International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 13, Issue 4, April 2024)

# Machine Learning Techniques for Prediction of Malicious Intrusions in IoT Empowered Cybersecurity: A Review

Yatharth Upadhyay[1], Dr.Damodar Tiwari[2], Dr.Shital Gupta[3], Twinkle Sharma[4]
[1]Research Scholar, Dept. of CSE, Bansal Institute of Science and Technology, Bhopal, India
[2]Professor, Dept. of CSE, Bansal Institute of Science and Technology, Bhopal, India
[3]Associate Professor, Dept. of CSE, Bansal Institute of Science and Technology, Bhopal, India
[4]Assistant Professor, Dept. of CSE, Bansal Institute of Science and Technology, Bhopal, India

***Abstract*— With the rapid proliferation of Internet of Things (IoT) devices, ensuring cybersecurity has become a paramount concern. Malicious intrusions pose a significant threat to the integrity and security of IoT systems. Machine learning (ML) techniques have emerged as a promising approach for detecting and predicting such intrusions due to their ability to analyze vast amounts of data and identify patterns indicative of malicious activities. This paper provides a comprehensive review of machine learning techniques utilized for predicting malicious intrusions in IoT-enabled cybersecurity. We categorize and analyze various ML algorithms, discuss their strengths and limitations, and highlight recent advancements and challenges in this domain. Furthermore, we identify research gaps and propose future directions to enhance the efficacy of ML-based intrusion detection systems in IoT environments.**

***Keywords*— *Machine Learning, IOT, Cybersecurity, Intrusions.***

## I. INTRODUCTION

Cybersecurity refers to the practice of protecting computer systems, networks, data, and devices from unauthorized access, cyberattacks, theft, damage, or any other form of malicious intent [1]. It encompasses a broad range of technologies, processes, and practices designed to safeguard digital assets and ensure the confidentiality, integrity, and availability of information [2]. In today's interconnected world, cybersecurity is a critical concern for individuals, businesses, governments, and organizations of all sizes. With the increasing reliance on digital technologies for communication, commerce, healthcare, transportation, and other essential services, the potential impact of cyber threats has grown significantly [3]. Cyberattacks can disrupt operations, compromise sensitive data, violate privacy, cause financial losses, and even pose risks to public safety and national security. The proliferation of Internet of Things (IoT) devices has led to unprecedented connectivity and convenience in various domains, ranging from smart homes and healthcare to industrial automation and transportation [4]. However, the pervasive deployment of IoT devices has also introduced significant cybersecurity challenges. These challenges stem from the inherent vulnerabilities of IoT ecosystems, including limited computational resources, constrained communication channels, and diverse device types [5].

Malicious intrusions targeting IoT systems pose a severe threat to data privacy, system integrity, and overall cybersecurity. Traditional security mechanisms such as firewalls and encryption alone are insufficient to combat the sophisticated and evolving nature of cyber threats targeting IoT environments [6]. Consequently, there is a growing interest in leveraging machine learning (ML) techniques for predictive intrusion detection in IoT ecosystems. Machine learning offers a data-driven approach to cybersecurity, wherein algorithms are trained on historical data to recognize patterns indicative of malicious behavior. By continuously analyzing network traffic, device activity logs, and system behaviors, ML-based intrusion detection systems can identify anomalous activities and potential security breaches in real-time[7]. Moreover, ML algorithms can adapt to new attack vectors and emerging threats, making them well-suited for the dynamic nature of IoT environments.

Conduct a comprehensive review of machine learning techniques employed for predicting malicious intrusions in IoT-enabled cybersecurity. We categorize ML algorithms

based on their underlying principles, such as supervised learning, unsupervised learning, and semi-supervised learning [8]. For each category, we discuss prominent algorithms, their applications, strengths, and limitations in the context of IoT security. Examine recent advancements in ML-based intrusion detection systems, including ensemble methods, deep learning architectures, and federated learning approaches tailored for IoT environments. We also highlight the challenges associated with deploying ML models in resource-constrained IoT devices, such as computational overhead, energy consumption, and privacy concerns [9][10].

## II. LITERATURE SURVEY

I. A. Kandhro et al.,[1] computer viruses, malicious, and other hostile attacks can affect a computer network. Intrusion detection is a key component of network security as an active defence technology. Traditional intrusion detection systems struggle with issues like poor accuracy, ineffective detection, a high percentage of false positives, and an inability to handle new types of intrusions. To address these issues, we propose a deep learning-based novel method to detect cybersecurity vulnerabilities and breaches in cyber-physical systems. The proposed framework contrasts the unsupervised and deep learning-based discriminative approaches. This work presents a generative adversarial network to detect cyber threats in IoT-driven IICs networks. The results demonstrate a performance increase of approximately 95% to 97% in terms of accuracy, reliability, and efficiency in detecting all types of attacks with a dropout value of 0.2 and an epoch value of 25.

V. S. A. Raju et al.,[2] the expanding landscape of IoT-Botnet attacks, this research delves into the augmentation of Network Intrusion Detection (NID) through the utilization of Machine Learning (ML) algorithms. Beginning with an exploration of NID's vital role in cybersecurity, this study embarks on a comprehensive investigation. Within a controlled IoT lab, in Canadian Institute for Cybersecurity (CIC), both legitimate and malicious traffic data are meticulously captured and subjected to thorough analysis. Simulated attacks, executed via Kali Linux tools, generate datasets converted into csv formats for systematic examination.

S. E. Hajla et al.,[3] The rapid expansion of the Internet of Things (IoT) gives Intruders a wide attack surface from which they can conduct more damaging cyber-attacks. Scan, Spying, Denial of Service, Data Type Probing, Malicious Control, and Malicious Operation are such attacks and anomalies that can bring down an IoT system, which makes Attack and anomaly detection in IoT a rising concern and creating a powerful Intrusion Detection System (IDS) a primary need. The main goal of an intrusion detection system (IDS) is detecting attacks and any attempt to break down networks. Machine learning techniques have recently been used in intrusion detection systems since they have shown the ability to learn and adapt, besides providing a quick response. This work proposes an intrusion detection framework that can classify network activities as “Normal” or “Attack” using various machine learning methods. A common dataset called BoT-IoT evaluated the suggested model using KNIME analytics Platform.

A. Ahmed et al.,[4] Security is a major concern for Internet of Things (IoT) devices. Due to their vulnerabilities, these devices are an easy target for unauthorized access. Traditional security mechanisms are not easily deployed on these tiny devices. Therefore, machine learning-based algorithms are proving to be key enablers in IoT attack detection. In this work, we critically investigate the efficacy of classification algorithms; Logistic Regression (LR), Gaussian Naive Bayes (GNB), Decision Trees (DT), Random Forest (RF), K-Nearest Neighbors KNN), and Extreme Gradient Boosting (XGB) for malicious attack detection in an IoT network flow traffic. A real-time heterogeneous dataset is used in this study. The data is preprocessed before experimentation. In addition, a feature selection method is implemented to identify the most important features.

N. Karmous et al.,[5] presents a proposed artificial intelligence (AI) framework used to detect attacks in an IoT ecosystem. The proposed framework is an intrusion detection system (IDS) using a machine learning strategy to monitor the IoT system and detect malicious and suspicious activity. In this work, we used supervised machine learning (ML) method to increase detection accuracy and minimize data processing time. Four classification algorithms are used to evaluate the proposed model, namely Random Forest (RF), Support Vector Machines (SVM), k Nearest Neighbors (kNN) and Gaussian Naïve Bayes (GNB) algorithm. Experimental results showed that KNN performs best with 97.5% accuracy and fastest training times with 0.03 seconds (i.e. the training times are the CPU time to build the model). At the end, we proposed an implementation of the proposed IDS in a real IoT environment.

T. Gazdar et al.,[6] IoT environments are highly diverse with regard to devices, applications, and communications protocols. Consequently, they are highly vulnerable to many new attacks specific to this particular network. Existing Intrusion detection

systems have shown their inefficiency in loT and this is for many reasons related basically to the limited computation capability of the devices, their mobility, the inherent Internet connectivity, and the large scale of the IoT network. Thus, a lightweight and efficient intrusion detection system designed for loT is required. Inspired by the success of Machine Learning in many fields and its potential in attack detection, we propose in this work an intrusion detection system for Smart Home. The main goal is to design a model that detects different attacks on different Smart Home devices.

K. Cao et al.,[7] With the rapid development of the Internet of Things (IoT), the continuous emergence of cyberattacks have brought great threat to the security of the network. Intrusion Detection System (IDS) which can identify malicious network attacks has become a strong tool to ensure network security. Many deep learning-based approaches have been used in IDS. However, most of these researches ignore the internal structural characteristics of the network traffic, and cannot accurately learn the key features of the malicious traffic. Thus, they have a low accuracy in classifying different kinds of network attacks. In this work, we build an intrusion detection model DAL (Dense-Attention-LSTM, DAL), in which dense dilated convolutions is used to extract the underlying features of the network traffic.

I. Ullah et al.,[8] The growing development of IoT (Internet of Things) devices creates a large attack surface for cybercriminals to conduct potentially more destructive cyberattacks; as a result, the security industry has seen an exponential increase in cyber-attacks. Many of these attacks have effectively accomplished their malicious goals because intruders conduct cyber-attacks using novel and innovative techniques. Convolutional neural networks are an excellent alternative for anomaly detection and classification due to their ability to automatically categorize main characteristics in input data and their effectiveness in performing faster computations. In this work, we design and develop a novel anomaly-based intrusion detection model for IoT networks. First, a convolutional neural network model is used to create a multiclass classification model. The proposed model is then implemented using convolutional neural networks in 1D, 2D, and 3D.

D. Park et al.,[9] As cyberattacks become more intelligent, the difficulty increases for traditional intrusion detection systems to detect advanced attacks that deviate from previously stored patterns. To solve this problem, a deep learning-based intrusion detection system model has emerged that analyzes intelligent attack patterns through data learning. However, deep learning models have the disadvantage of having to re-learn each time a new cyberattack method emerges. In the training and testing steps, a Siamese Convolutional Neural Network (Siamese-CNN) is constructed using the few-shot learning method, which shows excellent performance by learning a small amount of data. Siamese-CNN determines whether the attack type is the same based on the similarity score of each cyberattack sample converted to an image.

I. Siniosoglou et al.,[10] presented an Intrusion Detection System (IDS) specially designed for the SG environments that use Modbus/Transmission Control Protocol (TCP) and Distributed Network Protocol 3 (DNP3) protocols. The proposed IDS called MENSA (anoMaly dEtection aNd claSsificAtion) adopts a novel Autoencoder-Generative Adversarial Network (GAN) architecture for (a) detecting operational anomalies and (b) classifying Modbus/TCP and DNP3 cyberattacks. In particular, MENSA combines the aforementioned Deep Neural Networks (DNNs) in a common architecture, taking into account the adversarial loss and the reconstruction difference.

O. Alkadi et al.,[11] There has been significant research in incorporating both blockchain and intrusion detection to improve data privacy and detect existing and emerging cyberattacks, respectively. In these approaches, learning-based ensemble models can facilitate the identification of complex malicious events and concurrently ensure data privacy. Such models can also be used to provide additional security and privacy assurances during the live migration of virtual machines (VMs) in the cloud and to protect Internet-of-Things (IoT) networks. This would allow the secure transfer of VMs between data centers or cloud providers in real time. This article proposes a deep blockchain framework (DBF) designed to offer security-based distributed intrusion detection and privacy-based blockchain with smart contracts in IoT networks.

T. Yu et al.,[12] In recent years, due to the increased frequency of cyber-attacks, the negative impacts of cyber-attacks on society have increased. Therefore, the research on cyber-security and prevention of cyber-attacks, including intrusion detection as an effective means of defense against cyber-attacks, is warranted. Both in the research and in the development of the systems for intrusion detection, the machine learning and deep learning methods are widely utilized, and the NSL-KDD dataset is frequently used in algorithm research and verification. In this paper, we propose a new two-stage dimensionality reduction (TSDR) feature selection method and verified by NSL-KDD dataset. The

method reduces the dimensionality of the dataset and significantly improves the calculation efficiency.

G. Kadam et al.,[13] A network intrusion detection system is proposed which is tailored to detect these attacks. The main objective is to classify the aforementioned types of attacks with minimum uncertainty and reduce the number of false positives for more reliable detection. With data mining coupled with machine learning and deep learning algorithms, a feature selection and a classification model is built by primarily training it on the KDDCup99 dataset and the ISTS Dataset, then tweaking the models by testing it on real-time data gathered from tcpdump. Real-time data collected using the ISTS dataset is firstly labelled using unsupervised machine learning methods and also by matching the data with the KDDCup99 dataset records. A model with the most optimum algorithms used for feature selection and classification procedure is developed. Also, different algorithms used on various parameters are compared.

B. Kızıltaş et al.,[14] a deep learning based model has been devoloped in order to detect the known network attacks and increase the detection performance of the zero-day attacks. NSL-KDD data set which has been used to simulate the zeroday attacks and compare the performance with the previous studies. Our convolutional neural network based denoising, sparse stacked auto encoder (CNN-DSSAE) model, using the swish activation function in the last layer and SGD with decoupled weight decay (SGDW) as the optimization algorithm, has achieved higher performance than the studies done with different machine learning and deep learning models on the same dataset.

G. Kaur et al.,[15] The security community has witnessed an unprecedented upsurge in cyber attacks in recent years. These attacks have proved to be successful in achieving their catastrophic objectives. Intrusion detection and prevention systems remain the principal point of defense against these devastating attacks. However, most of the anomaly datasets in the past are neither up-to-date nor reliable. Researchers used various machine learning techniques to classify anomaly-based attacks due to their capability to keep pace with the evolution of such attacks and gave encouraging predictions. Nevertheless, deep neural networks turned out to be revolutionary in detecting and characterizing such intrusions. In this paper, first of all, we propose an imagebased deep neural model to classify various attacks by using two comprehensive datasets called CICIDS2017 and CSE-CICIDS2018. Secondly, we provide a list of best network flow features to identify these attacks.

H. Zhang et al.,[16] In recent years, network traffic data have become larger and more complex, leading to higher possibilities of network intrusion. Traditional intrusion detection methods face difficulty in processing high-speed network data and cannot detect currently unknown attacks. Therefore, this paper proposes a network attack detection method combining a flow calculation and deep learning. The method consists of two parts: a real-time detection algorithm based on flow calculations and frequent patterns and a classification algorithm based on the deep belief network and support vector machine ( DBN-SVM ) . Sliding window ( SW ) stream data processing enables real-time detection, and the DBN-SVM algorithm can improve classification accuracy. Finally, to verify the proposed method, a system is implemented. Based on the CICIDS2017 open source data set, a series of comparative experiments are conducted. The method ’ s real-time detection efficiency is higher than that of traditional machine learning algorithms.

G. Efstathopoulos et al.,[17] With the rapid progression of Information and Communication Technology (ICT) and especially of Internet of Things (IoT), the conventional electrical grid is transformed into a new intelligent paradigm, known as Smart Grid (SG). SG provides significant benefits both for utility companies and energy consumers such as the two-way communication (both electricity and information), distributed generation, remote monitoring, self-healing and pervasive control. However, at the same time, this dependence introduces new security challenges, since SG inherits the vulnerabilities of multiple heterogeneous, co-existing legacy and smart technologies, such as IoT and Industrial Control Systems (ICS). An effective countermeasure against the various cyberthreats in SG is the Intrusion Detection System (IDS), informing the operator timely about the possible cyberattacks and anomalies.

R. Vinayakumar et al.,[18] presented, a deep neural network (DNN), a type of deep learning model, is explored to develop a flexible and effective IDS to detect and classify unforeseen and unpredictable cyberattacks. The continuous change in network behavior and rapid evolution of attacks makes it necessary to evaluate various datasets which are generated over the years through static and dynamic approaches. This type of study facilitates to identify the best algorithm which can effectively work in detecting future cyberattacks. A comprehensive evaluation of experiments of DNNs and other classical machine learning classifiers are shown on various publicly available benchmark malware datasets. The optimal network parameters and network topologies for DNNs are chosen through the following hyperparameter selection

methods with KDDCup 99 dataset. All the experiments of DNNs are run till 1,000 epochs with the learning rate varying in the range [0.01-0.5].

Y. Zhou et al.,[19] With the accelerated growth of internet of things IoT application in recent years, cities have become smarter to optimize resource and improved the quality of life for residents. On the other hand, the IoT face the severe security problem like confidentiality, integrity, privacy, and availability. To prevent the cyberattack irreversible damage, we propose a framework, called DFEL, to detect the internet intrusion in the IoT environment. Through the experimental results, authors present that DFEL not only boosts classifiers' accuracy to predict cyberattack but also significantly reduce the detection time. Furthermore, the paper demonstrates how the DFEL balance the detection performance and speed.

K. K. Nguyen et al.,[20] With the rapid growth of mobile applications and cloud computing, mobile cloud computing has attracted great interest from both academia and industry. However, mobile cloud applications are facing security issues such as data integrity, users' confidentiality, and service availability. A preventive approach to such problems is to detect and isolate cyber threats before they can cause serious impacts to the mobile cloud computing system. Through experimental results, we show that our proposed framework not only recognizes diverse cyberattacks, but also achieves a high accuracy (up to 97.11%) in detecting the attacks. Furthermore, we present the comparisons with current machine learning-based approaches to demonstrate the effectiveness of our proposed solution.

## III. CHALLENGES

Predicting malicious intrusions in IoT empowered cybersecurity using machine learning techniques presents several challenges, including:

1. **Scalability**: IoT environments generate vast amounts of data from numerous interconnected devices. Processing and analyzing this data in real-time to detect intrusions require scalable machine learning algorithms capable of handling large datasets efficiently.
2. **Resource Constraints**: Many IoT devices have limited computational resources, memory, and energy supply. Implementing machine learning models on resource-constrained devices poses challenges in terms of model complexity, memory footprint, and energy consumption.
3. **Data Heterogeneity**: IoT ecosystems comprise diverse devices with varying data formats, communication protocols, and sensor types. Integrating heterogeneous data sources for training machine learning models requires preprocessing techniques to standardize data formats and extract relevant features.
4. **Data Imbalance**: In cybersecurity datasets, malicious instances often represent a minority class compared to normal behavior. Class imbalance can lead to biased models that prioritize accuracy on the majority class while overlooking rare but critical malicious events. Addressing class imbalance requires techniques such as oversampling, undersampling, or using specialized algorithms like anomaly detection.
5. **Adversarial Attacks**: Attackers may attempt to evade detection by crafting adversarial examples—subtle perturbations to input data that deceive machine learning models. Adversarial attacks pose a significant challenge in IoT security, as adversaries can exploit vulnerabilities in sensor readings or communication protocols to manipulate input data and bypass intrusion detection systems.
6. **Privacy Concerns**: IoT devices collect sensitive data about users, their environments, and activities. Machine learning models trained on such data may pose privacy risks if they inadvertently disclose sensitive information or enable unauthorized surveillance. Ensuring privacy-preserving machine learning techniques, such as differential privacy or federated learning, is crucial in IoT cybersecurity.
7. **Transferability**: Machine learning models trained in one IoT environment may not generalize well to new or unseen environments due to differences in device configurations, network topologies, or attack strategies. Achieving model transferability across diverse IoT deployments requires robust model validation and adaptation techniques.
8. **Dynamic Environments**: IoT ecosystems are dynamic, with devices joining, leaving, or changing their behavior over time. Machine learning models must adapt to evolving threats, device configurations, and network conditions to maintain effective

intrusion detection capabilities in dynamic IoT environments.

9. **Interpretability**: Understanding the rationale behind machine learning predictions is crucial for trust and accountability in cybersecurity applications. Interpretable machine learning techniques enable security analysts to interpret model outputs, identify false positives, and fine-tune detection rules based on domain expertise.

Addressing these challenges requires interdisciplinary collaboration between cybersecurity experts, machine learning researchers, IoT engineers, and policymakers. By developing robust, scalable, and privacy-preserving machine learning techniques tailored to the unique characteristics of IoT environments, it is possible to enhance the resilience of IoT empowered cybersecurity against malicious intrusions.

## IV. CONCLUSION

The integration of machine learning techniques for predicting malicious intrusions in IoT empowered cybersecurity holds immense promise in enhancing the resilience and effectiveness of cybersecurity measures. However, this endeavor is not without its challenges. From scalability and resource constraints to data heterogeneity, adversarial attacks, and privacy concerns, numerous obstacles must be addressed to realize the full potential of machine learning in IoT security. Despite these challenges, the research and development efforts in this field have been substantial, with significant progress made in developing scalable, adaptive, and privacy-preserving machine learning algorithms tailored for IoT environments. By addressing the challenges identified in this review, such as data imbalance, adversarial attacks, and model interpretability, researchers can pave the way for more robust and reliable intrusion detection systems in IoT cybersecurity.

## REFERENCES

1. I. A. Kandhro et al., "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," in IEEE Access, vol. 11, pp. 9136-9148, 2023, doi: 10.1109/ACCESS.2023.3238664.
2. V. S. A. Raju and S. B, "Network Intrusion Detection for IoT-Botnet Attacks Using ML Algorithms," 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/CSITSS60515.2023.10334188.
3. S. E. Hajla, E. Mahfoud, Y. Maleh and S. Mounir, "Attack and anomaly detection in IoT Networks using machine learning approaches," 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM), Istanbul, Turkiye, 2023, pp. 1-7, doi: 10.1109/WINCOM59760.2023.10322991.
4. A. Ahmed and C. Tjortjis, "Machine Learning based IoT-BotNet Attack Detection Using Real-time Heterogeneous Data," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 2022, pp. 1-6, doi: 10.1109/ICECET55527.2022.9872817.
5. N. Karmous, M. O. -E. Aoueileyine, M. Abdelkader and N. Youssef, "IoT Real-Time Attacks Classification Framework Using Machine Learning," 2022 IEEE Ninth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 2022, pp. 1-5, doi: 10.1109/ComNet55492.2022.9998441.
6. T. Gazdar, "A New IDS for Smart Home based on Machine Learning," 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), Al-Khobar, Saudi Arabia, 2022, pp. 393-400, doi: 10.1109/CICN56167.2022.10008310.
7. K. Cao, J. Zhu, W. Feng, C. Ma, M. Liu and T. Du, "Network Intrusion Detection based on Dense Dilated Convolutions and Attention Mechanism," 2021 International Wireless Communications and Mobile Computing (IWCMC), 2021, pp. 463-468, doi: 10.1109/IWCMC51323.2021.9498652.
8. I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," in IEEE Access, vol. 9, pp. 103906-103926, 2021, doi: 10.1109/ACCESS.2021.3094024.
9. D. Park, S. Kim, H. Kwon, D. Shin and D. Shin, "Host-Based Intrusion Detection Model Using Siamese Network," in IEEE Access, vol. 9, pp. 76614-76623, 2021, doi: 10.1109/ACCESS.2021.3082160.
10. I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1137-1151, June 2021, doi: 10.1109/TNSM.2021.3078381.

11. O. Alkadi, N. Moustafa, B. Turnbull and K. -K. R. Choo, "A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9463-9472, 15 June15, 2021, doi: 10.1109/JIOT.2020.2996590.
12. T. Yu, Z. Liu, Y. Liu, H. Wang and N. Adilov, "A New Feature Selection Method for Intrusion Detection System Dataset – TSDR method," 2020 16th International Conference on Computational Intelligence and Security (CIS), 2020, pp. 362-365, doi: 10.1109/CIS52066.2020.00083.
13. G. Kadam, S. Parekh, P. Agnihotri, D. Ambawade and P. Bhavathankar, "An Approach to Reduce Uncertainty Problem in Network Intrusion Detection Systems," 2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS), 2020, pp. 586-590, doi: 10.1109/ICIIS51140.2020.9342634.
14. B. Kızıltaş and E. Gül, "Network Anomaly Detection With Convolutional Neural Network Based Auto Encoders," 2020 28th Signal Processing and Communications Applications Conference (SIU), 2020, pp. 1-4, doi: 10.1109/SIU49456.2020.9302202.
15. G. Kaur, A. Habibi Lashkari and A. Rahali, "Intrusion Traffic Detection and Characterization using Deep Image Learning," 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2020, pp. 55-62, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00025.
16. H. Zhang, Y. Li, Z. Lv, A. K. Sangaiah and T. Huang, "A real-time and ubiquitous network attack detection based on deep belief network and support vector machine," in IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 3, pp. 790-799, May 2020, doi: 10.1109/JAS.2020.1003099.
17. G. Efstathopoulos et al., "Operational Data Based Intrusion Detection System for Smart Grid," 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1-6, doi: 10.1109/CAMAD.2019.8858503.
18. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," in IEEE Access, vol. 7, pp. 41525-41550, 2019, doi: 10.1109/ACCESS.2019.2895334.
19. Y. Zhou, M. Han, L. Liu, J. S. He and Y. Wang, "Deep learning approach for cyberattack detection," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2018, pp. 262-267, doi: 10.1109/INFCOMW.2018.8407032.
20. K. K. Nguyen, D. T. Hoang, D. Niyato, P. Wang, D. Nguyen and E. Dutkiewicz, "Cyberattack detection in mobile cloud computing: A deep learning approach," 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1-6, doi: 10.1109/WCNC.2018.8376973.