International Journal of Basic and Applied Sciences, 14 (SI-1) (2025) 319-324

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/h2qnce11
Research paper

Deep Learning Techniques for Enhancing Cybersecurity in IoT Networks

Bhavuk Samrat [1] *, Dr. Trapty Agarwal [2], Shashikant Deepak [3],
Dr. Bharat Jyoti Ranjan Sahu [4], Dr. S. Emalda Roslin [5],
G. N. Mamatha [6], Bhanu Juneja [7]

[1] Chitkara Center for Research and Development, Chitkara University, Himachal Pradesh, India
[2] Associate Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India
[3] Assistant Professor, uGDX, ATLAS SkillTech University, Mumbai, India
[4] Associate Professor, Center for Cyber Security, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India
[5] Professor, Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India
[6] Assistant Professor, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Ramnagar District, Karnataka, India
[7] Center of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India
**Corresponding author E-mail: bhavuk.samrat.orp@chitkara.edu.in*

Received: May 2, 2025, Accepted: May 31, 2025, Published: October 31, 2025

Abstract

The progression of internet technologies, such as Industry 4.0, IoT (Internet of Things), Industrial IoT, Medical of Things (MoI), and Web 3.0, has led to a continual increase in cybersecurity issues. These technologies improve users' lives by making devices accessible online. This is sometimes referred to as the Internet of Everything, or IoE. With the rise in internet users and connected gadgets, fraudsters might take advantage of susceptible hosts. The networked gadgets display specific weaknesses that enable their exploitation. Malicious software such as malware, botnets, and intrusions can be utilized to compromise these devices. The ability of fileless malware to infiltrate a system without leaving evidence of exploitation has been utilized by astute, systematic, and targeted hackers. The malicious software exploits the system's vulnerabilities. As per OWASP (Open Web Application Security Project [1], the ten most exploited vulnerabilities in 2021 encompass server-side request forgery, injection, insecure design, compromised authentication, software and data integrity failure, security misconfiguration, broken access control, and inadequate logging and monitoring. Machine learning and deep learning methodologies exhibit promise in identifying the substantial cybersecurity dangers mentioned above. As a result, deep learning models were developed to identify and categorize these risks.

Keywords: *Cyber Security; ML; DL and Risk; Security.*

1. Introduction

Recent research indicates that machine learning and deep learning are efficacious techniques for detecting and classifying cybersecurity threats, facilitating the identification of dangers before they can exploit a network or device [5] [13] [19]. The network's dangerous tendencies can be detected by the learning models, which can then notify the administrator of any questionable activity. Using ML and DL techniques, as well as the analysis and extraction of network data, researchers have put forth numerous solutions for the automatic detection of botnets. Both the host and network levels can be used to implement the botnet detection methods. However, IoT devices lack the computing power and memory necessary to implement security solutions for the detection of harmful events [3]. As a result, the way the IoT devices operate must be monitored for any unusual network activity. It is feasible to put in place a network-level security system that can recognize the malicious activity of the linked devices—in this case, a botnet. Binary classification is the term used to describe the process of distinguishing harmful traffic from benign communication. That's where machine learning (ML) comes into play, enhancing our ability to work with computers by allowing us to tackle problems that don't have manually designed algorithms [9]. You can think of an algorithm as non-constructive when it uses examples of correct behavior [1]. In this sense, ML algorithms act as a sort of meta-algorithm, generating algorithms based on the information provided about what they should produce [11]. This approach offers a much more effective way to interact with computers, as it focuses on supplying data for computation rather than relying solely on predefined algorithms [2]. While expanding our ability to solve problems with computers is a significant reason to study ML, it's not the only one. Learning helps us understand what can realistically be computed, and in turn, studying computation can deepen our grasp of learning itself. As a scientific field, ML investigates the computational foundations of learning. By attempting to solve problems through computational models of learning, we gain insights into how our minds work, and what we learn about the brain can inspire new models in ML [7] [15]. IGAN-IDS refers to the Intrusion Detection System based on Integrated Generative Adversarial Networks (IGAN). It combines the generative capabilities of GANs with traditional IDS methods to enhance anomaly detection in IoT networks. In this paper, the term IDS will specifically refer to the IGAN-IDS model.

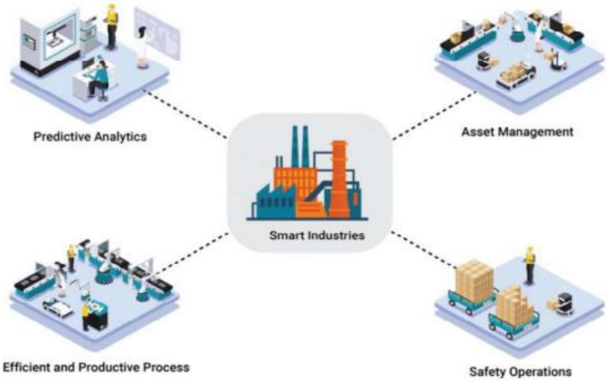

Fig. 1: IIoT in Industrial Processes.

Fig. 1: Illustrates the role of IIoT in industrial processes, highlighting how IoT technologies are integrated into manufacturing environments to enhance productivity and operational efficiency.

Machine learning techniques have the potential to tackle a wide range of practical and business challenges [17]. As researchers, our primary focus is on advancing scientific knowledge. We can either start by developing a new method and then look for a problem it can address, or we can identify a specific issue and work our way toward a solution [4]. Federated deep learning (FDL) has emerged as a key technique for privacy-preserving IoT systems [16] [20] [18]. It enables decentralized training of models on distributed data without the need to share sensitive data, addressing key privacy concerns. However, challenges include data heterogeneity and communication inefficiencies. European studies emphasize the need for stronger IoT security standards to mitigate risks, especially in sectors like healthcare and autonomous vehicles.

2. Materials and Methods

The Random Forest (RF) algorithm is often hailed as one of the top choices for classification tasks. Initially, it generates multiple decision trees (DTs), which are then combined to achieve accurate classifications. The accuracy of this algorithm tends to improve with the number of decision trees used—essentially, the more trees, the better the results. Even without fine-tuning its hyperparameters, Random Forest performs quite well. It employs an ensemble learning technique, like bagging, to help minimize overfitting while creating these decision trees. One of its great strengths is its flexibility; you can add any number of features to the decision trees. This algorithm can handle various types of input data, whether it's categorical, numerical, or binary. However, in real-world applications, it can be a bit slower since it generates a significant number of decision trees [12]. With an increase in the number of iterations, the classifier's overall accuracy generally enhances.

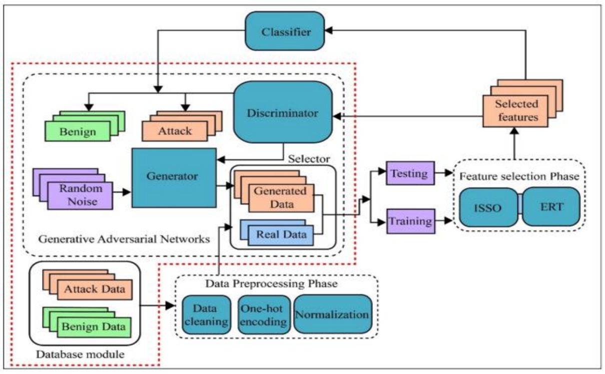

Fig. 2: Overall Architecture of the Proposed IDS Models.

When it comes to deep neural networks (NNs), two major issues often pop up: the vanishing and exploding gradient problems, along with the challenge of not having access to high-performance computing systems. Recent breakthroughs in processing technology, coupled with the creation of novel deep learning architectures and improvements in optimizers, activation functions, and loss functions, have effectively addressed these gradient difficulties [21]. Currently, deep learning (DL) is significantly impacting the domain of cybersecurity, demonstrating superior efficacy compared to conventional machine learning (ML) techniques in multiple applications. Deep learning architectures are categorized into two main types: generative and discriminative, as seen in Figure 2. The generative category includes models like deep Boltzmann machines (DBM), deep autoencoders (DAE), deep belief networks (DBN), and recurrent architectures, while the discriminative category mostly consists of recurrent architectures and convolutional neural networks (CNN). Among these, recurrent structures and convolutional neural networks are the most prominent deep learning architectures. Deep Belief Networks (DBN) and Deep Boltzmann Machines (DBM) are based on restricted Boltzmann machines (RBM), whereas generative adversarial networks (GANs) integrate both generative and discriminative categories inside deep learning frameworks [14]. An artificial neural network (ANN) is a computational model derived from the operations of biological neural networks (NNs) [6] [8].

3. Results and Discussion

To get more reliable results, we use the 10-fold cross-validation (CV) method. This means we divide the entire dataset into ten separate parts. In each round, one part is set aside for testing, while the other nine are used to train the algorithm. After running this process, we take the average of all 10 tests to evaluate the performance. The great thing about the 10-fold CV method is that the testing dataset is independent, which can really boost the reliability of our results. However, it's worth mentioning that just one run of the 10-fold CV might not give us a completely accurate outcome because of the inherent variability in the dataset [10].

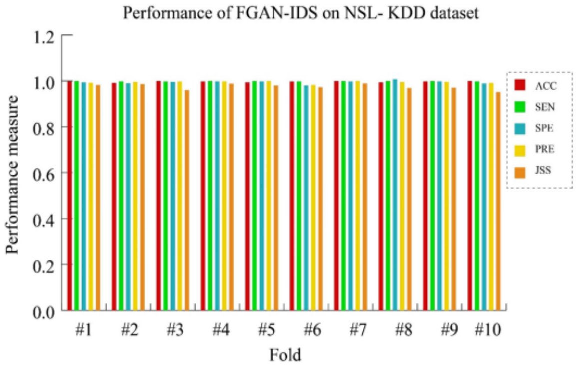

Fig. 3: Results of IGAN-IDS Model Regarding ACC, SEN, SPE, PRE, and JSS.

Fig. 3: Shows the performance properties of the IGAN-IDS model, which show improved accuracy, sensitivity, and specificity of the model compared to traditional machine learning models.

To ensure we get reliable results, we calculate all outcomes based on the average of 10 runs.

- The IGAN-IDS model performance was measured with the help of different measures:
- Accuracy (ACC): Reflects the general accuracy of the model.
- Sensitivity (SEN): This measures how well the model is correct in the identification of positive results.
- Specificity (SPE): Refers to the ability of the model to point out negatives.
- Precision (PRE): Shows the proportion of true positive predictions.
- Jaccard Similarity Score (JSS): Measures the overlap between predicted and actual positive instances.

These metrics, compared to classical ML models such as Support Vector Machines (SVM) and decision trees, demonstrate a significant improvement in the robustness and accuracy of the IGAN-IDS model.

We additionally assess the standard deviation of the performance measures to evaluate the efficacy of the desired IDS model. The proposed fused IGAN-IDS model is evaluated using the NSL-KDD dataset, with comprehensive performance results presented in Figure 4.

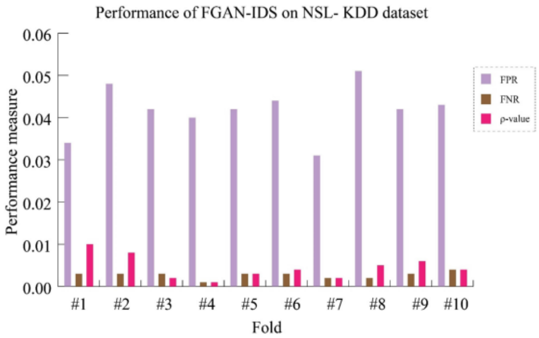

Fig. 4: Results of IGAN-IDS on NSL-KDD Regarding FPR, FNR, and ρ-Value.

Fig. 4: Displays the evaluation results of IGAN-IDS on the NSL-KDD dataset, emphasizing performance indicators such as false positive rate (FPR) and false negative rate(FNR).

These days, a huge chunk of social, financial, commercial, and administrative activities around the world happens online. This includes everyone from individuals to government and non-government organizations.

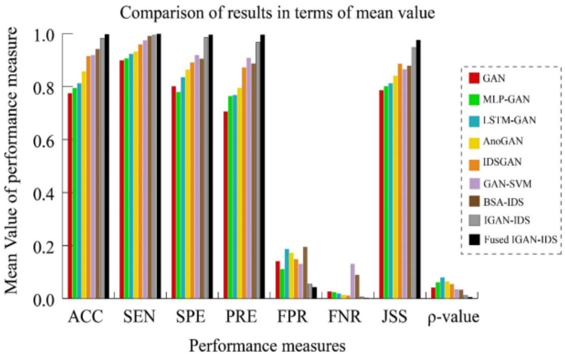

Fig. 5: Mean Value of Measures.

The rise of modern digital industrial technology, often referred to as Industry 4.0, is revolutionizing how we collect and analyze data from industrial equipment. This shift allows for quicker, more organized, and adaptable processes, ultimately leading to higher-quality products at lower costs.

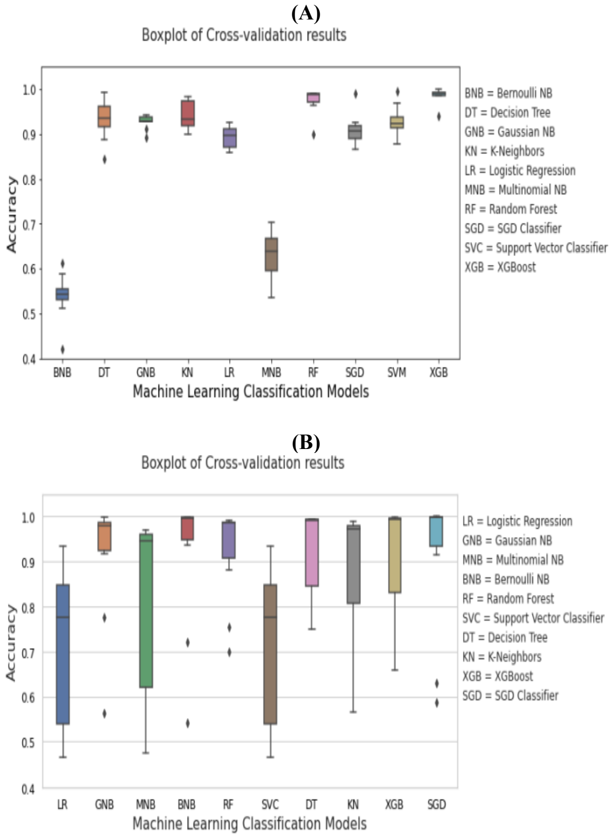

Fig. 6: Boxplot Comparative Performance Analysis of Various Classifiers.

Fig. 6: Presents a boxplot comparative analysis of various classifiers, showcasing the relative performance of IGAN-IDS against other models.

This industrial transformation is set to drive growth, reshape economies, boost productivity, and redefine the workforce landscape across various industries. In the end, it enhances the competitive edge of businesses and regions alike. Central to Industry 4.0 is the Industrial Internet of Things (IIoT), which facilitates novel business models and enhanced consumer interactions via advanced digital connectivity and the strategic utilization of high-performance computing resources. The IIoT connects people, intelligent machines, and other industrial tools, leveraging real-time data analytics and communication systems.

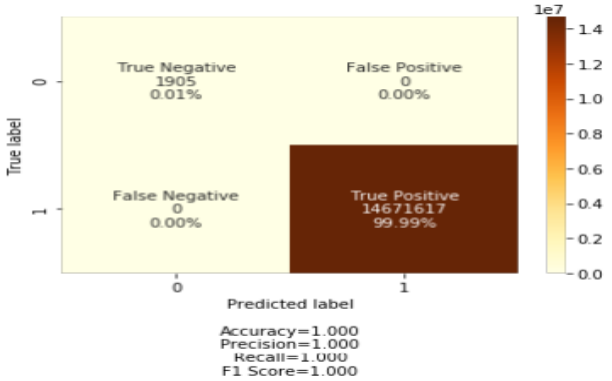

Fig. 7: Performance of the Proposed Model.

This connectivity enables automation across industrial applications, bringing a host of benefits like improved performance, increased productivity, reduced costs, minimized resource downtime, effective monitoring, optimized production scheduling, and fewer human errors. As a result, IIoT finds its place in a variety of industries. The IoT networks consist of smart sensors, actuators, instruments, and embedded software that can track and record data, along with distributed communication networks that gather, process, and analyze vast amounts of information. However, these features also make them attractive targets for cyber threats, as malicious actors can easily exploit insecure IoT devices. Consequently, many public and private organizations face hurdles in adopting IIoT technology. To truly transform their processes at the core, industries must tackle these challenges head-on. If the barriers to IoT implementation remain unaddressed, fully harnessing the potential of this technology will be a tough uphill battle.

4. Conclusion

In the latest research, deep neural network (DNN) models have been utilized to tackle a variety of challenges in cybersecurity. Even though these problems differ in nature, they all employ similar methods to enhance performance. A notable characteristic of these models is their scalability, enabling them to manage extensive datasets and high-dimensional areas during training. This scalability enables them to deliver impressive results, not just on benchmark datasets but also on real-time data collected from significant practical issues. The models excel at extracting optimal features in an implicit manner and learning distributed representations. These features are highly abstract and hierarchical, enabling the models to learn multiple levels of non-linear feature extraction. Given the numerous parameters involved, task-specific engineering was employed to determine the best values. Future research in IoT cybersecurity should focus on developing lightweight deep learning models capable of operating efficiently on resource-constrained devices. Additionally, addressing adversarial attacks on deep learning-based IDS systems remains a significant challenge. Principal research inquiries encompass: How can we enhance deep learning models for low-power IoT devices? What are the most effective techniques to mitigate adversarial attacks aimed at intrusion detection systems in IoT networks? This process involved running various experimental trials within a predefined range for the model's parameters. For comparison, classical machine learning (ML) models were also used, with task-specific engineering applied to extract hand-designed input features. Across all experiments related to different cybersecurity challenges, DNN models consistently outperformed the others.

References

[1] Maghrabi, L. A., Shabanah, S., Althaqafi, T., Alsalman, D., Algarni, S., Al-Malaise Al-Ghamdi, A., & Ragab, M. (2024). Enhancing cybersecurity in the internet of things environment using bald eagle search optimization with hybrid deep learning. *IEEE Access, 12*, 8337–8345. https://doi.org/10.1109/ACCESS.2024.3352568.

[2] Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. *IEEE Access, 9*, 138509–138542. https://doi.org/10.1109/ACCESS.2021.3118642.

[3] Robles, T., Alcarria, R., De Andrés, D. M., De la Cruz, M. N., Calero, R., Iglesias, S., & Lopez, M. (2015). An IoT based reference architecture for smart water management processes. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 6*(1), 4–23.

[4] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., &Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. *IEEE Access, 7*, 124379–124389. https://doi.org/10.1109/ACCESS.2019.2937347.

[5] Pinto, L., Brito, C., Marinho, V., & Pinto, P. (2022). Assessing the relevance of cybersecurity training and policies to prevent and mitigate the impact of phishing attacks. *Journal of Internet Services and Information Security, 12*(4), 23–38. https://doi.org/10.58346/JISIS.2022.I4.002.

[6] Alkhudaydi, O. A., Krichen, M., & Alghamdi, A. D. (2023). A deep learning methodology for predicting cybersecurity attacks on the internet of things. *Information, 14*(10), 550. https://doi.org/10.3390/info14100550.

[7] Senthil, T., Rajan, C., & Deepika, J. (2021). An improved optimization technique using deep neural networks for digit recognition. *Soft Computing, 21*, 1647–1658. https://doi.org/10.1007/s00500-020-05262-3.

[8] Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. *Authorea Preprints*. https://doi.org/10.22541/au.166379475.54266021/v1.

[9] Salman, R. H., & Alomari, E. S. (2023). Survey: Homomorphic encryption-based deep learning that preserves privacy. *International Academic Journal of Science and Engineering, 10*(2), 153–163. https://doi.org/10.9756/IAJSE/V10I2/IAJSE1019.

[10] Roopak, M., Tian, G. Y., & Chambers, J. (2019). Deep learning models for cyber security in IoT networks. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 452–457). IEEE. https://doi.org/10.1109/CCWC.2019.8666588.

[11] Bharath, K. C. P., Udayakumar, R., Chaya, J., Mohanraj, B., & Vimal, V. R. (2024). An efficient intrusion detection solution for cloud computing environments using integrated machine learning methodologies. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications.

[12] Perera, M., & Murshid, N. (2023). Payment for Ecosystem Services (PES) in Forest Management: A Pathway to Sustainable Climate Financing. *National Journal of Forest Sustainability and Climate Change*, *1*(1), 9-16.

[13] Havalam, N. K., & Bosco, R. M. (2025). High-efficiency solar-piezo hybrid energy harvester for long-term autonomous operation of smart agriculture sensor nodes. Progress in Electronics and Communication Engineering, 3(2), 36–43.*

[14] Ahmad, M., & Cide, F. (2025). AI-driven anomaly detection framework for industrial IoT using edge-enabled wireless sensor networks. Journal of Wireless Sensor Networks and IoT, 3(1), 33–39.

[15] Charabi, Y., & Wei, B. L. (2025). Scalable reconfigurable architectures for quantum-inspired computing: Design, challenges, and opportunities. SCCTS Transactions on Reconfigurable Computing, 3(2), 11–20.

[16] Hugh, Q., & Soria, F. (2025). Spatiotemporal transformer networks for real-time video-based anomaly detection in smart city surveillance. National Journal of Signal and Image Processing, 1(4).

[17] Barhoumia, E. M., & Caddwine, H. (2025). Reliability analysis and hardware fault injection for safety-critical embedded applications. Journal of Integrated VLSI, Embedded and Computing Technologies, 2(3), 63–72.

[18] Soria, F., & Metachew, K. (2025). Hybrid beamforming and physical layer security techniques for 6G massive MIMO communication systems. National Journal of RF Circuits and Wireless Systems, 3(1), 1–7.

[19] Zengeni, T. G., & Bates, M. P. (2025). Transformer-based end-to-end speech recognition for noisy real-world environments. National Journal of Speech and Audio Processing, 1(4), 1–8.

[20] Pavalam, S. M., & Babylatha, M. (2025). Smart sensor node design with energy harvesting for industrial IoT applications. National Journal of Electrical Electronics and Automation Technologies, 1(3), 10–18.

[21] Flammini, F., & Trasnea, G. (2025). Battery powered embedded system in IoT applications: Low power design techniques. SCCTS Journal of Embedded Systems Design and Applications, 2(2), 39–46.

[22] Alvarez, R. (2023). Integrating Precision Livestock Farming Technologies for Early Detection of Zoonotic Disease Outbreaks. *National Journal of Animal Health and Sustainable Livestock*, *1*(1), 17-24.

[23] Abid, N. (2023). Enhanced IoT network security with machine learning techniques for anomaly detection and classification. *International Journal of Current Engineering and Technology, 13*(6), 536–544.

[24] Sadaram, G., Sakuru, M., Karaka, L. M., Reddy, M. S., Bodepudi, V., Boppana, S. B., & Maka, S. R. (2022). Internet of Things (IoT) cybersecurity enhancement through artificial intelligence: A study on intrusion detection systems. *Universal Library of Engineering Technology, 2022*. https://doi.org/10.70315/uloap.ulete.2022.001.

[25] Bhuvaneshwari, A. J., &Kaythry, P. (2023). A review of deep learning strategies for enhancing cybersecurity in networks: Deep learning strategies for enhancing cybersecurity. *Journal of Scientific & Industrial Research (JSIR), 82*(12), 1316–1330. https://doi.org/10.56042/jsir.v82i12.1702.

[26] Gonaygunta, H., Nadella, G. S., Pawar, P. P., & Kumar, D. (2024). Enhancing cybersecurity: The development of a flexible deep learning model for enhanced anomaly detection. In *2024 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 79–84). IEEE. https://doi.org/10.1109/SIEDS61124.2024.10534661.

[27] Kimbugwe, N., Pei, T., &Kyebambe, M. N. (2021). Application of deep learning for quality of service enhancement in internet of things: A review. *Energies*, *14*(19), 6384. https://doi.org/10.3390/en14196384.

[28] Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks detection in iot-based smart city applications using machine learning techniques. *International Journal of environmental research and public health*, *17*(24), 9347. https://doi.org/10.3390/ijerph17249347.

[29] Bukhari, S. M. S., Zafar, M. H., Abou Houran, M., Qadir, Z., Moosavi, S. K. R., & Sanfilippo, F. (2024). Enhancing cybersecurity in Edge IIoT networks: An asynchronous federated learning approach with a deep hybrid detection model. *Internet of Things*, *27*, 101252. https://doi.org/10.1016/j.iot.2024.101252.

[30] Dutta, V., Choraś, M., Pawlicki, M., & Kozik, R. (2020). A deep learning ensemble for network anomaly and cyber-attack detection. *Sensors*, *20*(16), 4583. https://doi.org/10.3390/s20164583.

[31] Soliman, S., Oudah, W., &Aljuhani, A. (2023). Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alexandria Engineering Journal*, *81*, 371-383. https://doi.org/10.1016/j.aej.2023.09.023.

[32] Dixit, P., &Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer science review*, *39*, 100317. https://doi.org/10.1016/j.cosrev.2020.100317.