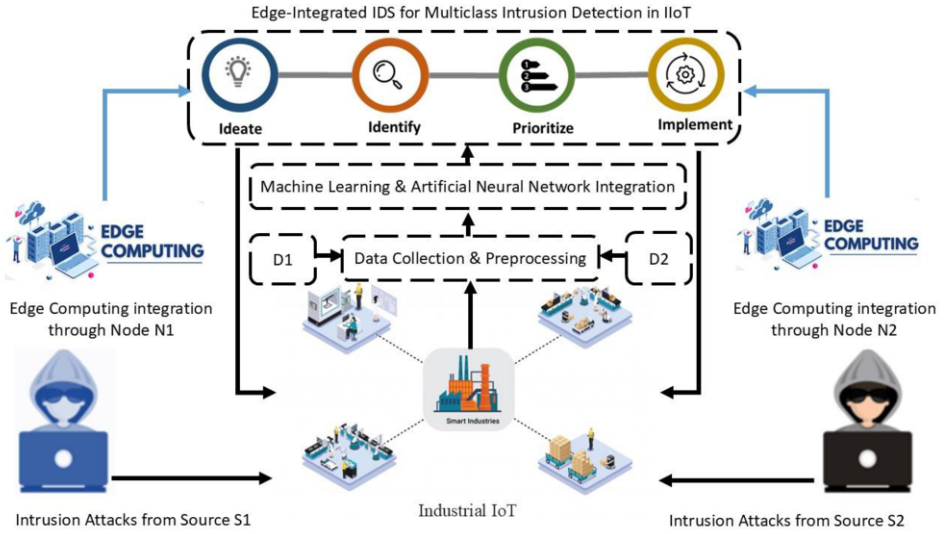

Figure 1: Edge-Integrated IDS Framework for Multiclass Intrusion Detection in IIoT

Algorithm 1: IDS for Multiclass Classification across Multiple Datasets in Industrial IoT

1. ***Begin***
2. **Input:** $D1, D2$: Two IIoT dataset
   A: Set of intrusion attacks
   E: Edge nodes for local data processing
   M_{XGB}: XGBoost Model
   M_{DNN}: Deep Neural Network Model
   T_{Train}, T_{Test}: Training and Testing sets
3. **Output:** Real-time decisions O(t) on intrusion status at time t
4. **Procedure: IDS for Multiclass Classification across Multiple Datasets**
5. **Initialization:**
   - Collect IIoT Datasets D1 & D2
6. **Data Preprocessing:**
   - Feature extraction

   $X = P_{XGB}\ (D1, D2)\ \ for\ XGBoost$
   $Y = P_{DNN}\ (D1, D2)\ \ for\ DNN$
   - Normalization

   $X_{norm} = Normalize\ (X)$
   $Y_{norm} = Normalize\ (Y)$
7. **Edge Computing Integration for Real-Time Processing:**
   - Distributing preprocessed data X_{norm} and Y_{norm} to edge nodes E for processing

   $X_E = E\ (X_{norm})$
   $Y_E = E\ (Y_{norm})$
8. **Models Implementation & Intrusions Detection:**
   - Split the data into training and testing as T_{Train}, T_{Test}

   $T_{Train} = (X_{E,Train}\ , Y_{E\ ,Train}\ )$

$$T_{Test} = (X_{E,Test}\ , Y_{E\ ,Test}\ )$$

- Model Training

$$M_{XGB} \leftarrow Train\ (X_{E,Train}\ , A)$$
$$M_{DNN} \leftarrow Train\ (Y_{E,Train}\ , A)$$

- Intrusion Detection

$$I_{XGB}(t) = M_{XGB}(X_E(t))$$
$$I_{DNN}(t) = M_{DNN}(Y_E(t))$$

9. **Decision Making**
   - Deploy on Edge Devices

$$O(t) = \begin{cases} Normal, & if\ I\ (t) = No\ attack \\ Alert/Countermeasures, & if\ I\ (t) = Intrusion\ Detected \end{cases}$$

10. ***End***

4. Experiments, Results and Discussions

In this study, we evaluate the performance of our proposed IDS using two models: XGBoost and Recurrent Neural Network (RNN), applied to two datasets, D1 and D2. We have used the dataset NF-ToN-IoT-V2 [19] as D1 and dataset Edge-IIoTset Cyber Security Dataset of IoT & IIoT [20] as D2. Both the datasets are publicly available on Kaggle platform. The dataset D1 is from the NFV2-collection compiled by the University of Queensland to eliminate challenges of compatibility in network security datasets to allow for scalability. It is an integrated dataset that aims to replicate the actual IIoT context and includes data of IoT sensors, operating systems, and network traffic. It is labeled for a number of cyber security incidents, including distributed denial of service (DDoS), ransomware, and others. It consists of normal and attack traffic, making it ideal for training machine learning algorithms for intrusion detection and other security-related purposes. The dataset D2 is a well-conceived dataset for cybersecurity in the IoT and IIoT realms. It encompasses a broad spectrum of IoT/IIoT network activities and offers a variety of labeled data to identify security threats and abnormalities. This dataset is particularly useful in training and testing machine learning models that can be used in areas such as intrusion detection, categorization of cyber-attacks, and detection of anomalies in different IoT/IIoT network scenarios.

The evaluation measures that are used to determine the performance of the models include precision, recall, F1 measure, and accuracy measures, which you look at to get to know the predictive nature of the models. We also used confusion matrix to display the performance of the models. The procedure of the experiment includes data preparation and feature scaling of the datasets and model training on the corresponding test samples of D1 and D2. This comprehensive setup will allow evaluating the IDS framework proposed in this paper in detecting intrusions in IIoT scenarios and compare the XGBoost and RNN models' strengths when working with multiple datasets.

In Table 1, the comparison of the performance between XGBoost and DNN on Dataset D1 shows that XGBoost yields a better result than DNN for most classes, including DOS, injection, and password attacks. Precision and recall values according to F1-score are high for benign traffic 1.00, backdoor 1.00, and ransomware 1.00. DNN fails in several cases, including DOS, scanning, and XSS, and has zero recall, which significantly drops the macro and weighted averages. This difference shows that although DNN can be used for identifying normal traffic, it is significantly less effective

for certain forms of malicious traffic, which might restrict its effectiveness in strong anomaly detection systems. As it can be seen from Table 2, even for dataset D2, both XGBoost and DNN yield nearly perfect accuracy of around or more than 99% for most of the classes. XGBoost stays slightly ahead, especially in identifying classes such as port scanning and ransomware, for which DNN has slightly lower recall and F1-scores. The proposed DNN achieves reasonable accuracy and reasonably high precision, recall, and F1-scores for important classes, including DDoS_TCP and DDoS_HTTP. The high accuracy achieved by both models in Dataset D2 is due to the relatively simpler attacks to detect as opposed to those in D1, for which DNN proved to have blind spots in specific classes.

When comparing the results from both Table 1, using the D1 dataset, and Table 2, using the D2 dataset, both models have high precision, recall, and F1-score on dataset D2 for each class in the model assessment, and XGBoost and DNN outcompeted all other models.

Table 1: Classification report for Dataset D1

Class	Precision		Recall		F1-score		Accuracy	
	XGBoost	DNN	XGBoost	DNN	XGBoost	DNN	XGBoost	DNN
Benign	1.00	0.98	0.99	0.97	1.00	0.97	0.79	0.70
dos	0.80	0.00	0.97	0.00	0.88	0.00		
injection	0.65	0.60	0.48	0.89	0.55	0.72		
ddos	0.97	0.74	0.63	0.76	0.76	0.75		
scanning	0.65	0.00	0.65	0.00	0.65	0.00		
password	0.47	0.32	0.53	0.14	0.49	0.19		
mitm	0.97	0.56	0.97	0.03	0.97	0.06		
xss	0.53	0.00	0.66	0.00	0.59	0.00		
backdoor	1.00	1.00	1.00	0.98	1.00	0.99		
ransomware	1.00	0.00	1.00	0.00	1.00	0.00		
Macro Avg	0.80	0.42	0.79	0.38	0.79	0.37		
Weighted Avg	0.80	0.62	0.79	0.70	0.79	0.65		

Table 2: Classification report for Dataset D2

Class	Precision		Recall		F1-score		Accuracy	
	XGBoost	DNN	XGBoost	DNN	XGBoost	DNN	XGBoost	DNN
Backdoor	1.0000	1.0000	0.9367	0.9853	0.9673	0.9926	0.9942	0.9931
DDoS_HTTP	0.9934	0.9916	1.0000	1.0000	0.9967	0.9958		
DDoS_ICMP	1.0000	1.0000	1.0000	0.9993	1.0000	0.9997		
DDoS_TCP	1.0000	1.0000	1.0000	0.9881	1.0000	0.9940		
DDoS_UDP	0.9997	1.0000	1.0000	1.0000	0.9998	1.0000		
Normal	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000		
Password	0.9990	1.0000	0.9930	0.9818	0.9960	0.9908		
Port_Scanning	0.9965	0.9435	1.0000	1.0000	0.9983	0.9710		
Ransomware	0.9448	0.9985	0.9863	0.9673	0.9651	0.9827		
SQL_injection	1.0000	0.9900	1.0000	0.9990	1.0000	0.9945		

Uploading	0.9880	0.9995	1.0000	0.9990	0.9940	0.9992		
Vulnerability_scanner	0.9970	0.9964	0.9995	0.9787	0.9983	0.9875		
XSS	0.9995	0.9796	0.9960	0.9965	0.9978	0.9880		
Macro Avg	0.9937	0.9922	0.9932	0.9919	0.9933	0.9920		
Weighted Avg	0.9943	0.9934	0.9942	0.9931	0.9941	0.9932		

It is revealed that XGBoost is slightly more accurate and precise than DNN, particularly in different classes such as port scanning and ransomware, for which DNN has lower recall values. This suggests that dataset D2 may contain more identifiable attack patterns, which could enable both models to make better predictions. The high level of accuracy in the classification of benign traffic and other simple attacks such as DDoS and SQL injection also demonstrates that Dataset D2 is less complex than Dataset D1.

Figure 2 and Figure 3 show the performance of XGBoost and DNN on Dataset D1. Both models have high prediction strength in identifying the Benign class and the Injection class, with XGBoost showing better overall accuracy across some attack classes.

Figure 2: Confusion matrix for XGBoost with dataset D1

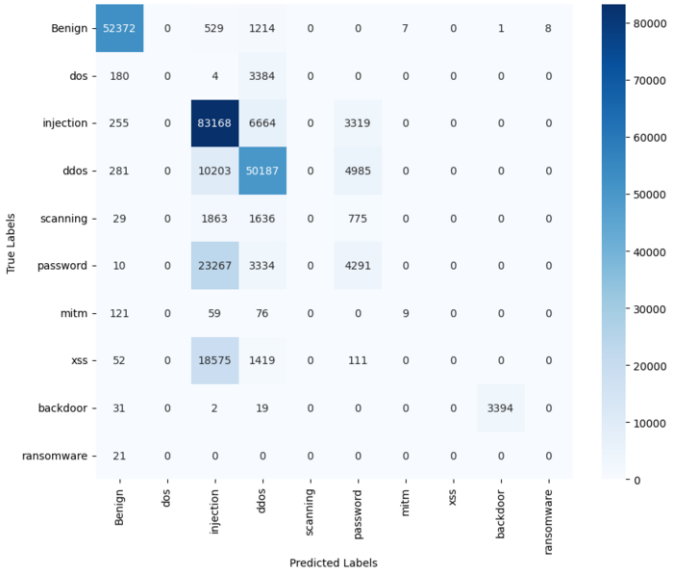

Figure 3: Confusion matrix for DNN with dataset D1

According to Figure 2, which is heavy on the benign, injection, and backdoor attacks (presumably resulting in greater miss-classifications), the XGBoost model can do a better job than other models. Still, a bit of confusion exists while classifying similar classes like DDoS and Scanning, as hundreds of instances are misclassified between these two classes. On the other hand, in Figure 3(DNN), again the model does well on benign and injection classes, but their performance dropped down mainly for rare attacks such as DOS, scanning, and MITM. For these attacks, the failure rate is higher in the DNN model than XGBoost; this could mean specific patterns of certain attack types are hard to distinguish by the neural network, particularly if their feature distributions overlap. Which means that DNN is technically more robust, but XGBoost provides higher overall precision and better ability to handle specific (small size) classes, particularly in detecting more subtle types of attacks. In general, both models work well for bigger classes, but XGBoost seems to do better at more diverse attack types.

Figures 4 and 5 present the confusion matrices for the XGBoost and DNN models applied to dataset D2, respectively, showcasing their performance in multiclass classification tasks related to network intrusion detection.

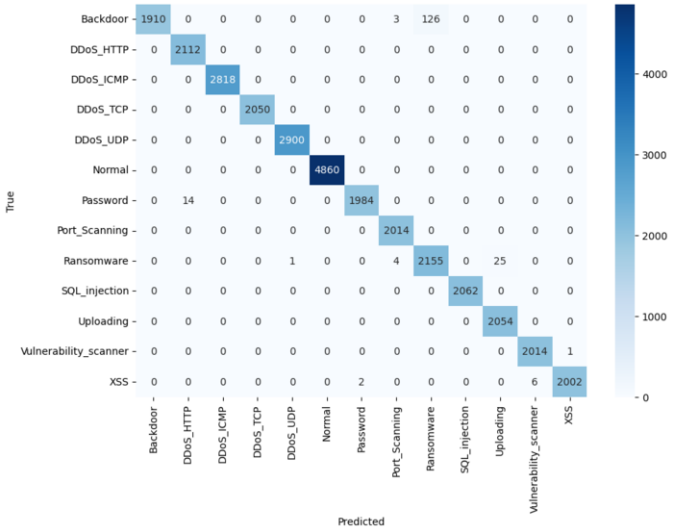

Figure 4: Confusion matrix for XGBoost with dataset D2

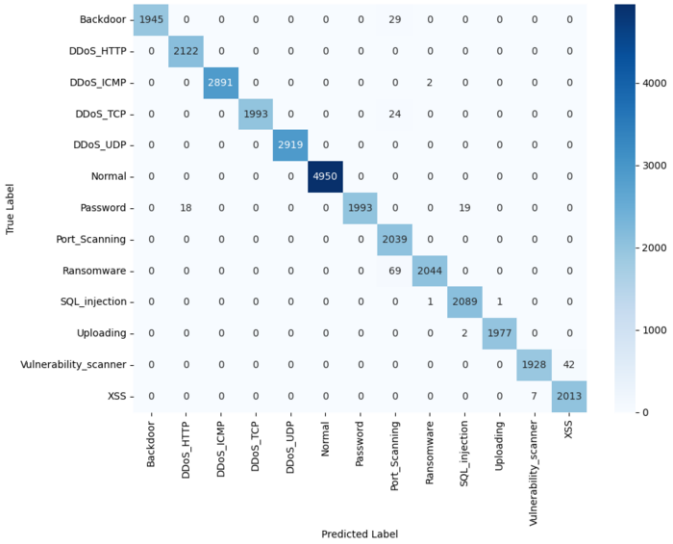

Figure 5: Confusion matrix for DNN with dataset D2

Figure 4 reveals that the model has effectively classified most instances across various attack types, particularly excelling in detecting the Normal and SQL_injection classes, which have the highest true positive counts. However, it does show some challenges, particularly with the Ransomware and Uploading classes, which experience several misclassifications. This can be attributed to the inherent complexities of these classes, as they often share features with other types, leading to confusion. In contrast, Figure 5 (DNN) exhibits an overall strong performance, with particularly high accuracy in identifying Normal traffic, similar to the XGBoost model. However, the DNN struggles more with distinguishing Backdoor and XSS attacks, as evidenced by the higher false positive rates in these categories. This suggests that while DNNs can model

intricate relationships in data, they may require further tuning or additional data for effective differentiation among closely related classes. The comparative analysis indicates that while both models perform well, they exhibit different strengths and weaknesses. XGBoost appears more reliable in identifying certain attack types, while the DNN shows a more balanced performance across various classes.

The comparative analysis of the XGBoost and DNN model results in the proposed framework for cybersecurity in Industrial IoT shows notable characteristics that stress the merits and demerits of each method. For Dataset 1 (D1), the performance of the XGBoost model was quite high, reaching almost 96.5% accuracy, with the parameters of benign traffic being 1.00 and 0.88 F1 score for DoS attacks. The performance of the DNN model resulted in a general accuracy of about 94%, while the benign traffic had a precision of 0.98 and the DoS Attack F1 score was 0.70. This difference indicates that while both models are robust, D1 XGBoost relatively outperforms the other in detecting and classifying the different types of attacks.

Results are similar to what is observed from D1, but with fewer such differences while exploring Dataset 2 (D2). They had reached accuracy scores of about 99.7% with the XGBoost model, but this was not the case for the XGBoost model; however, it still showed enhanced results around 99.4% accuracy and high metrics such as 1.00 precision for correct predictions of normal traffic in XSS attacks. The DNN model achieved a good accuracy with about 93.1% with several categories such as password (0.99) and ransomware (0.98) have better recall, indicating that in specific attack patterns it might be more sensitive, followed by an increase in false positive rate.

This study emphasizes the role of machine learning in the reinforcement of IDS capabilities and could lead to hybrid techniques combining models to benefit from their identified traits. The performance discrepancies between the two datasets indicate that model hyperparameter tuning and feature engineering can help to solve the issue of varying types of attacks. The results from this study are interesting as both XGBoost and DNN demonstrate high classification performance of cyber threats in the dataset used; the choice of the model seems to be dependent on system requirements. XGBoost, on the other hand, might be suitable for environments wherein a fine level of accuracy is needed in determining benign activities.

5. Conclusion

The study examines the improvement of cybersecurity approaches in industrial IoT spaces using modern machine learning procedures. This paper used XGBoost and DNN to perform a comparative analysis in the classification for several types of cyber threats, highlighting the importance of a machine learning approach about construction adaptive real-time intrusion detection systems. The framework intends to enhance the effectiveness of detection without generating false positives, thereby maintaining the system integrity and dependability of industrial IoT. Consistent with current research recommending that intelligent systems will be essential for cyber security to keep pace with the increasing sophistication of cyber threats.

The results from this comparative analysis showed that the XGBoost model has surpassed DNN model accuracy and precision in both datasets. Notably, for Dataset 1, the XGBoost model outperformed DNN with an accuracy of around 96.5% as compared to that of a slightly less accurate (94%) DNN and perform well on Dataset 2, clocking an impressive accuracy of around 99.4%. The obtained results demonstrate that the

proposed machine learning techniques are efficient; however, they also suggest the necessity of selecting models according to relevant attack detection needs. We provide the insights from the confusion matrices, which give a clear understanding of how the models perform in identifying different types of attacks, explaining further that we can strengthen our cybersecurity in industrial IoT environments by utilizing these algorithms.

In the future, we aim to focus on the implementation of hybrid models to improve performance and robustness against various cyber threats. We also aim to make research on the effect of emerging attack vectors on model responses, verifying that cybersecurity solutions are adaptable as well as resilient to continuous technological advancements.

Acknowledgment

This research has been funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No AP23489127).

References

[1] O. Peter, A. Pradhan, and C. Mbohwa, "Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies," *Procedia Comput. Sci.*, vol. 217, pp. 856–865, 2023, doi: 10.1016/j.procs.2022.12.282.

[2] N. Sahani, R. Zhu, J.-H. Cho, and C.-C. Liu, "Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey," *ACM Trans. Cyber-Physical Syst.*, vol. 7, no. 2, pp. 1–31, Apr. 2023, doi: 10.1145/3578366.

[3] M. Babar, M. S. Khan, U. Habib, B. Shah, F. Ali, and D. Song, "Scalable Edge Computing for IoT and Multimedia Applications Using Machine Learning," *Human-centric Comput. Inf. Sci.*, vol. 11, 2021, doi: 10.22967/HCIS.2021.11.041.

[4] Q. N. Minh, V.-H. Nguyen, V. K. Quy, L. A. Ngoc, A. Chehri, and G. Jeon, "Edge Computing for IoT-Enabled Smart Grid: The Future of Energy," *Energies*, vol. 15, no. 17, p. 6140, Aug. 2022, doi: 10.3390/en15176140.

[5] K. Cao, S. Hu, Y. Shi, A. Colombo, S. Karnouskos, and X. Li, "A Survey on Edge and Edge-Cloud Computing Assisted Cyber-Physical Systems," *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7806–7819, Nov. 2021, doi: 10.1109/TII.2021.3073066.

[6] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge-Computing-Enabled Smart Cities: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10200–10232, 2020, doi: 10.1109/JIOT.2020.2987070.

[7] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 2019, pp. 305–310. doi: 10.1109/CCWC.2019.8666450.

[8] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *J. Cloud Comput.*, vol. 7, no. 1, pp. 1–20, 2018, doi: 10.1186/s13677-018-0123-6.

[9] B. Alotaibi, "A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities," *Sensors*, vol. 23, no. 17, p. 7470, Aug. 2023, doi: 10.3390/s23177470.

[10] A. Akbarzadeh, L. Erdodi, S. H. Houmb, and T. G. Soltvedt, "Two-stage advanced persistent threat (APT) attack on an IEC 61850 power grid substation," *Int. J. Inf. Secur.*, vol. 23, no. 4, pp. 2739–2758, Aug. 2024, doi: 10.1007/s10207-024-00856-6.

[11] Y. Mei, W. Han, S. Li, K. Lin, Z. Tian, and S. Li, "A Novel Network Forensic Framework for Advanced Persistent Threat Attack Attribution Through Deep Learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 9, pp. 12131–12140, Sep. 2024, doi: 10.1109/TITS.2024.3360260.

[12] U. AlHaddad, A. Basuhail, M. Khemakhem, F. E. Eassa, and K. Jambi, "Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks," *Sensors*, vol. 23, no. 17, p. 7464, Aug. 2023, doi: 10.3390/s23177464.

[13] A. Corallo, M. Lazoi, M. Lezzi, and P. Pontrandolfo, "Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level," *IEEE Trans. Eng. Manag.*, vol. 70, no. 11, pp. 3745–3765, Nov. 2023, doi: 10.1109/TEM.2021.3084687.

[14] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.*, vol. 114, p. 103165, Jan. 2020, doi: 10.1016/j.compind.2019.103165.

[15] R. Kumar and N. Agrawal, "Analysis of multi-dimensional Industrial IoT (IIoT) data in Edge–Fog–Cloud based architectural frameworks : A survey on current state and research challenges," *J. Ind. Inf. Integr.*, vol. 35, p. 100504, Oct. 2023, doi: 10.1016/j.jii.2023.100504.

[16] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "An effective intrusion detection approach based on ensemble learning for IIoT edge computing," *J. Comput. Virol. Hacking Tech.*, vol. 19, no. 4, pp. 469–481, Dec. 2022, doi: 10.1007/s11416-022-00456-9.

[17] S. Dalal *et al.*, "Next-generation cyber attack prediction for IoT systems: leveraging multi-class SVM and optimized CHAID decision tree," *J. Cloud Comput.*, vol. 12, no. 1, p. 137, Sep. 2023, doi: 10.1186/s13677-023-00517-4.

[18] H. Nandanwar and R. Katarya, "Deep learning enabled intrusion detection system for Industrial IOT environment," *Expert Syst. Appl.*, vol. 249, p. 123808, Sep. 2024, doi: 10.1016/j.eswa.2024.123808.

[19] Kaggle, "NF-ToN-IoT-V2." Accessed: Aug. 16, 2024. [Online]. Available: https://www.kaggle.com/datasets/dhoogla/nftoniotv2/data

[20] Kaggle, "Edge-IIoTset Cyber Security Dataset of IoT & IIoT." Accessed: Aug. 20, 2024. [Online]. Available: https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot