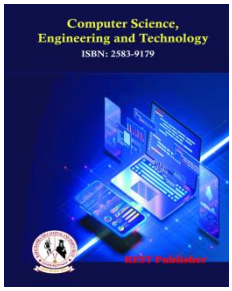
Computer Science, Engineering and Technology

Vol: 2(3), September 2024

REST Publisher; ISSN: 2583-9179 (Online)

Website: https://restpublisher.com/journals/cset/

DOI: https://doi.org/10.46632/cset/2/3/1



Leveraging Deep Learning for Intrusion Detection in Industrial IoT Landscapes

Vismaya KK, *P. J Arul Leena Rose

SRM IST Kattangulathur, Chennai, Tamil Nadu, India.

**Corresponding Author Email: leena.rose527@gmail.com*

Abstract. *The security of linked devices and systems has become a top priority due to the Industrial Internet-of-Things' (IIoT) rapid expansion. The identification and prevention of any intrusions that might compromise the availability and integrity of IIoT networks is one of the major difficulties in this field. The exploration of Deep Learning (DL) architectures for Intrusion Detection Systems (IDS) in IIoT contexts has been driven by their promising findings in a variety of cybersecurity applications. This survey explores and evaluates the current deep learning architectures utilized for IIoT intrusion detection in order to provide an overview of them. It also points out possible areas that need improvement. This article evaluates the durability, performance, and adaptability of several deep learning (DL) methodologies, including hybrid architectures, recurrent-neural-networks (RNNs), deep-neural-networks (DNNs) and convolutional-neural-networks (CNNs), in the context of IIoT environments.*

Keywords: *Industrial-Internet-of-things-(IIOT), Deep Learning, Intrusion-Detection-System-(IDS).*

1. INTRODUCTION

Industrial processes have undergone a change with the spread of IIoT, resulting in a new era of automation, efficiency, and connection. However, intrusion detection is a crucial component of IIoT security since this interconnection presents previously unseen cybersecurity dangers [1]. The dynamic nature of cyber threats makes traditional methods unable to keep up, which makes the investigation of cutting- edge technologies like Deep Learning (DL) necessary. Due to DL's impressive performance across a range of domains, researchers are looking into how it might improve IIoT network security.

The purpose of this survey is to systematically investigate and assess the use of DL architectures for IIoT intrusion detection. IIoT presents unique issues that require specific solutions because of its unique characteristics, which include real-time limits, resource limitations, and varied communication protocols [2]. A wide range of DL architectures, such as CNNs, DNNs, and hybrid models, are covered in the paper. Providing information on these designs' efficacy, suitability for IIoT contexts, and general state of the art is the aim. This survey looks at some of the available literature to find trends, problems, and areas that still need to be researched.

Additionally, by outlining prospective directions for innovation and enhancement in the use of DL for IIoT intrusion detection, it seeks to direct future research efforts. In order to offer flexible, scalable, and proactive intrusion detection systems, cutting-edge deep learning techniques will need to be combined with industrial cybersecurity requirements as IIoT continues to advance.

2. BACKGROUND

A. ***Industrial Internet of Things (IIOT):*** The Industrial Internet of Things (IIoT) represents an innovative bringing together of advanced digital technologies and traditional manufacturing. IIoT in industrial settings is defined by the extensive integration of sensors and devices that are thoughtfully included into machinery and

equipment. Real-time data collection is made possible by this network of connections, and sensors that measure vibration, pressure, and temperature. CoAP and MQTT are two examples of robust communication protocols and data connectivity that allow for easy information sharing. IIoT uses sophisticated analytics, such as AI and machine-learning, to extract insightful information for uses like process optimization and predictive maintenance.

The paradigm also enables remote monitoring and control, giving operators the ability to monitor industrial processes from any location with internet connectivity. The idea of Cyber-Physical Systems (CPS), in which physical and computational systems are tightly integrated to improve adaptability and autonomy, is fundamental to the IioT [4]. Figure.1 shows the connectivity of IIOT, The Internet of Things has security concerns despite these benefits, which emphasizes how important it is to have strong cybersecurity defences like intrusion detection and prevention in place to guarantee the safety, accessibility, and integrity of industrial data. It is crucial to find a balance between innovation and cybersecurity as industry embrace IIoT more widely in order to fully realize the potential of this revolutionary technology.

B. ***Security Challenges in IIOT:*** Numerous security challenges have been caused by the Industrial Internet of Things (IIoT) Figure.2, and practical examples show how urgent it is to address these problems. Consider the malware that was employed in the 2010 Stuxnet attack, which was intended to attack industrial systems, especially those found in nuclear power plants. Stuxnet demonstrated the possibility for physical consequences from a digital breach in addition to highlighting the susceptibility of vital infrastructure to highly skilled cyberattacks. A cyberattack on the Ukraine power grid in 2015 brought out energy for over 200,000 people.

The impact of IIoT security vulnerabilities in the real world was demonstrated by the attackers, who took advantage of weaknesses in the linked systems within the industry. Moreover, ransomware assaults such as the 2017 WannaCry attack focused on manufacturing and healthcare institutions, demonstrating the widespread nature of cyber dangers across all industries. These instances highlight the necessity of strong cybersecurity safeguards in the IIoT since breaches can have severe consequences, compromising not just data but also operations and even posing a risk to public safety. IIoT security offers ever- changing issues that necessitate constant innovation and adaptation in cybersecurity tactics in order to stop and reduce new and emerging threats.

c. ***Importance of Intrusion-Detection in IIoT:*** The significance of intrusion detection in the context of the Industrial Internet of Things (IIoT) cannot be emphasized. Because IIoT environments are networked and frequently crucial, they are ideal targets for cyber assaults. Robust intrusion detection systems serve as vigilant protectors, constantly scanning the extensive network of sensors and devices for indications of malicious behavior. The importance of intrusion detection in IIoT is demonstrated by real-world incidents like the 2017 petrochemical plant attack by the Triton malware.

The goal of this attack was to manipulate industrial safety systems, which put human safety and operational integrity at serious danger. Another major example is the 2016 Mirai botnet assault, which demonstrated the potential for significant disruptions by taking advantage of weak IIoT devices. In addition to rapidly recognizing and resolving such threats, intrusion detection is essential for preserving the dependability and robustness of IIoT systems in the face of constantly changing cyber threats.

d. ***Challenges in Traditional Intrusion Detection Systems:*** Safeguarding Industrial Internet of Things (IIoT) environments presents a number of issues for traditional intrusion detection systems (IDS). Since traditional IDS are usually made for more standardized networks, there are compatibility problems due to the variety of devices and communication protocols found in IIoT ecosystems [3]. In addition, traditional IDS may find it difficult to collect and evaluate the increasing quantity of data produced by networked devices due to the scalability requirements of IIoT deployments. The difficulty is made worse by the need for real-time IIoT operations. Conventional intrusion detection systems may not be able to meet the strict latency requirements, which could cause a delay in the detection and reaction to security problems.

Another challenge is the inherent resource limitations of many IIoT devices, which result in traditional intrusion detection systems using excessive resources or being unable to adjust to changing IIoT network topologies. Because encrypted communications are so common, it might be difficult for typical intrusion detection systems to scan them for any threats. Furthermore, the diverse behaviors of IIoT systems make it difficult for conventional IDS to reliably distinguish between normal and abnormal activity. Innovative strategies suited to

the particularities of IIoT environments are needed to address these issues. Examples include investigating sophisticated anomaly detection methods and adaptable security measures.

e. ***Deep Learning in Cyber Security:*** Deep Learning (DL), which provides advanced abilities for threat detection, anomaly identification, and pattern recognition, is essential to improving cybersecurity measures [6]. Intrusion Detection Systems (IDS) are one prominent cybersecurity use of deep learning (DL), where DL models are able to understand complex patterns and behaviors to identify both known and unknown threats. Deep Neural Networks (DNNs) are one example of how DL is useful in reducing cybersecurity threats. DNNs have been used to detect malicious activity in network data.

Malware detection is one more application area. To find malware variants that have never been seen before, DL models—in particular, Recurrent Neural-Networks (RNNs and) Convolutional Neural-Networks (CNNs) can examine file properties and behavior. Because deep learning can automatically identify relevant components from data, it is very useful in addressing the constantly changing cyber threat landscape [5].

Additionally, DL is used in email security to thwart phishing scams. To discern between emails that are malicious or legitimate, deep learning models can examine email headers, content, and sender behavior. For example, Google's Gmail uses DL algorithms to improve its spam filtering, which lowers the chance that users would fall for phishing scams [7]. DL is used in the field of online security to find vulnerabilities and harmful activity. Online application firewalls monitor online traffic using DL models to spot and stop possible security risks like cross-site scripting and SQL injection. Because it can adjust to typical user and system behavior, DL is also useful in behavior analytics. It is possible to identify any deviations from the established patterns as possible security incidents. This is especially helpful for insider threat detection, where the goal is to find unusual activity occurring inside a company.

To put it briefly, the integration of deep learning (DL) into cybersecurity procedures improves the capacity to identify and address a variety of cyber threats, offering a more flexible and proactive safeguard against the constantly shifting field of malicious action.

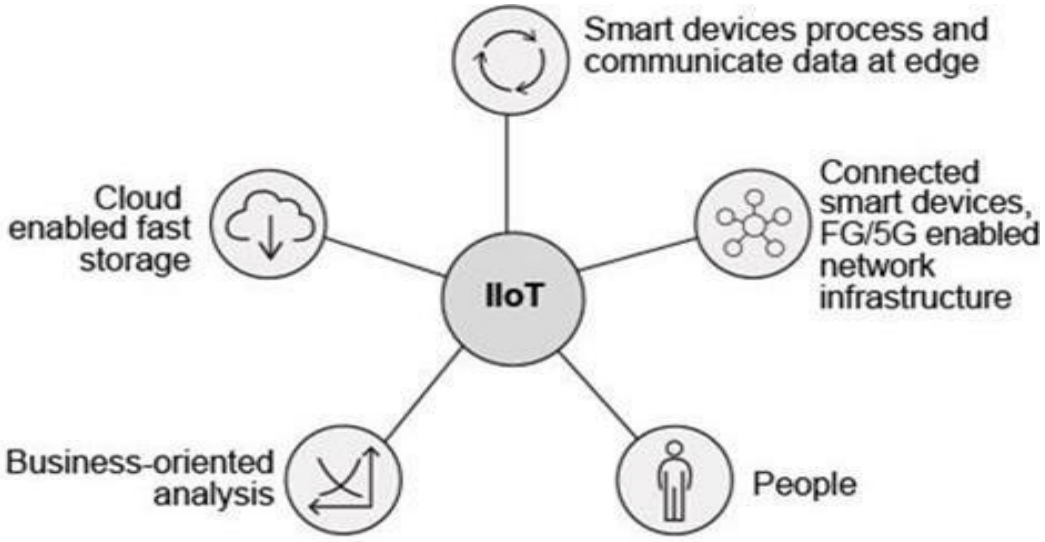


FIGURE 1. Industrial Internet of Things

3. LITERATURE REVIEW

TABLE 1. Literature Review

Year	RF.NO	Method	Dataset	Metric	Result
2024	8	DNN	CICIDS, NSL-KDD	Accuracy(ACC)	ACC 99.68%
2024	9	Transfer learning(TL) and CNNs architecture	CICIDS-2017, 2018 and UNSW-NB15	Accuracy	ACC for CICIDS 2017-98.98% CICIDS 201.8- 99.13% UNSW-NB15- 99.89%
2024	10	CGL-DNN	NSL-KDD CICIDS-2017	Accuracy	ACC for NSL-KDD: 0.83 ACC for CICIDS-2017: 0.84
2024	11	Evaluated Bird - SwarmOptimization based Deep Belief Network (EBSO-DBN)	NSL-KDD	Accuracy Detection Rate False Positive rate	ACC 98.75% DR 98.9% FPR 93.21%
2024	12	IDQN	NSL-KDD, UNSW-NB15, IDS2018.	Accuracy	ACC 98.85%
2024	13	DNN, 2D-CNN,1D-CNN	NSL-KDD new, UNSW_NB15new	Accuracy	NSL-KDD new: ACC 0.99 UNSW_NB15new: ACC 0.80
2024	14	DL-SkLSTM (Deep Learning- Stacked Long Short-Term Memory)	Edge_IIoT	AccuracyF1 Score Detection Rate Precision	ACC: 98.30% F1 Score: 98.46% DR: 98% PR: 99.43%
2024	15	CNN, GA	Edge_IIoT	AccuracyF1 Score Recall Precision	ACC: 97.17% F1 Score: 96.86% Recall: 97.17% PR: 97.33%
2024	16	Gated-Attention Dual Long –Short Term Memory	TON-IOT, NSL-KDD	Accuracy	TON-IOT ACC: 98.76% NSL-KDD ACC: 99.65%
2023	17	CNN, LSTM	KDDCUP99, UNSW_NB15 , NSL-KDD	Accuracy False Positive-Rate(FPR)Detection-rate(DR)	For KDDCUP99 the ACC, DR, FPR 0.9705, 0.9998, 0.0059 respectively.For NSL-KDD the ACC, DR, FPR 0.999, 0.999, 0.0029 respectively. For UNSW_NB15 the ACC, DR, FPR 0.9443, 0.935, 0.0397
2023	18	XAI based Bi-LSTM	NSL-KDD, Honeypot	Accuracy Detection Rate	Accuracy-98.2% DR for honeypot-97.2% NSL-KDD- 95.8%
2023	19	CNN-LSTM	CICIDS-2017	AccuracyRecall	Accuracy 95.21% Recall 82.59%
2022	20	CNN, CNN-1D	HEIDS	AccuracyF1 Score Recall Precision	Accuracy: 1.000 F1 Score: 1.000 Recall: 1.000 Precision: 1.000
2021	21	DFFNN, ANN	UNSW NB15,NSL-KDD	Accuracy False Positive Rate Detection-rate	For NSL-KDD: ACC, DR, FPR is 99.0%, 99.0%, 1.0% For UNSW-NB15: ACC,DR, FPRis 98.9%, 99.9%, 1.1%
2021	22	BBFO(ANN)-GRU	NSL-KDD,CICIDS	Accuracy	Accuracy 98.45%

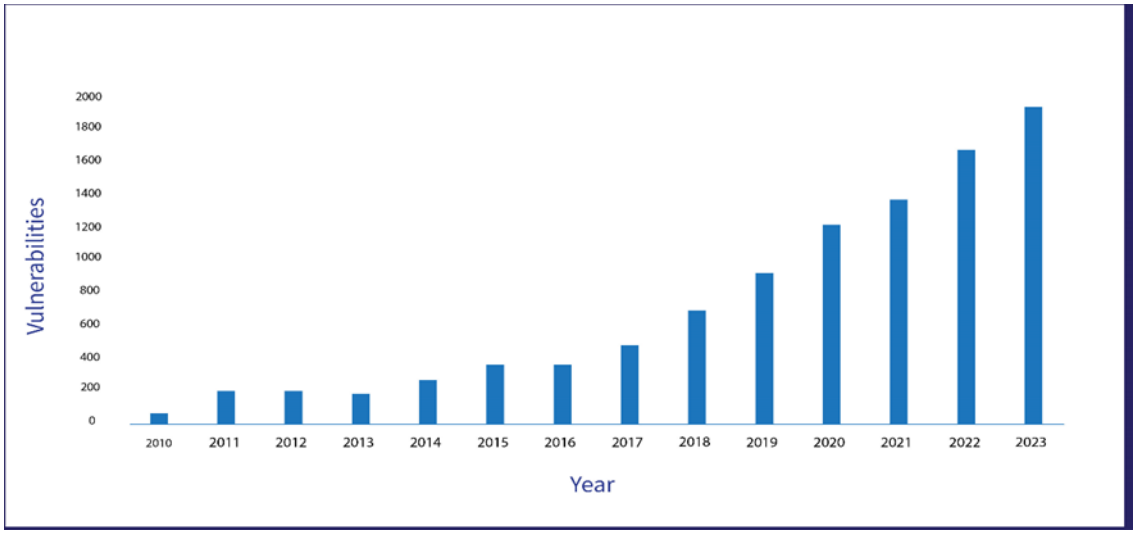


FIGURE 2. Vulnerabilities in IIOT

TABLE 2. Datasets

DATASET	ATTACKS	Publishedyear	No Of Features
TON-IOT	Reconnaissance, DDoS, XSS, verification, , Passwordcracking attacks, Injection attacks, Ransomware, DoS, Backdoors, and Man in the middle	2020	Win 7: -132 Network: -42 Win 10:- 124
CICIDS-2017	Web attack, infiltration, DoS ,Botnet, Heart-bleedand DDoS, Brute force.	2017	80
UNSW-NB15	Analysis, Backdoors, Fuzzers, Worms, Generic,Shell-code, DoS-Exploits and Reconnaissance.	2015	49
BOT-IOT	DDoS, Service Scanning DoS, OS Finger-printing,Key-logging, Data Theft.	2019	29
NSL-KDD	DoS, U2R, PROBE, R2L ,	2009	41

4. FINDINGS AND LIMITATIONS

In this section, we will examine the results of our investigation in more detail. We are able to recognize the significant facts and trends that emerged due to this thorough analysis in Table 1 and to understand about the datasets used in IIOT described in Table 2 provides a platform for future discussions and applications. The K-means clustering technique and neural networks were used by the authors in [8] to create a hybrid classifier. They compare the classifiers' performances with the NSL- KDD and KDD'99datasets. The Deep Belief Network's performance improved with the application of an optimization technique. With a loss of 0.0102, the Deep Neural Network model achieved an accuracy score of 99.68%. When the CICIDS 2017 dataset was used, the trustworthy security model (TSM) for IIoT attacks on industrial robots is proposed by the authors in [9]. An enhanced deep Q-network (IDQN) and a control model are integrated by the TSM. With a low latency of 0.01s, the TSM achieves a high detection rate of 98.7%. The TSM offers a way to quickly and precisely detect IoT assaults on industrial robots. A security methodology for identifying

intrusions in 5G and IoT networks is presented by the authors in [12]. The hybrid model and deep learning are used in the suggested framework. The CICIDS-2017, 2018, and UNSW-NB15 datasets were used for the simulation, and time-series to image transformation was used to turn the datasets into image datasets. On IDS datasets, binary and multi-class classification was also carried out. The suggested hybrid model performed better in MCC, accuracy, and precision than the current models. In order to overcome class imbalance, the research [10] suggests a hierarchical clustering approach for under sampling. To get rid of feature interference and redundancy, an ideal feature selection method based on greedy thinking is presented. A proposal has been made fora deep neural network intrusion detection model that relieson the simultaneous connection of global and local sub-networks. The suggested techniques enhance Industrial Internet of Things (IIOT) intrusion detection. However, there are significant restrictions, such as a sharp disparity in the quantity of samples across the dataset's various classifications. The samples contained redundant and nonsensical features, and standard intrusion detection

techniques were unable to match the increasingly sophisticated IIOT's requirements for detection accuracy. Paper [13] conducted a systematic literature review on MLDL techniques for intrusion detection systems. Explored the importance of security and privacy in IoT networks. They highlighted about how ineffective signature-based intrusion detection systems are in identifying novel or zero-day threats, and how ineffective it is to store attacks in databases for Internet of Things networks. Also computation for devices in IoT networks is in efficient. A methodology for IIoT intrusion detection utilizing ensemble learning, hyper parameter tuning, and DTL was presented in Paper [15]. They trained using the Edge- IIoT set dataset and seven effective CNN architectures. It fared better in terms of attack detection accuracy than the most advanced IDS. [21] Paper with a 99.0% detection rate and 1.0% false alarms, the proposed ADS model performs well. Feature selection using hybrid rules enhances the consistency of the model. 99.0% detection rate, 99.0% accuracy and 1.0% FPR were achieved on the NSL-KDD dataset. 99.9% detection rate, 98.9% accuracy and 1.1% FPR were obtained on the UNSW-NB15 dataset. They listed restrictions such the need for low false alarm rate and high detection accuracy, the difficulty of gathering data for the creation of intelligent NIDS, and the difficulties of identifying both new and current assaults. Additionally, they emphasized the significance of quick and accurate cyber threat warning in key infrastructures. The proposal in Paper [19] Self-similarity Integration in SCADA systems, the Hurst parameter combined with the CNN-LSTM model improves anomaly detection. The hybrid model produced a 95.21% detection accuracy and an 82.59% recall rate. They mentioned difficulties such as complicated model integration and dataset constraints.

Paper [11] The classification method known as EBSO- DBN yielded results with 99.4% precision, 98.7% accuracy, and 98.8% recall. A 93.21% false alarm rate and a 98.9% detection rate were shown by the suggested model. They had to deal with issues like incomplete study of DBNs, insufficient focus on rectifying imbalanced cyber-security datasets, and evaluation metrics that were limited to accuracy alone—recall and precision were not discussed. A Honeypot Early Intrusion Detection System (HEIDS) utilizing deep learning methods is proposed in the study [20]. Convolutional neural networks with one dimension are used to create the HEIDS model (CNN 1D). HEIDS has considerably increased its accuracy in identifying and classifying anomalies in IIoT networks. In terms of accuracy, the HEIDS dataset performs better than other reference datasets. The NIDS-CNNLSTM model, which has a low false alarm rate and a good detection and classification accuracy, was proposed in Paper [17]. When used to large-scale, multi-scenario network data, it works well. The intrusion detection method suggested in Paper [18] yields detection rates of 95.8% and 97.2%. For feature selection, the Bidirectional- Long-Short-Term Memory based Explainable- Artificial- Intelligence (BiLSTM-XAI) framework was used, and the krill herd optimization(KHO) technique was applied. The use of hybrid metaheuristic techniques to identify unknown hostile attacks is part of future work. The authors of Paper [14] introduced a 5G threat detection DL model with a dense layer and classifier to identify and classify cyberattacks. They also used AI and stacked LSTM. Using the publicly accessible Edge-IIoT set dataset, the model was tested and found to have a 98% detection rate and 98.30% accuracy. A novel BBFO-GRU model for security and robustness in industrial CPS was developed in Paper [22]. The NADAM approach and the BBFO algorithm enhance detection performance. The proposed model's accuracy in detecting intrusions in industrial CPS was 98.45%. Gated- Attention Dual-Long and Short-Term Memory (Dugat- LSTM), a deep-learning based network intrusion detection system, was designed for attack classification in Paper [16]. The TON-IOT dataset yields an accuracy of 98.76% for the suggested model. The suggested method achieves an accuracy of 99.65% on the NSL-KDD dataset. The method outperforms other models in use today in terms of accuracy and robustness.

5. FUTURE DIRECTION

Future research opportunities hold promise for further advancements in intrusion detection systems (IDS) inside Industrial Internet of Things (IIoT) contexts, given the substantial efforts being made in this area. Investigating novel solutions to enduring problems like feature duplication, class disparity, and the inadequacy of traditional methods is one possible direction. Techniques including ensemble learning, hyper parameter tuning, deep transfer learning, and optimal feature selection have the ability to reduce these problems and raise intrusion detection system accuracy. Enhancing model integration is also a priority in order to guarantee efficient deployment and operation in sophisticated industrial networks. Furthermore, in order to strengthen the security of IIoT environments, more research should be done on cutting- edge techniques and new technologies. Through the adoption of these problems and opportunities, researchers can further advance IIoT intrusion detection techniques, thereby augmenting the resilience of vital infrastructures against dynamic cyber threats.

6. CONCLUSION

The literature analysis concludes by highlighting the notable developments made in intrusion detection systems (IDS) for Industrial Internet of Things (IIoT) contexts. By combining advanced algorithms, hybrid models, and

deep learning techniques, researchers have shown substantial improvements in efficiency and accuracy in detection. Furthermore, the emergence of specialized security models—like the proposed TSM—highlights the possibility of customized solutions to deal with certain IIoT security issues. However, issues including class imbalance, feature repetition, and dataset restrictions still exist and call for more research. The field of IIoT intrusion detection seems to have a bright future despite these obstacles, with chances to experiment with novel strategies and take advantage of cutting-edge technologies. Stakeholders may improve the security architecture of IIoT ecosystems by tackling these issues and adopting novel approaches to research.

REFERENCES

[1]. Verma, P., & Bharot, N. (2023). A Review on Security Trends and Solutions Against Cyber Threats in Industry 4.0. ICSCCC 2023 - 3rd International Conference on Secure Cyber Computing and Communications, 397–402. https://doi.org/10.1109/ICSCCC58608.2023.10176999

[2]. Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J. P. C., & Park, Y. (2020). Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges. In IEEE Access (Vol. 8, pp. 3343– 3363). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2962829

[3]. Yu, K., Tan, L., Mumtaz, S., Al-Rubaye, S., Al-Dulaimi, A., Bashir, A. K., & Khan, F. A. (2021). Securing Critical Infrastructures: Deep- Learning-Based Threat Detection in IIoT. IEEE Communications Magazine, 59(10), 76–82. https://doi.org/10.1109/MCOM.101.2001126

[4]. Sharma, S., & Guleria, K. (2022). Machine Learning Techniques for Intelligent Vulnerability Detection in Cyber-Physical Systems. 2022 International Conference on Data Analytics for Business and Industry, ICDABI 2022, 200–204. https://doi.org/10.1109/ICDABI56818.2022.10041602

[5]. Mikkelsplass, S. A., & Jörgensen, P.-A. (2023). Cyber Security Anomaly Detection In An Industry 4.0 Testbed -- Results and Experiences. 3422–3429. https://doi.org/10.3850/978-981-18- 8071-1_p564-cd

[6]. Vaiyapuri, T., Sbai, Z., Alaskar, H., & Alaseem, N. A. (n.d.). Deep Learning Approaches for Intrusion Detection in IIoT Networks – Opportunities and Future Directions. In IJACSA) International Journal of Advanced Computer Science and Applications (Vol. 12, Issue 4). www.ijacsa.thesai.org.

[7]. Kalpesh Patel, S., Sadhwani, S., Muthalagu, R., & Mothabhau Pawar, P. (2023). Deep Learning Based Intrusion Detection Systems Techniques in IoT-Survey. Proceedings of 3rd IEEE International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2023, 53–58. https://doi.org/10.1109/ICCIKE58312.2023.10131739.

[8]. Osa, E., Orukpe, P. E., & Iruansi, U. (2024). Design and implementation of a deep neural network approach for intrusion detection systems. E-Prime - Advances in Electrical Engineering, Electronics and Energy, 7. https://doi.org/10.1016/j.prime.2024.100434

[9]. Lilhore, U. K., Dalal, S., & Simaiya, S. (2024). A cognitive security framework for detecting intrusions in IoT and 5G utilizing deep learning. Computers and Security,136. https://doi.org/10.1016/j.cose.2023.103560.

[10]. Biju, A., & Franklin, S. W. (2024). Evaluated bird swarm optimization based on deep belief network (EBSO-DBN) classification technique for IOT network intrusion detection. Automatika, 65(1), 108–116. https://doi.org/10.1080/00051144.2023.2269646.

[11]. Lu, Y., Chai, S., Suo, Y., Yao, F., & Zhang, C. (2024). Intrusion detection for Industrial Internet of Things based on deep learning. Neurocomputing, 564. https://doi.org/10.1016/j.neucom.2023.126886.

[12]. Li, L., Zhao, X., Fan, J., Liu, F., Liu, N., & Zhao, H. (2024). A trustworthy security model for IIoT attacks on industrial robots. Future Generation Computer Systems, 153, 340–349. https://doi.org/10.1016/j.future.2023.11.027

[13]. Sharma, B., Sharma, L., Lal, C., & Roy, S. (2024). Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach. Expert Systems with Applications, 238. https://doi.org/10.1016/j.eswa.2023.121751.

[14]. Rajak, A., & Tripathi, R. (2023). DL-SkLSTM approach for cyber security threats detection in 5G enabled IIoT. International Journal of Information Technology (Singapore). https://doi.org/10.1007/s41870-023-01651-7

[15]. Latif, S., Boulila, W., Koubaa, A., Zou, Z., & Ahmad, J. (2024). DTL-IDS: An optimized Intrusion Detection Framework using Deep Transfer Learning and Genetic Algorithm. Journal of Network and Computer Applications, 221. https://doi.org/10.1016/j.jnca.2023.103784

[16]. Devendiran, R., & Turukmane, A. v. (2024). Dugat-LSTM: Deep learning based network intrusion detection system using chaotic optimization strategy. Expert Systems with Applications, 245. https://doi.org/10.1016/j.eswa.2023.123027

[17]. Du, J., Yang, K., Hu, Y., & Jiang, L. (2023). NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning. IEEE Access, 11, 24808–24821. https://doi.org/10.1109/ACCESS.2023.3254915

[18]. Sivamohan, S., & Sridhar, S. S. (2023). An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework. Neural Computing and Applications, 35(15), 11459–11475. https://doi.org/10.1007/s00521-023-08319-0

[19]. Balla, A., Habaebi, M. H., Elsheikh, E. A. A., Islam, M. R., Suliman, F. E. M., & Mubarak, S. (2024). Enhanced CNN-LSTM Deep Learning for SCADA IDS Featuring Hurst Parameter Self- Similarity. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3350978

[20]. Pashaei, A., Akbari, M. E., Lighvan, M. Z., & Charmin, A. (2023). Deep Learning Based Early Intrusion Detection in IIoT using Honeypot. Majlesi Journal of Electrical Engineering, 17(2), 69–77. https://doi.org/10.30486/mjee.2023.1970288.0

[21]. Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection. Wireless Communications and Mobile Computing, 2021. https://doi.org/10.1155/2021/7154587

[22]. Althobaiti, M. M., Pradeep Mohan Kumar, K., Gupta, D., Kumar, S., & Mansour, R. F. (2021). An intelligent cognitive computing based intrusion detection for industrial cyber-physical systems. Measurement: Journal of the International Measurement Confederation, 186. https://doi.org/10.1016/j.measurement.2021.110145

[23]. Wai, E., & Lee, C. K. M. (2023). Seamless Industry 4.0 Integration: A Multilayered Cyber-Security Framework for Resilient SCADA Deployments in CPPS. Applied Sciences, 13(21), 12008. https://doi.org/10.3390/app132112008

[24]. Arshad, I., Alsamhi, S. H., Qiao, Y., Lee, B., & Ye, Y. (2023). A Novel Framework for Smart Cyber defence: A Deep-Dive into Deep Learning Attacks and defences; A Novel Framework for Smart Cyber defence: A Deep-Dive into Deep Learning Attacks anddefences.https://doi.org/10.1109/ACCESS.2017.DOI.

[25]. Shen, S., Cai, C., Li, Z., Shen, Y., Wu, G., & Yu, S. (2024). Deep Q-network-based heuristic intrusion detection against edge-based SIoT zero-day attacks. Applied Soft Computing, 150, 111080. https://doi.org/10.1016/j.asoc.2023.111080

[26]. Kasongo, S. M. (2021). An advanced intrusion detection system for IIoT Based on GA and tree based algorithms. IEEE Access, 9, 113199–113212. https://doi.org/10.1109/ACCESS.2021.3104113.

