Journal of Information Systems Engineering and Management
2025, 10(26s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CNN-RGU Hyperparameter Tuning for Improving Cybersecurity Intrusion Detection in Industrial IOT Environment

Ahmed Zaki Wafi [1,2], Mohsen Nickray [3]

[1] PhD Student, College of Computing and IT Engineering, Information Technology Department, University of Qom, Baghdad, Iraq.
[2] Assistant Lecturer, College of Science, Uruk University, Baghdad, Iraq.
[3] Professor, College of Computing and IT Engineering, Information Technology Department, University of Qom, Iran.
*Corresponding Author: eng.ahmed9113@gmail.com

ARTICLE INFO

Received: 30 Dec 2024

Revised: 22 Feb 2025

Accepted: 04 Mar 2025

ABSTRACT

Internet of Things (IoT) has revolutionized the manufacturing and industrial sectors by simplifying and making operations more productive. It consists of a networked ecosystem of smart machines, advanced data analytics, and workforce convergence within the workplace. The convergence yields increased production efficiency, improved quality monitoring and control, and improved worker and machine operator safety. However, ensuring security from cyber-attacks and intrusion detection in IoT environment has become a critical concern for modern industries. In recent years, we have witnessed the creation of intrusion detection systems with targeted solutions. To address these challenges, this paper focuses on hyper parameters' optimization of CNN-GRU using Grey Wolf Optimization (GWO) detecting normal sessions and attack attempts within an IoT environment. Our experimental findings confirm the efficiency of the optimized CNN-GRU model, which outperforms recent comparative studies in performance measures like accuracy, precision, recall, F1-score, and detection cost. Especially, the GWO-optimized GRU model outperforms the CNN-GRU model in multi-class traffic classification with 99% accuracy, 97% F1-score, 98% precision, and 96% recall.

Keywords Internet of Things (IoT), Gray Wolf Optimization, CNN-GRU, Infiltration, Cybersecurity

INTRODUCTION

The Internet of Things (IoT) refers to the concept of connecting devices to the internet and other connected devices. It is also a massive network of interconnected things and individuals, all of which collect and share data about their usage and surrounding environments. Essentially, anything that can be connected to the internet can be considered part of the IoT [1]. The IoT introduces numerous opportunities and technical challenges across various domains, particularly in the industrial sector [2,3]. One of its key applications is in industry, where the Industrial Internet of Things (IIoT) specifically connects a diverse set of devices or objects with unique identifiers and standardized communication protocols. This enables seamless interoperability among IoT-enabled industrial devices, fostering a highly integrated and efficient system [4]. The term Industrial Internet of Things (IIoT) refers to a network of thousands of smart devices, ranging from tiny temperature sensors in industrial settings to advanced equipment in satellite engines. These devices, all equipped with high-precision sensors, collect data and transmit it over the internet to remote computing systems, where advanced processing and analysis take place. This technology is designed based on a "retrofit and reuse" approach, moving away from the traditional "rip and replace" model. This shift is critical for modern industries, as it not only enhances production efficiency but also reduces errors, improves security, and lowers costs. Additionally, it enables fast and efficient decision-making with minimal human intervention. The IIoT has unlocked new opportunities across various fields, including engineering, power systems, irrigation, transportation, and other critical infrastructures. To maximize the benefits of this technology, companies must leverage robust cloud infrastructures for data storage, processing, and analysis, utilizing advanced artificial intelligence (AI) techniques. In recent years, several sectors—such as water and electricity management, smart agriculture, coal mining, and data security—have successfully leveraged this technology. For instance, in agriculture, IoT technology allows farmers to monitor their fields in real-time, tracking weather conditions and soil moisture levels to increase crop yield and efficiency [5].

Today, smart refrigerators have entered the market, offering not only exceptional quality but also internet connectivity. One of the most notable features of these refrigerators is their ability to monitor stored food items and notify users of expiration dates. Similarly, companies can utilize IIoT technology to predict the lifespan of machines and equipment, monitor production processes, and optimize human resource management. A key application of the Internet of Things (IoT) in the power industry is cost reduction. In traditional energy management, significant wastage of resources and energy occurs, which is particularly critical given the current challenges faced by many countries. One of the primary reasons for adopting IoT in various industries is to enable more efficient energy management. In fact, IoT-driven solutions for the power sector help organizations significantly reduce maintenance and operational costs. As a result, IIoT technology is shaping a new era of real-time application management in complex industrial environments [6]. Despite the growing importance of the Industrial Internet of Things (IIoT) and its critical applications in industry, security concerns have not received sufficient attention from manufacturers and users. As a result, many of these devices have become tempting targets for attackers, who may seek to carry out sabotage or gain access to sensitive information. A review of various sources reveals that a significant number of IIoT devices are publicly accessible on the internet without the necessary security measures in place to protect them [7]. Cyberattacks can have severe consequences in general, but when industrial systems are targeted, the impact can be catastrophic. Such attacks may range from stealing confidential information to causing severe damage to industrial equipment. For instance, if an attacker gains control over the actuators of an industrial system, they could potentially inflict physical harm on personnel and create dangerous situations [8]. Each of these scenarios can have catastrophic consequences. For example, Stuxnet has the potential to trigger a "new Chernobyl" by disrupting industrial control systems at nuclear power plants. While this represents an extreme and critical scenario, even less severe attacks can lead to significant economic damage, especially due to disruptions in the production process or the leakage of vital intellectual property information. This issue has been exacerbated in recent years by modern manufacturing trends, particularly when the disclosure of settings for a connected device can lead to the leakage of sensitive information about products created by reconfigurable manufacturing systems [9]. Industrial devices require advanced Intrusion Detection Systems (IDS) capable of conducting high-accuracy data analysis and ensuring the security levels of the systems [10,11]. These IDS systems play a critical role as an integral part of information security systems, with their primary function focusing on detecting anomalies and threats within the system. To perform this task, IDS typically rely on two main approaches: knowledge-based detection and anomaly-based detection. In the knowledge-based method, also known as signature-based detection, a database containing attack patterns and stored signatures is used to identify malicious behaviors. In this approach, incoming network traffic is compared to stored signatures to determine if there is any indication of known attacks. However, it is important to note that this method has inherent limitations and may not detect zero-day attacks. In contrast, the anomaly-based detection method utilizes statistical techniques or machine learning algorithms to analyze user behavior and network activity in order to identify potential attacks [12].

LITERATURE REVIEW

Rangwani et al. [13]: In this study, a three-factor authentication protocol with privacy preservation and strong security for the Industrial Internet of Things (IIoT) is designed to counter all existing security attacks. The design has been evaluated using both informal and formal security reviews, including well-known random oracle models and BAN logic, and has been analyzed through the ProVerif simulation. The results show that this protocol is completely secure against all existing security threats. In terms of performance, it has also been proven that the proposed design is not only lighter but also more efficient than other similar designs.

Babiciano et al. [14]: This research addresses the issue of cyber resilience protection in the Industrial Internet of Things (IIoT). The proposed approach is based on a software-defined network architecture, which shifts data management to a centralized and logical control panel. This structure allows for customized planning based on the specific needs of each application. From a security perspective, such an architecture implies that anyone with access to the software- managing computers controlling the network could potentially dominate the entire network. The paper introduces an experimental platform based on SDN and a hybrid ontology of cyber resilience and cybersecurity, which can be used to document the requirements for the design phases of virtual manufacturing networks. Additionally, it presents a framework for cyber resilience protection mechanisms in virtual manufacturing applications. Finally, the paper concludes by addressing the need for future research to implement the proposed framework.

Romero et al. [15]: In this study on security in the Industrial Internet of Things (IIoT), the C-SEC approach is utilized, which provides simple, flexible, and repeatable evaluations to support decision-making in cybersecurity related to emerging technologies.

Wang et al. [16]: To improve the accuracy in identifying malicious traffic in Internet of Things (IoT) devices, a hybrid model is proposed, combining Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) for intrusion detection. A comparative analysis is presented at the end, showing that the proposed model not only guarantees high accuracy but also requires less processing time compared to other methods. The results indicate that the proposed method performs better in terms of accuracy and recall metrics when compared to classic intrusion detection algorithms in the field of IoT.

Tao Nguyen Da et al. [17]: This research presents an innovative approach for fault detection in industrial diesel generators, which is designed based on a hybrid deep learning algorithm (CNN-BGRU). The proposed algorithm combines a Convolutional Neural Network (CNN) with a Bidirectional Gated Recurrent Unit (BGRU) to extract deep features from long and sequential historical signals and classify anomalous conditions. To accurately evaluate the performance, experiments were conducted at three sampling frequencies of 10 seconds, 20 seconds, and 30 seconds. The results analysis, using various metrics, shows that the proposed method exhibits comparable or even superior performance to other traditional deep learning algorithms, including RNN, CNN, GRU, LSTM, BRNN, and BGRU methods.

Muhammad Ishaq , Ibrahim Khan et al. [18]: In this study, which focuses on TCP flood attack detection in Internet of Things (IoT) devices using deep learning models, a hybrid CNN-GRU deep learning model is proposed. The model is designed and tested on 9 different IoT devices. For this purpose, a dataset based on Narrowband IoT devices (N-BaIoT), including Bashlite and Mirai, is created to detect software attacks such as the TCP flood attack. The main focus of the research is on detecting TCP flood attacks, with the goal of achieving minimal error and maximum accuracy in real-time data corresponding to each of these 9 devices. This study provides a comprehensive framework that utilizes advanced deep learning and AI-based algorithms to effectively and efficiently detect unknown patterns in the data and identify flood attacks in IoT devices.

Zhai et al. [19]: In a study on intrusion detection in smart grid environments, an intrusion detection model with a local training process based on Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), called CNN-GRU-FL, is designed. Using an attention mechanism, the ability to extract and describe features is enhanced, and a new method for parameter aggregation is proposed to improve the model quality under conditions of data quality and volume differences. Additionally, a trust-based node selection mechanism is designed to enhance convergence in Federated Learning (FL). The experimental results show that the proposed method effectively creates a global intrusion detection model across multiple independent entities. The training accuracy, recall rate, and other metrics reached 78.79%, 64.15%, and 76.90%, respectively. The improved mechanism enhances the performance and efficiency of parameter aggregation under varying data quality conditions.

Table 1 Comparative analysis of related works

S.NO.	Authers	Methodology	IOT	Security	Task Allocation	Fog Computing	Cloud Computing	Optimization
1	Rangwani	Random Oracle and BAN Logic	Iiot	Yes	NO	NO	NO	No
2	Babisiano	SDN and a hybrid ontology of cyber resilience and cybersecurity	Iiot	Yes	NO	NO	NO	No
3	Romero	C-SEC	Iiot	Yes	NO	NO	NO	C-SEC approach

4	Wang	CNN-RNN	IOT	Yes	NO	NO	NO	CNN-RNN Neural networks
5	Thao Nguyen	CNN-BGRU	NO	Yes	NO	NO	Yes	CNN-BGRU Neural networks
6	Ishaq	CNN-GRU	IOT	Yes	NO	NO	NO	CNN-GRU Neural networks
7	Zhai	CNN-GRU-FL	IOT	Yes	NO	NO	Yes	CNN-GRU-FL Neural networks

A comparative analysis of related works is presented in Table 1, which indicates that the main focus of the research has been on security and optimization through neural networks and deep learning. Traditional methods, such as the Oracle Random Model and BAN Logic (as in Rangwani's study), have solely addressed security, while more recent studies (such as those by Wang, Nguyen, Isaac, and Zhai) have utilized deep learning algorithms (e.g., CNN-RNN, CNN- BGRU, CNN-GRU, and Federated Learning) for optimizing security and detecting cyber threats. Additionally, cloud computing has been employed in some studies, but fog computing has not been utilized in any of these works. This trend reflects the growing importance of artificial intelligence and deep learning in optimizing security and processing data within the Industrial Internet of Things (IIoT).

METHODS

Test environment settings

his research was conducted in the MATLAB R202X environment on a system with the following specifications:

- Processor (CPU): Intel Core i7/i9
- Memory (RAM): 16GB
- Graphics Processing Unit (GPU): NVIDIA
- Operating System: Windows 10/11

Additionally, this MATLAB version provides the necessary capabilities for deep learning, parallel processing, and the implementation of the proposed algorithms. The utilized toolboxes include:

- Deep Learning Toolbox: For designing and training the CNN-GRU network
- Optimization Toolbox: For certain optimization operations
- Parallel Computing Toolbox: If parallel processing is used to accelerate learning
- Custom Implementation of GWO: Implementation of the Grey Wolf Optimizer (GWO) algorithm in MATLA.

The various stages of the proposed method are presented in Figure (1). As illustrated in this figure, the proposed method consists of the following steps:

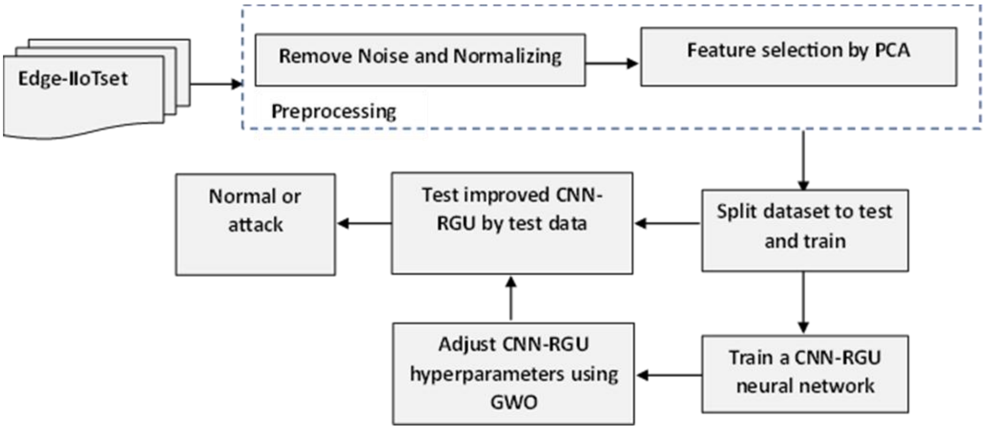
Edge-IIoTset
Remove Noise and Normalizing
Feature selection by PCA
Preprocessing
Normal or attack
Test improved CNN-RGU by test data
Split dataset to test and train
Adjust CNN-RGU hyperparameters using GWO
Train a CNN-RGU neural network

Figure 1. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications: Centralized and Federated Learning | IEEE Data Port

Dataset Selection

The first step in building a successful intrusion detection system is selecting an appropriate dataset. Both benign and malicious session records must be included in the dataset to simulate the variety of records that the model will encounter in real-world scenarios. In this study, the Edge-IIoTset dataset (Table 2) is utilized, which is a benchmark dataset for intrusion detection in Industrial Internet of Things (IIoT). This dataset can be used by machine learning-based intrusion detection systems in two different modes: centralized learning and federated learning. The IIoT data is generated from various IoT devices (more than 10 types), such as: Low-cost digital sensors for measuring temperature and humidity, Ultrasonic sensors, Water level detection sensors, pH sensors, Soil moisture sensors, Heartbeat sensors, Flame sensors, etc. The dataset includes various cyber-attacks, such as: reconnaissance attacks, man-in-the-middle (MITM) attacks, injection attacks, malware-based attacks. Additionally, the dataset provides features extracted from multiple sources, including: alerts, system resources, logs, and network traffic. From the 1,176 identified features, 61 highly correlated features have been selected for use in the model.

Table 2 Part of the Edge-IIoTset dataset

	A	B	C	E	F	H	I	G	K
	http.respone	tcp.ack	tcp.ack_raw	tcp.check sum	tcp.connection.fin	tcp.connection.rst	tcp.connection.syn	tcp.connection.synack	tcp.dsport
1	0	1	1.75E+09	1681	0	0	0	0	80
2	0	836202	1.14E+09	59281	0	0	0	0	5900
3	0	1	1.68E+09	51038	0	0	0	0	1883
4	0	1	1.78E+09	2122	0	0	0	0	1883
5	0	0	0	0	0	0	0	0	0
6	0	6	4.06E+09	13429	0	0	0	0	1883
7	0	5	1.79E+09	39965	0	0	0	0	1883
8	0	561452	2.37E+09	30032	0	0	0	0	60944
9	0	87	3.15E+09	28558	0	0	0	0	39234

Feature Selection (PCA algorithm)

Specific features are selected to reduce the dimensionality of the dataset using the Principal Component Analysis (PCA) algorithm. Utilizing all features for intrusion detection classification is generally not effective. When developing a robust and efficient statistical model, not all features have equal importance or weight. Some features are highly informative and significantly contribute to the model's predictions, playing a crucial role in classification accuracy. In contrast, others hold less value and have minimal impact on the model's performance. Therefore, it is essential to refine the feature set. In the second stage of the proposed method, feature selection is performed using the classical PCA feature selection algorithm.

Splitting the dataset for testing and training

For training and evaluating neural networks, it is essential to split the data into two main parts, training and testing, to ensure that the model learns effectively and generalizes well to new data. The training set allows the model to identify patterns and relationships within the data and adjust its parameters accordingly. In contrast, the test set contains unseen data that is used to evaluate the model's performance on unknown inputs. This separation prevents overfitting (overlearning from the training data) and ensures the model's ability to generalize its knowledge to real-world or new data.

Adjust CNN-RGU hyperparameters using GWO

Tuning the hyperparameters of the CNN-RGU neural network is crucial to achieving optimal performance in learning and generalization. Hyperparameters such as the number of convolutional layers, filter sizes, learning rate, the number of recurrent units in the RGU section, and the number of epochs can significantly affect the model's accuracy and efficiency. If these parameters are not properly set, the model may suffer from phenomena such as overfitting or underfitting, resulting in poor performance on new data. Given the vast search space for these hyperparameters, manual or experimental methods may be inefficient, making automated and intelligent optimization approaches highly valuable. One powerful optimization method that can be used for automatic hyperparameter tuning is the Grey Wolf Optimizer (GWO) algorithm. Inspired by the hunting behavior and social hierarchy of grey wolves, this metaheuristic optimization algorithm can be used to search for optimal values in the complex hyperparameter space. By leveraging its hierarchical structure and modeling the interactions between leaders and group members, GWO can efficiently explore the search space. Its ability to avoid local optima and achieve fast convergence makes it an effective approach for tuning the hyperparameters of neural networks.

Test improved CNN-RGU by the test data

Testing the CNN-RGU neural network using the test dataset, as the final step in the flowchart, is performed to evaluate the model's real-world performance. In this stage, the trained model is executed on unseen data to assess its ability to generalize and make accurate predictions. The test dataset is statistically similar to the training data but has not been used during training. Metrics such as accuracy, F1-score, precision, and recall are calculated to evaluate the model's performance. This step ensures that the improved model has learned correctly and can provide reliable results in real-world scenarios or on new data.

RESULTS

In this section, the performance of the proposed method is evaluated against the baseline method based on four criteria: Accuracy, F1-score, Precision, and Recall. The obtained results are presented in Figure 2,3.

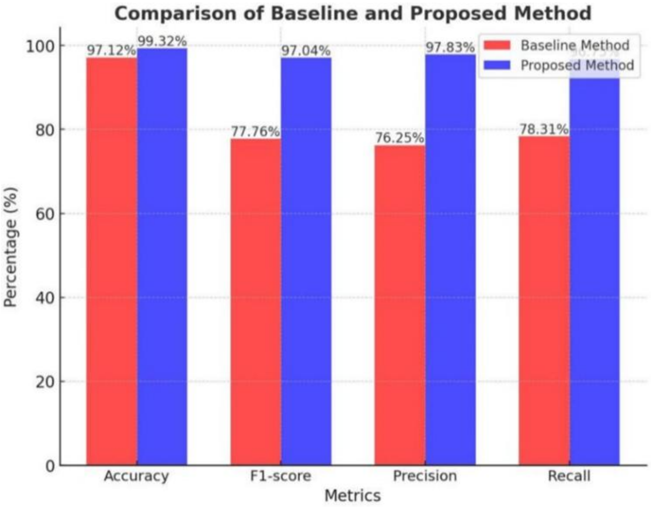

Figure 2 Results chart of the proposed method and the baseline method

- **Accuracy**

As shown in Figure 2,3 the accuracy of the proposed method is 99.3199%, whereas the baseline method achieved an accuracy of 97.1194%. This ≈2.2% improvement demonstrates the effectiveness of optimizing the model’s weights and hyperparameters using the Grey Wolf Optimizer (GWO) algorithm.

- **F1-score**

The F1-score balances Precision and Recall, providing an overall evaluation of the model’s performance in distinguishing positive and negative samples. The results indicate that the F1- score of the proposed method is 97.0365%, compared to 77.7584% for the baseline method—an≈19.3% increase. This improvement highlights the proposed model's enhanced capability in reducing the misclassification rate of both positive and negative samples.

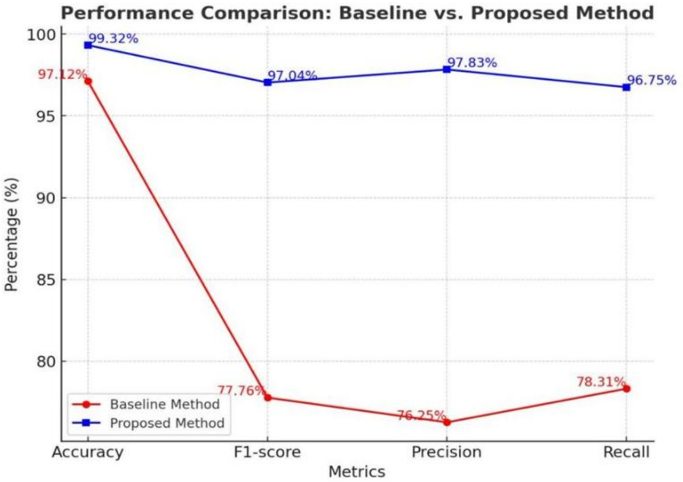

Figure 2 Results chart of the proposed method and the baseline method

- **Precision**

Precision represents the ratio of correctly predicted positive samples to the total predicted positive samples. According to Figure 2,3, the Precision of the proposed method is 97.8334%,

while the baseline method achieves 76.2499%. The ≈21.5% increase in this metric indicates that the proposed method has a lower error rate in positive predictions and demonstrates higher reliability compared to the baseline approach.

- **Recall**

Recall measures the model’s ability to correctly identify positive samples from the total actual positive samples. According to Figure 1, the Recall of the proposed method is 96.7524%, whereas the baseline method achieves 78.3074%. This ≈18.4% improvement indicates that the proposed method outperforms the baseline approach in correctly identifying positive instances.

- **Overall Performance Improvement**

The significant improvements in Accuracy, F1-score, Precision, and Recall demonstrate that integrating the CNN-GRU network with the Grey Wolf Optimizer (GWO) has led to a substantial enhancement in deep learning model performance. These results confirm that employing GWO for optimizing weights and hyperparameters has effectively improved the model’s efficiency compared to the baseline method. Furthermore, ANOVA (Analysis of Variance) results indicate that the performance difference between the proposed method and the baseline method is statistically significant (p-value < 0.05), confirming the reliability of the observed improvements. Therefore, utilizing GWO as an optimization technique can significantly enhance accuracy while reducing error rates in CNN-GRU hybrid models.

DISCUSSION

In this study, we examined the CNN-GRU neural network, optimized using the proposed Grey Wolf Optimizer (GWO). Based on the results and tables in the previous section of the paper, our findings demonstrate that integrating CNN-GRU with GWO has significantly improved model performance. Optimizing the parameters using GWO led to higher accuracy and enhanced key evaluation metrics, including F1-score, Precision, and Recall. Compared to other optimization approaches, GWO-based weight tuning for CNN-GRU has made the model more resistant to local optima and more robust against improper hyperparameter settings.

CONCLUSION

Overall, the findings of this study demonstrate that optimizing the CNN-GRU model using the Grey Wolf Optimizer (GWO) significantly enhances accuracy and improves model performance. Comparisons with previous methods indicate that this approach can serve as an effective solution for optimizing deep learning models across various applications. However, to further improve efficiency and reduce computational costs, future research should explore the integration of multiple metaheuristic algorithms and leverage distributed computing techniques to enhance optimization performance.

REFRENCES

[1] Collier, S.E. The Emerging Enernet: Convergence of the Smart Grid with the Internet of Things. IEEE Ind. Appl. Mag. 2017, 23, 12–16. [CrossRef]

[2] Chang, T.; Tuset-Peiro, P.; Vilajosana, X.; Watteyne, T. OpenWSN & OpenMote: Demo'ing a Complete Ecosystem for the Industrial Internet of Things. In Proceedings of the IEEE International Conference on Sensing, Communication, and Networking (SECON), London, UK.

[3] Petersen, S.; Carlsen, S. WirelessHART versus ISA100.11a: The format war hits the factory floor. IEEE Ind. Electron. Mag. 2011, 5, 23–34. [CrossRef].

[4] Peter Wegner. 1996. Interoperability. ACM Computing Surveys (CSUR) 28, 1 (1996), 285–287.

[5] Johannes Vrana and Berlin DGZfP. 2019. NDE 4.0: The Fourth Revolution in Non-Destructive Evaluation: Digital Twin, Semantics, Interfaces, Networking, Feedback, New Markets and Integration into the Industrial Internet of Things.

[6] Gordon S Blair, Massimo Paolucci, Paul Grace, and Nikolaos Georgantas. 2011. Interoperability in complex distributed systems. In International School on Formal Methods for the Design of Computer, Communication and Software Systems. Springer, 1–26.

[7] Roland Bodenheim, Jonathan Butts, Stephen Dunlap, and Barry Mullins. Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. International Journal of Critical Infrastructure Protection, 7(2):114–123, 2014.

[8] Sujit Rokka Chhetri, Nafiul Rashid, Sina Faezi, and Mohammad Abdullah Al Faruque. Security trends and advances in manufacturing systems in the era of industry 4.0. In Proc. of IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2017.

[9] Erik Puik, Daniel Telgen, Leo van Moergestel, and Darek Ceglarek. Assessment of reconfiguration schemes for Reconfigurable Manufacturing Systems based on resources and lead time. Robotics and Computer- Integrated Manufacturing, 43:30–38, 2017.

[10] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. Security and Privacy Challenges in Industrial Internet of Things. In Proc. of the 52nd IEEE/ACM Design Automation Conference (DAC), page
54. ACM.

[11] Jianxiong Liao,Jie Hu,Peng Chen,Hanming Wu,Maoxuan Wang,Yuankai Shao &Zhenguo Li. et al. Prediction of transient emission characteristic from diesel engines based on CNN-GRU model optimized by PSO algorithm. Pages 1800-1818 | Received 14 Aug 2023, Accepted 07 Nov 2023, Published online: 21 Jan 2024. https://doi.org/10.1080/15567036.2024.2302376.

[12] Chuan Lin 1ORCID,Kailiang Weng 1,2,*ORCID,Youlong Lin 3,Ting Zhang 1,Qiang He 2 andYan Su. et al. Time series prediction of dam deformation using a hybrid STL–CNN–GRU model based on sparrow search algorithm optimization 2022, 12(23), 11951; https://doi.org/10.3390/app122311951.

[13] Rangwani, D., Sadhukhan, D., Ray, S. et al. A robust provable-secure privacy-preserving authentication protocol for Industrial Internet of Things. Peer-to-Peer Netw. Appl. 14, 1548–1571 (2021). https://doi.org/10.1007/s12083-020-01063-5

[14] Radu F. Babiceanu, Remzi Seker. et al. Cyber resilience protection for industrial internet of things: A software-defined networking approach Computers in Industry. Volume 104, January 2019, Pages 47-58. https://doi.org/10.1016/j.compind.2018.10.004

[15] Romero-Mariona J., Hallman R., Kline M., San Miguel J., Major M. and Kerr L. (2016). Security in the Industrial Internet of Things - The C-SEC Approach . In Proceedings of the International Conference on Internet of Things and Big Data - Volume 1: IoTBD, ISBN 978-989-758-183-0, pages 421-428. DOI: 10.5220/0005877904210428.

[16] Zhaolian Wang, Hong Huang *, Rui Du, Xing Li, Guotao Yuan. et al. IoT Intrusion Detection Model based on CNN-GRU. Frontiers in Computing and Intelligent Systems. Vol. 4, No. 2, 2023 ISSN: 2832-6024.

[17] Thao Nguyen Da , Phuong Nguyen Thanh , Ming-Yuan Cho. . et al. Novel cloud-AIoT fault diagnosis for industrial diesel generators based hybrid deep learning CNN-BGRU algorithm. Internet of Things Volume 26, July 2024, 101164

[18] Muhammad Ishaq; Ibrahim Khan; Syed Irfan Ullah; Tahseen Ullah . et al. TCP Flood Attack Detection on Internet of Things devices using CNN-GRU Deep Learning Model. Islamabad, Pakistan. 23 November 2023. 10.1109/ICoDT259378.2023.10325694

[19] by Feng Zhai 1,2ORCID,Ting Yang 1ORCID,Hao Chen 2,Baoling He 3 andShuangquan Li . et al. Intrusion Detection Method Based on CNN–GRU–FL in a Smart Grid Environment. Electronics 2023, 12(5), 1164; https://doi.org/10.3390/electronics12051164

[20] Rui Li, Mingtao Wang, Xingyu Li, Jian Qu, Yuhan Dong. et al. Short-term photovoltaic prediction based on CNN-GRU optimized by improved similar day extraction, decomposition noise reduction and SSA optimization. 24 January 2024 https://doi.org/10.1049/rpg2.12934