Deep Learning Towards Intrusion Detection System (IDS): Applications, Challenges and Opportunities

Selvam Ravindran and Velliangiri Sarveshwaran*

Department of Computational Intelligence, SRM Institute of Science and Technology, Kattankulathur Campus, Chengalpattu 603203, Tamil Nadu, India
E-mail: sr9997@srmist.edu.in; vellians@srmist.edu.in
**Corresponding Author*

Received 19 January 2023; Accepted 01 July 2023;
Publication 11 August 2023

Abstract

With the growth of numerous technological areas, including sensors, embedded computing, broadband Internet access, wireless communications, distributed services, automatic identification, and tracking, the potential for integrating smart objects into our daily activities through the Internet has increased. The Internet of Things (IoT) is the confluence of the Internet and intelligent objects that can converse and cooperate with one another. IoT is a brand-new example that unifies Cyberspace with actual physical objects from various areas, including, business processes, human health, home automation, and environmental monitoring. It intensifies the use of Internet-connected strategies in our regular lives, carrying with it several advantages as well as security challenges. Intrusion Detection Systems (IDS) have been a crucial device for the defence of systems and material schemes for more than 20 years. However, applying traditional IDS techniques was challenging due to the IoT's inimitable features, like resource-constrained

Journal of Mobile Multimedia, Vol. 19_5, 1299–1330.
doi: 10.13052/jmm1550-4646.1958

devices and particular protocol stacks and standards. As a result, this survey will focus on various Deep Learning (DL)-based intrusion detection techniques. This study makes use of 50 research papers that focused on different techniques, and a review of studies that used those techniques was given. This research enables categorizing the methods employed for intrusion detection in IoT based on Convolutional Neural Network (CNN)-based methods, Deep Neural Network (DNN)-based methods, Optimization-based methods, and so on. Moreover, the categorization of approaches, published year, the dataset used, tools used, and the performance metrics are measured for intrusion detection in IoT. On the basis of the software used for implementation, performance achievement, and other factors, a thorough analysis was conducted. The conclusion identifies the research gaps and issues in a way that makes it clear why should create an efficient method for enabling efficient enhancement.

Keywords: Internet of Things, machine learning, deep learning, optimization, intrusion detection.

1 Introduction

The IoT is a cutting-edge technology that links smart devices to the Internet, including wireless cameras, the Internet of Vehicles (IoV), and other electronic gadgets [1]. IoT-connected nodes can communicate with one another on a predefined (Internet-based) network and can range from basic sensors in various environments to crucial components in various applications [2, 3]. IoT is an extensively adopted expertise in computerized systems that have recently influenced a variety of industries, including those in the agricultural, medical, transportation, and automobile sectors, as well as water monitoring. Due to their distributed structure and openness, many IoT devices capture, store, and process personal data, making them viable targets for attackers [4]. Security is becoming more important for the successful deployment of IoT networks. Examining IoT network traffic with IDS is necessary to spot cyber attacks [5]. Although it has more complexity, the IoT's core network is still a traditional network. The IoT network is more vulnerable due to the high number of nodes, and attacks may have more severe effects than they would on traditional networks [6]. Physical separation separates the conventional IoT system from the outside world. Information security is not taken into consideration and is primarily focused on the system's

stability and functional security. Designing and implementing an IoT defense mechanism is, therefore, crucial [7]. IoT frameworks are available everywhere and were primarily created by the loss of connections and compelled assets [8]. The functional hub of the entire IoT business system is the IoT server [9].

With the expansion of the IoT industry, security is becoming a more and more difficult problem. It is primarily caused by the heterogeneity of IoT architecture, the variety of accessed devices and communication [10] methods, the vast amount of data being transmitted through the network, and these factors combined. Authentication, data privacy, availability, confidentiality, integrity, energy efficiency, single-point failures that need to be verified, and other security-related issues are typically involved [11]. Because of the ongoing technological advancements, security is becoming an increasingly important aspect of cyber life. The IoT market is expanding quickly, there are an increasing number of terminals, and security risks are significant. In the IoT manufacturing chain, the percentage of security links is small. The IoT industry permeates numerous industries and has an extensive range of things on people's lives. Serious threats to life and property safety will also result from the corresponding security issues [9]. It is crucial to create a safety instrument for an IoT atmosphere while taking security precautions into account. In order to stop spiteful users from gaining unauthorized access to data sources, data-oriented security mechanisms must be prioritized. Focusing on data integrity and confidentiality is crucial because doing so significantly lowers the serious security threats in an IoT environment. Due to the large volume of data, conventional security mechanisms, which are developed using steganography techniques, are not commonly used in IoT environments. The network problems will be lessened if the threats are identified quickly. Conventional security models take more time to process such a large amount of data to identify the threats [12].

A subset of Machine Learning (ML), DL, can be applied to novel difficulties involving complex, high-dimensional data. Additionally, DL techniques enable the systematic training of nonlinear models on sizable datasets [13]. Because it can handle a lot of data and generalize to different kinds of network attacks, DL is effective at detecting intrusions [5, 14]. The ability of DL-based IDSs to extract complicated patterns has been demonstrated when a large amount of labelled information is available to develop classification techniques in order to recognize intrusions. Furthermore, it takes a lot of time and computing resources to completely retrain DL models with the new data

when a new intrusion is discovered. Since devices have limited computing power and datasets are scarce and unbalanced in IoT networks, DL-based IDSs are affected by these problems [15]. However, the DL approach has outperformed ML in terms of performance, especially for large datasets. Many IoT systems generate a significant amount of data, and DL methods are appropriate for such a system. It offers high-dimensional feature support. Additionally, it makes deep linking possible, allowing IoT-based devices and the applications running on them to communicate with one another automatically and without human intervention [11]. DNN and a variety of algorithms are used in DL to connect the network's layers. It is important to remember that these layers typically consist of an input layer with crucial data, followed by analysis through a number of hidden layers, and the final output layer. Unsupervised functions that create a high-level representation of data from low layers are what the model depends on [9].

The principal motive of this survey paper is to evaluate different methods of intrusion detection in IoT. Current approaches are divided into CNN-based approaches, Deep Neural Network-based approaches, and Optimization-based approaches, among others, based on the classification of the literature review. This study is established by seeing the used dataset, tools, classification of methods, etc. The research gaps and issues part of the current review papers clearly outlines the shortcomings that are present. As a result, the section on research gaps is seen as the driving force for future advancements in the IoT's efficient extraction.

An agreement of this survey is developed correspondingly as shown: Section 2 designates a review of the literature of Intrusion detection in IoT and Section 3 portrays the investigation gaps and problems of IDS. Section 4 signifies the investigation of intrusion detection in IoT in relation of used datasets, publication year, tools used, evaluation metrics, and lastly the conclusion of this survey paper is demonstrated in Section 5.

2 Literature Survey

This section illustrates the research that took into account the various IoT intrusion detection approaches. The categorizations of intrusion detection are revealed in Figure 1. Here, several approaches such as CNN-based methods, DNN-based methods, Optimization-based methods, and various other approaches are developed for intrusion detection. The difficulties with these approaches are evaluated in order to inspire researchers to create novel recovery techniques for IoT intrusion detection.

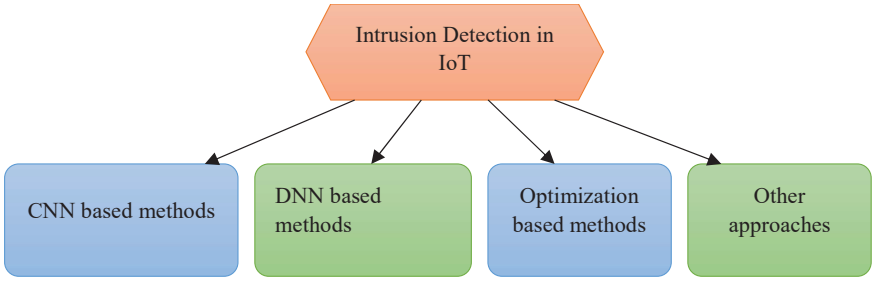

Figure 1 Categorization of IoT intrusion detection.

2.1 Classification of Intrusion Detection in IoT

Below are several research studies that looked at various methods for IoT intrusion detection.

(a) Deep Neural Network based methods

A highly extendable DNN was developed to detect IoT botnet attacks on networks of things. Ullah, S et al., [1] have introduced a method named as hybrid model for intrusion detection in IoV. In addition, a hybrid combination of Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) was established to reduce training and response time. Moreover, the method achieved high attack detection accuracy for and for the car-hacking dataset, and combined the Denial of Service (DDoS) dataset after analyzing the results. This model obtained an accuracy of 99.9% and 99.5% for car hacks, and DDoS attacks.

Yadav, N et al., [16] presented a smart IDS which was used to detect Internet of Things (IoT) based attacks was executed. A DL technique was additionally applied to identify fraudulent IoT network data. The identification solution allows the coordination of IoT connectivity protocols and validates operational security. An IDS was one of the famous security network technologies and it was used to protect the network. Moreover, the neural network was used to notice the attack works extremely well. Finally, the auto-encoder model was introduced to reduce the detection time and recovers detection precision had outstripped. After analyzing the results, the method certainly identified the actual global intruders. The accuracy obtained by this model was 99.41%.

Chao Liang et al., [6] employed a multi-agent hybrid placement strategy for the detection of IoT. In addition, the system was made up of four modules namely, data collection, analysis, response, and data management. Moreover,

the study employed a deep Neural Network (NN) algorithm for Intrusion Detection (ID) in the implementation of the analysis module. The results demonstrated the effectiveness of DL algorithms in detecting transport layer attacks. The analysis showed that DL algorithms were more appropriate for ID in an IoT network situation than traditional recognition methods used in IDSs. The evaluation was done based on accuracy and precision, and this model obtained the highest accuracy and precision of 98%.

Otoum, Y et al., [11] developed DL-based IDS to identify security threats. In addition, many IDDs can be found, but a lack of dataset management and optimal feature learning affected the accuracy of attack detection. Moreover, the method was combined with Stacked-Deep Polynomial Network (SDPN) and Spider Monkey Optimization algorithm (SMO) to achieve higher accuracy. In addition, the SMO procedure was used to cite the most appropriate structures from the dataset and SDPN was used to learn the best features and to analyze the data as anomalous or normal in various attack groups. Finally, the method achieved high performance in terms of precision, F-score and recall, and accuracy when analyzing the extensive results. The obtained accuracy, precision, recall, and F1-score of this model were 99.02%, 99.38%, 98.91%, and 99.14%, respectively.

Bhor, H.N. and Kalla, M., [17] discussed an intrusion detection strategy, which was named as Taylor-spider monkey optimization-based deep belief network (Taylor-SMO-based DBN) to detect the intrusion in the IoT network. Moreover, the actual presentation of DBN was based on the knowledge process working to exercise the classifier for which the Taylor-SMO algorithm was established. Finally, the analysis of the method was done, wherein the developed Taylor-SMO+DBN outdone existing methods with high accuracy, precision, recall, and false alarm rate with values of 90%, 90%, 92%, and 10%, respectively.

Susilo, B. and Sari, R.F., [8] discussed different DL and machine learning algorithms for the purpose of improving the security performance of the IoT. For the purpose of detecting Denial-of-Service (DoS) attacks, the deep learning technique was also introduced. Furthermore, the researchers used a programming language named Python including the packages of sea born, sci-kit-learn, and Tensor flow. Finally, the method was getting more accurate thereby the moderation of attacks that were present in IoT networks was real as possible. The accuracy of this model was 91%.

Khan, M. A et al., [18] developed DNN-based intrusion detection in the Message Queuing Telemetry Transport (MQTT)-based protocol. The effectiveness of the technique was also evaluated using the two different

datasets. The results for binary classification and the first dataset showed that the model achieved higher accuracy for uni-flow, bi-flow, and packet flow. However, in the multi-label classification, the accuracies were reduced. For the second dataset, the method gained the highest accuracy against GRU and LSTM. The highest accuracy obtained by this scheme was 97.13%.

Ge, M et al., [19] formulated a network IDS for the IoT through the acceptance of a custom-built DL technique. The IoT dataset also includes realistic attack traffic that includes data theft assaults, distributed denial of service attacks, denial of service attacks, and data collection. The dataset's high-dimensional classified features were also collected using a feed-forward neural networks approach with an embedding network. In addition, a binary classifier was created using a secondary feed-forward neural network model by using transfer learning to encode the data's highly dimensional categorical information. In the end, the technique produced classifiers that could distinguish between binary and multiple classes with excellent accuracy. Furthermore, a very extendable DNN was established for IoT systems for exposure to IoT botnet outbreaks. Finally, the method achieved high precision and accuracy when compared to other existing systems. This model offered an accuracy of 96.5%.

Qiu, H et al., [20] designed a method to produce adversarial network packets, and against DL-based Network Intrusion Detection Systems (NIDS) in NIDS. Also, when DL models were invisible to the opponents, the method had an impact on the model withdrawal procedure, permitting an effective attack. Additionally, the system used a saliency map to identify the important features. In addition, the assessments showed that successfully criticized the existing NIDS, kitsune. The average success rate of this model was 94.31%.

Islam, N et al., [21] developed a data analysis technique for intrusion detection in the IoT. In addition, many IoT threats, including shallow threats, use IDS. These threats include decision trees, support vector machines, random forests, deep machine learning, long short-term memories, deep belief networks, stacked LSTMs, and bidirectional LSTMs. Additionally, five different kinds of datasets were employed to assess the effectiveness of the machine learning-based IDS. Finally, it was discovered that IDSs using deep machine learning outperformed those using shallow machine learning to find IoT assaults. This method obtained the highest accuracy of 99.27%.

Alkahtani, H. and Aldhyani, T.H., [22] evaluated and developed DL algorithms to classify a long short-term memory, a CNN, hybrid convolution neural network with long short-term memory. In addition, the developed technology was enhanced and the network dataset's difficulty was minimized.

Additionally, the pertinent features from the network dataset were created using the particle swarm optimization technique. The method would be employed once the procedure was successfully performed on the selected dataset on a fresh variable dataset. The achieved accuracy of this technique was 98.80%.

Salih, A. A et al., [23] devised and investigated DL techniques that were highly effective in developing IDS for detecting different types of attacks. Furthermore, the method performed better and deals with big datasets than traditional machine learning algorithms. The method was compared with evaluating performance, feature learning, DL algorithms which were used to attack detection, and datasets used to determine the uses of employing network intrusion detection. The accuracy of this model was 96.3%.

Ge, M et al., [24] presented DL as an intelligent technique and it was a solution for the intrusion detection problem in IoT networks. In addition, it was classified traffic flow through DL concepts applications. Moreover, the arena evidence at the package level was adopted with the IoT dataset and generated generic features. Furthermore, multi and binary class classifications such as distributed denial of service, information theft occurrences, and investigation against IoT. Finally, the developed method achieved a high classification accuracy of 82% when analyzing the results.

Thamilarasu, G. and Chawla, S., [25] developed an intelligent IDS. In addition, the IoT environment was customized for the developed intelligent intrusion detection. Moreover, the method is used to identify anomalous behavior in IoT networks. A detection system that offers security as a service and promotes interoperability was also deployed, along with a variety of network communication protocols. Furthermore, the method was evaluated using real network traces for the purpose of proof of perception, and imitation was used for accommodating the scalability of evidence. Moreover, the method detected real-world intrusions perfectively. This model obtained a 97% recall rate and 95% average precision.

Li, D et al., [26] formulated a deep migration learning model-based IoT feature extraction and intrusion detection algorithm for intelligent cities, which combines DL and intrusion detection technology. In addition, the authors announced the relocation learning model and information feature extraction modeling scheme based on existing literature and algorithms. Moreover, the algorithm is then compared to existing algorithms. The testing findings show that the algorithm has a quicker detection time and greater detection efficiency of 95%.

Nathan Shone et al., [27] addressed a DL technique for intrusion detection. Moreover, a non-symmetric deep autoencoder (NDAE) was introduced for unsupervised feature learning. Moreover, the method was a DL organization model built with stacked NDAEs. Up to this point, the model had shown encouraging results, showing advancements over current methods and a great potential for usage in contemporary NIDSs. It obtained an accuracy of 89.22%.

Xiuzhang Yang et al., [28] introduced a lightweight IDS based on DL and knowledge graphs. The system extracts essential features and semantic links first using a knowledge graph and statistical analysis. IoT network queries were then translated into word vectors using feature alignment and multi-view feature fusion. Finally, a CNN- Bidirectional long short-term memory (BiLSTM) model with an attention-based architecture was developed to identify fraudulent request attacks by capturing contextual semantic information and long-distance reliance. The model outperforms the current approach in terms of model accuracy with a value of 90.01%, according to experimental results.

Xuan-Ha Nguyen et al., [29] presented Realguard, a DNN-based NIDS that operates directly on local gateways to protect IoT devices within the network. The approach was also superior since it quickly detected numerous cyberattacks with a minimal computational impact. The method was also made possible by the application of a quick feature extraction process and a powerful deep neural network-based attack detection model. Furthermore, the Real guard technique could reliably and in real-time detect ten different forms of attacks. The accuracy of the model was 99.57%.

Md Arafatur Rahman et al., [30] investigated and applied effective feature selection techniques to improve intrusion detection using machine learning methods. The approach was built on a central IDS that developed a model for spotting malicious and unusual activities in traffic employing feature selection, classification, and deep feature abstraction. Deep feature abstraction also used an unsupervised autoencoder, a DL approach of artificial neural networks, to create extra features for traffic. The experimental findings demonstrated that the Aegean Wi-Fi Intrusion Dataset had a high detection accuracy of 99.95% which was on par with earlier machine learning analyses of the same dataset.

Alkadi, O et al., [31] Deep Blockchain Framework (DBF) was introduced for IoT networks that provided security-based distributed intrusion detection and privacy-based blockchain with smart contracts. To provide privacy to the

distributed ID engines, the Ethereum library was used to develop privacy-based blockchain and smart contract methods. The experimental results demonstrated that the DBF framework outperformed the other competing theories when contrasted with peer privacy-preserving intrusion prevention strategies. The accuracy offered by this model was 98.54%.

Amir Basati et al., [32] introduced an asymmetric parallel auto-encoder (APAE), an intelligent network IDS based on an asymmetric parallel auto-encoder that detected various attacks in IoT networks. Lightweight architecture and two parallel encoders with three consecutive layers of convolution layers were also features of the APAE encoder. The APAE technique offered very strong generalization capability even after learning with very few training records and featured a lightweight and suitable structure for real-time attack detection. The highest accuracy of this model was 99.94%.

Chao Liang et al., [33] developed a hybrid placement method based on a multi-agent system, a blockchain, and DL algorithms used to design, implement, and test an IDS. In addition, the system was separated into four modules namely, data collection, data management, analysis, and response. The National Security Lab-KDD dataset, used for data mining and knowledge discovery was used to test the system. The findings demonstrated the potency of DL techniques in identifying transport layer threats. The evaluation is done based on accuracy with a value of 97%.

Almogren, A.S et al., [34] to realize the full potential of the IoT, an approach for quickly and accurately detecting intrusive activities in the EoT network. A DBN based on a sophisticated intrusion detection method is also recommended. Furthermore, they investigated various detection models using various DBN structures and associated them with existing recognition methods. According to test results, the system performed better accuracy of 85.73%.

Mohamed Abdel-Basset et al., [35] introduced a semi-supervised DL approach for intrusion detection (SS-Deep-ID), in which a multi-scale residual temporal convolutional (MS-Res) module was developed to fine-tune the network's capability in learning Spatio-temporal representations. Additionally, the SS-Deep-ID might be quickly integrated into a Fog-enabled IoT network to deliver effective real-time intrusion detection. Additionally, the SS-Deep-ID might be quickly integrated into a Fog-enabled IoT network to deliver effective real-time intrusion detection. Finally, experiential assessments on two new datasets showed that SS-Deep-ID improved intrusion detection efficiency and performance robustness while maintaining computational efficiency. It achieved the highest accuracy of 92.47%.

Li, B et al., [36] devised a Deep Fed, federated DL scheme for detecting cyber threats against industrial cyber-physical systems (CPSs). Additionally, start by creating an industrial CPS-specific DL-based intrusion detection model utilizing a CNN and a deep neural unit. Moreover, the second was to develop a federated learning framework that enabled several industrial CPSs to work together while respecting privacy to develop an extensive intrusion detection model. Extensive tests on an actual industrial CPS dataset also show the DeepFed scheme's great performance in identifying different kinds of cyber threats to industrial CPSs and its superiority over leading-edge methods. This approach achieved high accuracy, precision, recall, and F-score of 0.9920 0.9885, 0.9747, and 0.9814, respectively.

Balakrishnan, N et al., [37] developed an intelligent technique or methodology with the enhancement of DL algorithms that defend against security breaches. The approach of intelligent intrusion detection looks for malicious activities on the network and tries to enter. Also included was the inquiry about incorporating the DL approach. Results were compared between the regular IDS algorithms and the DBN security network upgrade. The precision, recall, and F1-score obtained by this approach were 86.21%, 74.61%, and 79.99%.

(b) CNN-based methods

The CNN algorithm is the most well-known and extensively used one in the arena of DL. The fundamental advantage of CNN over its forerunners is that it does it without human intervention, automatically identifying the pertinent features. Many various domains, including computer vision, audio processing, face recognition, etc., have made substantial use of CNNs. CNNs have a structure akin to a traditional neural network and were modeled after the neurons found in human and animal brains. This section presents the CNN-based methods of Intrusion detection in IoT: Yadav, N et al., [5] developed a Deep-Convolutional-Neural-Network (DCNN) based IDS. The suggested model seeks to boost efficiency while using less computing power. Then, the model was subjected to a variety of optimization techniques, and the performance of Adam, AdaMax, and Nadam was found to be optimal. In addition, the model was also contrasted with a number of sophisticated DL and conventional ML methods. Finally, the experimental analysis demonstrated that the method was more dependable and had higher accuracy of 99.84% than existing DL-based algorithms.

Qazi, E.U.H et al., [38] presented a One-Dimensional CNN (1D-CNN) for the identification of normal and different types of malicious network

traffic. Additionally, the approach was able to identify four distinct forms of the most frequent network invasions, including PortScan, a positive assault, and DDoS, DoS Hulk, and DoS Golden Eye, which are all active attack types. Moreover, the required purpose, the benchmark of the dataset was used for conducting the experiments. Using the current DL techniques and a 1D-CNN-based architecture, the multiclass arrangement was performed with high accuracy of 98.96%.

Antunes, M et al., [39] established a comparative study about using DL methods to detect network intrusions. Moreover, principal component analysis (PCA) and Autoencoder approaches were implemented to detect geographies discount in the unique dataset and overall detection performance. Finally, it was also able to draw the conclusion that feature reduction techniques did not affect overall detection performance, allowing processing times to be slashed without compromising overall detection performance accuracy. The highest accuracy, precision, recall, and F-measure of this model were 99.85%, 99.70%, 99.94%, and 99.77%, respectively.

Wang, Y et al., [40] developed a IoT-based DL-based network intrusion detection to the environment of the IoT. Initially, the detection of IoT was constructed based on edge computing. In addition, the researchers introduced the concept of gated convolution for improved CNN. Furthermore, data were passed through pooling, full connection, convolution layer, dropout, and softmax function was used to understand information multi-classification. Moreover, the Focal Loss function was used to control the exercise ratio of confident and adverse trials. Finally, the results showed that high accuracy of 92.14%, recall of 95.97%, F1-values of 90.89%, and precision of 90.03% when compared to other contrast algorithms.

Zhong, M et al., [9] the methods were developed by the features of the model by using the key point of the sequential model. The model collected structures from the application layer through system routines and the network layer through tcpdump packets. Moreover, the GRU and Text-CNN methods were selected since treat sequential data by means of the language model. Furthermore, the research showed that the DL methods consumed higher F1-score, and removes more structures from the data when the advantages compared with other modern methods. Finally, the researchers determined that consecutive model-based IDS by using DL methods gave security to the IoT servers with an accuracy of 97.8%.

Fatani, A et al., [41] introduced selection methods and feature extraction for the IoT IDS. In addition, capitalized proceed of DL techniques and Swarm Intelligence (SI) algorithms. Moreover, the designed CNN-based

feature abstraction technique was practical to obtain the input datasets. Furthermore, extensive evaluation was carried out with several algorithms to prove the inexpensive presentation of the established technique. Finally, the outcomes showed that high presentation of the established method by using dissimilar assessment gauges. The achieved accuracy of this approach was 91.6%.

Smys, S et al., [12] an IDS was used to detect several kinds of attacks through hybrid CNN and it was applicable for an extensive collection of IoT applications. The method was authorized and associated with conventional DL and machine learning models. Finally, the method proved more complex to occurrences in the IoT system when compared to other technical methods. The detection accuracy of this model was 98%.

Derhab, A et al., [42] identified five design principles for the development of DL-based intrusion detections for IoT. The Temporal Convolution Neural Network (TCNN), a DL architecture for IoT IDSs that blends casual difficulty with CNN, was developed based on the concepts. In addition, to handle unbalanced datasets, TCNN was combined with Synthetic Minority Oversampling Technique-Nominal Continuous (SMOTE-NC). Additionally, actual feature engineering methods like feature space reduction and feature transformation are combined with it. According to experimental findings, TCNN successfully balanced effectiveness and efficiency. When confirmed on the Bot-IoT dataset, it outstrips cutting-edge DL IDSs and records an accuracy rate of 99.9986%.

Lingjun Zhao et al., [43] treated the RSS signal as an RSS-image matrix and then performed a background removal process to isolate the variation component with distinguishing features. It was also planned to use a deep CNN to dynamically extract features for categorization. Utilizing a real-world dataset of outdoor DFL, the localization performance of the elimination-based CNN (BE-CNN) method was verified. The results of the experiments demonstrated that the approach had a distinct benefit in terms of enhancing DFL localization resilience and accuracy. BE-based approaches exceed all similar raw data-based methods in terms of localization accuracy. Furthermore, the approach beat rival approaches including DNNs with autoencoder, K-Nearest-Neighbor (KNN), Support Vector Machines (SVM), and others in terms of localization accuracy and robustness. The offered localization accuracy of this approach was 100%.

Yanmiao Li et al., [44] introduced a multi-CNN fusion method for DL intrusion detection. Additionally, CNN was added to the intrusion detection issue using the flow data visualization approach, and the top four results

stand out. The experimental outcomes convincingly show that the multi-CNN fusing framework was well suited for offering a high precision and low complication classification approach on the NSL-KDD dataset. Furthermore, it outperformed both conventional machine learning techniques and other contemporary DL approaches in terms of binary categorization and multiclass classification with an accuracy of 86.95%.

Xingbing Fu et al., [45] used the Fast Gradient Sign Method (FGSM) to generate adversarial examples in the paper to test the robustness of three intrusion detection models based on CNN, LSTM, and GRU. Additionally, three different training techniques were used: the first involved training the models with regular examples, the second involved training the models with adversarial attacks, and the third involved first training the designs with regular examples and then training the models with adversarial attacks. In addition, the efficiency of the 3 variables was examined under various training techniques, and it was shown that CNN performed the best under regular training for adversarial instances. After engaging in adversarial training, GRU and LSTM's robustness to adversarial cases significantly increased. The accuracy, precision, recall, and F1-measure attained by this approach were 83.02%, 81.29%, 83.02%, and 81.46%, respectively.

Imtiaz Ullah et al., [46] implemented a model for anomaly-based intrusion detection in IoT networks that detects and classifies binary and multiclass IoT network data using a CNN and GRU. The binaries and classifier recognition system surpassed the opposition with an accuracy of 99.20%.

(c) Optimization-based methods

To find solutions that maximize or decrease certain research criteria, such as minimizing expenses associated with producing a thing or service, maximizing profits, minimizing the number of raw materials needed to make a good, or maximizing output, optimization techniques are often used. Here, the optimization-based methods of intrusion detection in IoT are explained: Baniasadi, S et al., [3] introduced an algorithm of training for superior tuning of the parameters of the deep architecture. Additionally, the neighborhood search-based particle swarm optimization (NSBPSO) algorithm, a modified version of the Particle Swarm Optimization (PSO) technique, was added to the method to enhance its exploitation and exploration capabilities. The method's faultless training of the deep architecture as a network intrusion detector allowed for improved performance and accuracy. Finally, the method achieved high accuracy of 98.09% and high performance compared with other existing techniques.

Jothi, B. and Pushpalatha, M., [47] presented an IDS by using powerful DL models. Additionally, the broad IDS calculations were made in terms of authentication techniques and enlarged metrics of the various IoT threat situations. The unlike properties of typical harmful nodes in the network were also assessed. Finally, the method gained high precision of 99.5%, accuracy of 98.7%, and recall of 98.45%, when equaled to traditional approaches.

Zhang, Y et al., [48] established the improved Genetic Algorithm combined with a deep belief network. Furthermore, the genetic algorithm underwent numerous iterations to counteract different kinds of attacks. And when the ideal number of hidden layers and the number of neurons in each layer were created adaptively, the intrusion detection method on the DBN was able to obtain high detection rates. In addition, the algorithm was evaluated and simulated by using the NSL-KDD dataset. When the intrusion detection model was integrated with the DBN, the strategy reduced network complexity and enhanced the rate of attack intrusion recognition. The accuracy, precision, and recall of this model were 98.68%, 98.20%, and 98.2%.

Idrissi, I et al., [49] presented a DL -Based Host-Intrusion Detection System (DL-HIDS) for the analysis of the probability to deploy some specific commercial IoT devices. In addition, the method achieved several optimizations based on the types of user devices to reach restricted hardware provisions. Furthermore, to achieve which model was fitted correctly to the developed method and to expect which IDS was made and expectedly deploy the features of devices. The obtained accuracy of this approach was 99.74%.

Dahou, A et al., [50] devised a method for IDS of the IoT and cloud environments. The key idea is to develop reliable extraction of features and selection methods by utilizing the abundance of DL meta-heuristic optimization algorithms. As a feature extractor, CNN was initially used to develop more accurate and pertinent approximations of the data input in a reduced dimensional space. Additionally, the Reptile Search Algorithm (RSA) was used to choose the best feature to reduce data dimensionality and improve classification accuracy with a value of 92.040%. Comparing the framework to other recognized optimization techniques used for feature collection challenges, it demonstrated competitive performance in classification metrics.

Tharewal, S et al., [51] introduced deep reinforcement learning algorithm (DRL)-based IDS which was used to a feature selection algorithm based on LightGBM, which well removes the most absorbing feature set in the Industrial Internet of Things data; an Industrial Internet of Things intrusion

detection model was made through the Proximal Policy Optimization (PPO) algorithm. Furthermore, a vast number of trials' findings have demonstrated that IDS DRL GDS is effective in identifying different forms of malicious activities on the Commercial IoT. It performed better than the current IDS using DL in regard to an accuracy of 97.2%.

(d) Other approaches

de Souza, C. A et al., [52] developed a hybrid method of binary classification called DNN-KNN, with high recall rates and high accuracy and recovery rates for composing the first level of the two-stage detection of the presented architecture. The method was founded on the KNN algorithm and DNN. The technology also operated with little processing and memory expenses and achieved higher precision when compared to both traditional machine learning techniques and recent advancements in IoT systems. The accuracy obtained by this approach was 99.85%.

Yanqing Yang et al., [53] developed Improved Conditional Variation AutoEncoder (ICVAE)-DNN, an intrusion detection model that combined an ICVAE and a DNN. To find and examine probable segmentation methods of data transmission features and classes, ICVAE is employed. Three well-known oversampling techniques are outperformed by ICVAE-DNN, a data augmentation technique for DNN. Furthermore, the ICVAE-DNN outstripped the nine existing ID methods in relation to overall accuracy with a value of 96.5%.

S. K. B Sangeetha et al., [54] the transport layer of IoT networks was secured in the paper using a multilayered security approach based on DL. The multi-layered approach was evaluated using ID datasets from CIC-IDS-2018, ToN-IoT, and BoT-IoT. Eventually, based on the analyzed criteria, the new model performed better than the current approaches and attained a high level of accuracy of 98%.

Rodriguez, E et al., [15] introduced a method named Transfer Learning (TL) based intrusion detection, model refinement, and knowledge transfer for the observation of zero-day attacks, in the 5G IoT network with scare labeled dataset and unbalanced datasets. In addition, the method created three specialized datasets. Furthermore, the investigational consequences showed that TL based framework achieved the best accuracy of 98.85%.

Khalid Albulayhi et al., [55] examined DL approaches for IDSs in the IoT and the datasets associated with them in order to identify gaps, weaknesses, and neutral reference architecture. The evaluation was done based on accuracy with a value of 86.5%.

3 Research Gaps Identified

In [5], the CNN technique cannot distinguish the multi-class attacks' sub-categories in the network. One dimensional CNN technique was introduced in [38], but the method failed to use methods, like PCA, Independent Component Analysis (ICA), Autoencoders, and others. In [39], CNN was developed and this learning architecture was not extended to assess the impact of an ensemble-based model and omitted using other publicly available IDS datasets besides CSE-CIC-IDS2018 to evaluate the learning architecture. Moreover, the method failed to use the same knowledge approach and contrast the outcomes with network drifts. In [40], the DL technique was established and the method needed more infeasible technically and economically to concentrate the continuous-growing edge data to one or several data computing centers to complete the corresponding data computing tasks. The CNN technique was formulated in [41], and the method ignored different DL architectures and swarm intelligence techniques for IDS in the IoT environment.

In [12], CNN the technique was introduced. Furthermore, because it was not created for this purpose, the DNN-KNN method is incapable of noticing directing occurrences. The DL technique failed to take into account testing the IDS's [42] resistance to adversarial attacks, which can mislead the DL model and cause it to make inaccurate predictions. In [43], a background elimination (BE)-based BE-CNN was introduced. But robust principal component analysis method that can handle data with outliers was not developed. In [44], DL was established and the method neglected to take into account approaches aimed at DL fusion and online learning for the network intrusion detection problem, which can intelligently protect industrial IoT data. In [45], various methods named CNN, LSTM, and GRU were introduced. But the method failed to employ more sophisticated methods of classifier attack and defense to test the model's robustness, such as when adversarial training is done with a Generative adversarial network (GAN). CNN and DL were introduced in [46], and these methods were not taken into account attacks using different generative adversarial networks and DL models, and then contrasting the outcomes with the current model.

In [16], the DL algorithm was developed. In addition, the technique failed to use a computational resource-saving stack-based auto-encoder method. Moreover, the optimization of computational time can also receive more attention. In [6], blockchain and DL techniques were formulated. But the methods failed to take into account an information set of uncommon

occurrence types developed and used to train the ID model. DL-IDS technique was introduced in [11], moreover, the method failed to evaluate DL-IDS using various datasets, including KDD-99 and UNSW-NB 15, and classifiers such as Naive Bayes, decision trees, and random forests. In [8], the DL technique was established but the method failed to create models using various machine learning or DL algorithms or to combine several of them. In [18], the deep neural network was developed. But, the method failed to create models using various machine learning or DL algorithms or to combine several of them. In [19], the DL technique was introduced but the method failed to improve the classifier to operate in real-time for intrusion detection. DL method was established in [56]. The strategy fell short of efficiently and more effectively analyzing the routine traffic information records on the many types of future IoT devices to identify further unidentified botnet attacks.

In [20], the DL technique was established and the method failed to take into account looking into mitigation options to improve how robust DL models are at detecting intrusions. DL was developed in [22], and the system was evaluated and developed using a new real standard dataset generated from the IoT environment. DNN was introduced in [23]. By comparing and choosing features from other well-known and benchmark data sets, the system was unable to improve this strategy. In [24], DL was formed but the method failed to distinguish between each subcategory of attacks using a classifier. In [25], the DL technique was developed and the method failed to identify additional IoT attack types, such as location-based attacks like device ID cloning, spoofing, and Sybil attacks. In [26], the deep migration learning technique was established and the method needed to study how to modify the classifier in real-time with the inflow of data so that the model has better applicability. In [27], NDAE was introduced. The method failed to build on our previous analyses by using actual backbone network traffic to show the extended model's benefits.

In [28], the DL technique was developed and the method failed to construct a network IDS based on knowledge graphs and DL for larger-scale network traffic. In [29], DNN was introduced. For Real Guard to train the attack detection model, the traffic data was not properly labeled, which was considered a major drawback. In [31], DBF was developed. The method failed to apply the outline to various practical datasets to assess its usefulness and scalability. In [36], the DeepFed was developed. Federating data resources from various industrial CPSs across domains did not successfully address cyber security issues, which is considered a challenge. In [47], DL was introduced and the major drawback was in order to design more effective

IDS in IoT networks, hybrid learning models and feature optimization techniques will be necessary. In [48], a genetic algorithm was introduced and the deep network's other parameters, including those that would have cut training time and increased accuracy, were not optimized. In [49], a DL-HIDS was introduced and the method cannot generalize due to the differences between the devices that are currently on the market, which range from small sensors to high-definition cameras.

In [52], the DNN-KNN technique was developed and the method failed to look into mitigation options to improve the DL models' robustness in intrusion detection. ICVAE-DNN technique was introduced in [53]. In this technique, the spatial distribution of ICVAE latent variables was not explored using the adversarial learning method to improve input sample reconstruction. The reinforcement learning method was developed in [51], and the method is absent of investigation into Industrial IoT intrusion detection distributed architecture-based systems. In [15], transfer learning was established and also the method failed to extend the developed solution to the detection of other types of zero-day attacks and take into account real data from IoT networks. In [55], the established method is named a machine learning technique. Real-time sensor information from smart city apps can also be gathered and used to do machine-learning data analytics to uncover IoT security assaults, which is another technique flaw.

4 Analysis and Discussion

This section uses numerous research articles to show the analysis and debate of intrusion detection in the Internet of Things. These papers are categorized by the datasets used, the methodologies used, the performance evaluation metrics used, and the years were published.

4.1 Analysis Based on Methods

This section provides a summary of the analysis and debate of intrusion detection in the Internet of Things based on the datasets used, method classification, performance evaluation metrics, and publication years. The methods developed for Intrusion detection in IoT are shown in Figure 2. Figure 2, it is determined that 54% of research papers used Deep Neural Network methods, 24% of research papers used CNN methods, 10% of research papers utilized Optimization-based methods, and other methods are utilized 12% of research papers respectively.

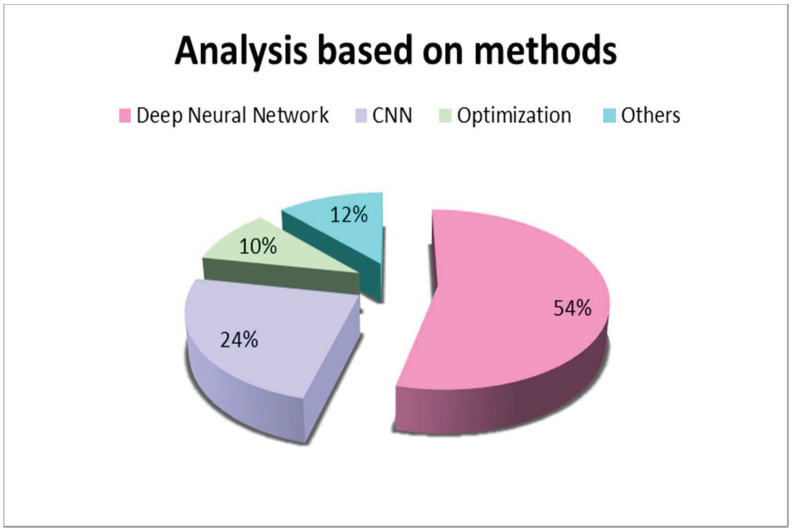

Figure 2 Methods developed for the intrusion detection in IoT.

4.2 Analysis in Terms of Employed Datasets

The analysis performed using datasets used for IoT intrusion detection is described in this section. Figure 3 displays the several datasets that were used for IoT intrusion detection. The usually used dataset in intrusion detection is Combined DDoS and Car-Hacking Dataset [55], UNSW-NB15 [8, 16, 19, 22, 24, 31, 32, 55], IoTID20 [5, 20, 21, 54], NSL-KDD [21, 26–28, 31, 33, 34, 41, 50, 52, 54], UNSW-NB16 [3], CICIDS2017 [1, 29, 32, 36, 38, 41], CSE-CICIDS2018 [1, 32, 36, 39, 50, 52], KDD99 [6, 9, 17, 28, 32, 37, 40], BoT-IoT [3, 8, 16, 19, 21, 31, 36, 41, 48, 50, 52, 54], ADFA-LDCIDDS-001 [9], MQTT-IoT-IDS2020 [18, 32, 54], IoTDevNet [21], DS2OS [21], Aegean Wi-Fi intrusion Dataset [30], outdoor – Device-Free Localization (DFL) [54], ToN-IoT [23], IoT-23 [24], and real industrial CPS dataset [25]. The most frequently used datasets, according to Figure 3, are BOT-IOT and NSL-KDD.

4.3 Analysis in Terms of Toolsets

The tools used for IoT intrusion detection are shown in this section. Figure 4 shows the IoT toolsets for intrusion detection. Python and MATLAB software toolkits were used to create the study articles. Based on Figure 4, it is clearly realized that Python software is often used software system for the ID in IoT.

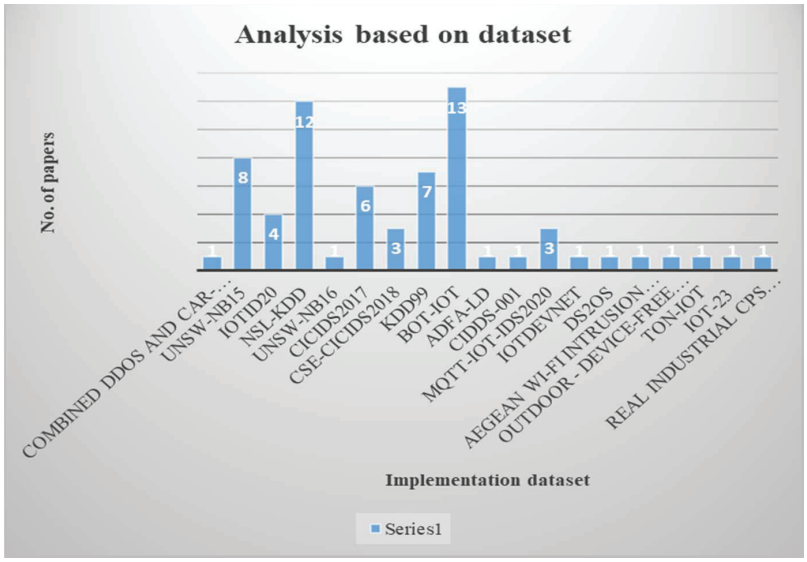

Figure 3 Dataset used for intrusion detection in IoT.

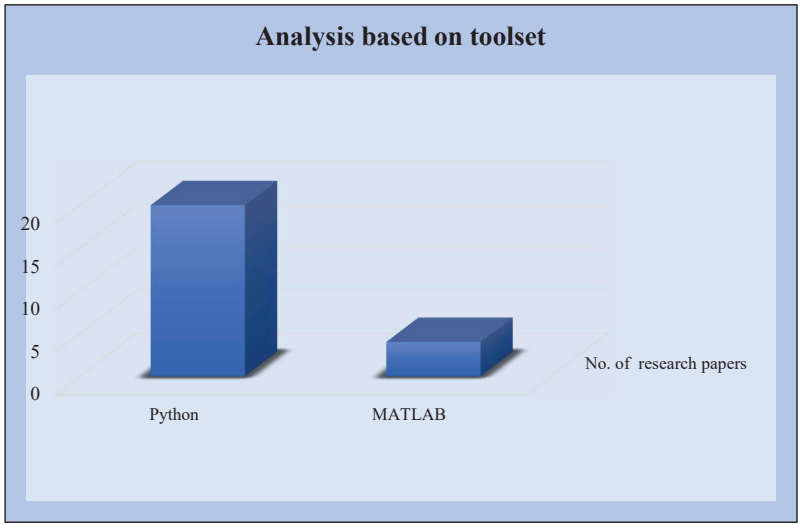

Figure 4 Toolsets used for the intrusion detection in IoT.

4.4 Analysis Based on Publication Years

This part serves as an example of the analysis based on previously published years, which examines 50 research articles for intrusion detection in IoT.

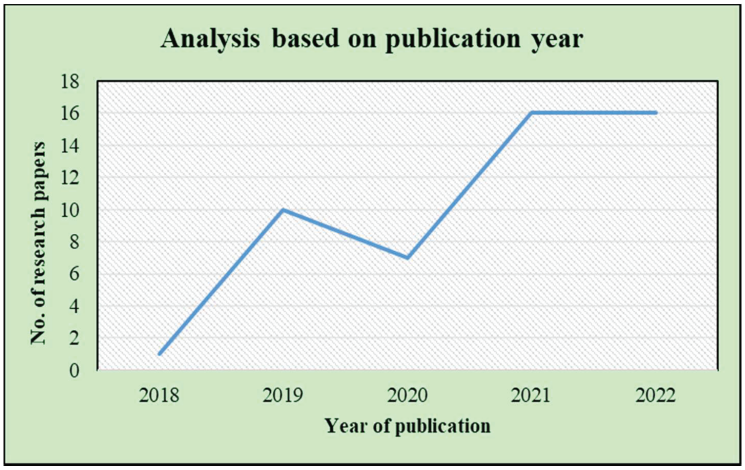

Figure 5 Investigation based on publication years.

Figure 5 illustrates the study based on reported years. Out of the 50 research papers that were assessed, more were published in 2021.

4.5 Analysis in Terms of Metrics Evaluation

In this part, the analysis based on performance measures is provided. For IoT intrusion detection, evaluation parameters including Accuracy, Precision, Recall, F1-score, False Alarm Rate, Sensitivity, Specificity, and False Positive Rate are taken into consideration. Accuracy is a frequently used performance statistic, as seen in Table 1.

4.6 Analysis Using the Values of the Evaluation Metrics

The analysis based on the evaluation metrics value is projected in this subdivision. Here, the evaluation in terms of Intrusion detection in IoT is represented.

4.6.1 Analysis by means of accuracy metric

This section uses Table 2 to illustrate the analysis using the accuracy metric. Furthermore, this table represents the evaluation in terms of intrusion detection in IoT for accuracy specified by three ranges as, 70%–80%, 81%–90%, and 91%–99%. From, the below table it is recognized that the maximum research papers obtained a better accuracy value of 91%–99%, and the research paper [45] had less accuracy value in the range of 70%–80%.

Table 1 Investigation based on evaluation metrics

Performance Metrics	Number of Research Papers
Accuracy	[1, 3, 5, 6, 8, 11, 15–19, 21–24, 27–36, 38–40, 42–54, 56]
Precision	[1, 5, 8, 11, 15, 17, 19, 21, 22, 24, 25, 27, 28, 32, 33, 35–39, 41, 42, 44–46, 50–54, 56]
Recall	[1, 5, 11, 15, 17, 19, 21, 24, 25, 27, 28, 32, 33, 35–42, 44–46, 50–54, 56]
F1-score	[1, 5, 9, 15, 18, 19, 21, 22, 24, 27, 28, 30, 33, 35–37, 40–42, 45, 46, 50–53, 56]
False Alarm Rate	[16, 17, 28, 30, 38]
Sensitivity	[3, 22, 47]
Specificity	[3, 22, 47]
False positive rate	[44, 53]

Table 2 Investigation based on accuracy metric

Accuracy	Number of Research Papers
70%–80%	[45]
81%–90%	[17, 34, 53]
91%–99%	[1, 3, 5, 6, 11, 12, 15, 16, 18, 19, 22–25, 29, 30, 32, 36–40, 42, 46–49, 51, 54, 56]

Table 3 Investigation based on precision metric

Precision	Number of Research Papers
80%–90%	[17, 45, 53]
91%–99%	[1, 5, 11, 15, 22, 25, 32, 36, 37, 39, 40, 42, 46, 50–52, 54]

4.6.2 Analysis using precision metric

This section uses Table 3 to illustrate the analysis using accuracy metrics. Furthermore, this table describes the appraisal in terms of Intrusion detection in IoT for precision is specified by two ranges as, 80%–90%, and 91%–99%. From, the below table it is recognized that the maximum research papers obtained a better precision value of 91%–99%, and the research paper [17, 45, 53] had less precision value in the range of 80%–90%.

4.6.3 Analysis using recall metric

This section uses Table 4 to illustrate the analysis using the recall measure. Additionally, this table shows the assessment in terms of intrusion detection in IoT for recall is specified by three ranges as, 70%–80%, and 81%–90%.

Table 4 Analysis based on recall metric

Recall	Number of Research Papers
70%–80%	[45]
81%–90%	[40]
91%–99%	[1, 5, 11, 15, 17, 25, 32, 36, 37, 39, 42, 46, 50–54]

From, the below table it is recognized that the maximum research papers obtained better recall value with 91%–99% and the research paper [45] had less precision value in the range of 70%–80%.

5 Conclusion

In this work, a survey of several IoT intrusion detection techniques is conducted. The reviews are from 50 research publications, and the gathered papers are categorized according to different methodologies, such as DNN-based methods, CNN-based methods, Optimization methods, and so on. In addition, a variety of resources were employed to compile the research papers for this survey, including Google Scholar, Institute of Electrical and Electronics Engineers (IEEE), Science Direct, and others. Here, the attained investigative papers are examined, and the shortcomings of the previous research papers are shown. Furthermore, the categorization methods, toolkits, datasets, and assessment metrics employed in the analysis of the survey are displayed. This study makes it quite evident that the majority of research articles use the DNN approach. Also, Python is a popular software tool for IoT intrusion detection, and the BOT-IOT dataset is a commonly used dataset. Furthermore, the majority of research publications employ accuracy as their primary performance criterion. In addition, this survey recommends future work for IoT intrusion detection by taking into account various research difficulties and gaps.

Conflict of Interest

The authors declare that there will be no conflict of interest.

Data Availability Statement

No datasets were generated or analyzed during the current study.

References

[1] Ullah, S., Khan, M.A., Ahmad, J., Jamal, S.S., e Huma, Z., Hassan, M.T., Pitropakis, N. and Buchanan, W.J.,"HDL-IDS: a hybrid deep learning architecture for intrusion detection in the Internet of Vehicles", Sensors, vol. 22, no. 4, p. 1340, 2022.

[2] Belli, L., Cirani, S., Davoli, L., Gorrieri, A., Mancin, M., Picone, M. and Ferrari, G., "Design and deployment of an IoT application-oriented testbed", Computer, vol. 48, no. 9, pp. 32–40, 2015.

[3] Baniasadi, S., Rostami, O., Martín, D. and Kaveh, M.,"A Novel Deep Supervised Learning-Based Approach for Intrusion Detection in IoT Systems", Sensors, vol. 22, no. 12, p. 4459, 2022.

[4] Zhang, Y., Li, P. and Wang, X., "Intrusion detection for IoT based on improved genetic algorithm and deep belief network", IEEE Access, vol. 7, pp. 31711–31722, 2019.

[5] Rodríguez, E., Valls, P., Otero, B., Costa, J.J., Verdú, J., Pajuelo, M.A. and Canal, R., "Transfer-Learning-Based Intrusion Detection Framework in IoT Networks", Sensors, vol. 22, no. 15, p. 5621, 2022.

[6] Liang, C., Shanmugam, B., Azam, S., Jonkman, M., De Boer, F. and Narayansamy, G., "Intrusion detection system for Internet of Things based on a machine learning approach", In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), pp. 1–6, IEEE, March, 2019.

[7] Ezechina, M.A., Okwara, K.K. and Ugboaja, C.A.U., "The Internet of Things (Iot): a scalable approach to connecting everything", The International Journal of Engineering and Science, vol. 4, no. 1, pp. 09–12, 2015.

[8] Susilo, B. and Sari, R.F.,"Intrusion detection in IoT networks using deep learning algorithm", Information, vol. 11, no. 5, p. 279, 2020.

[9] Zhong, M., Zhou, Y. and Chen, G., "Sequential model based intrusion detection system for IoT servers using deep learning methods", Sensors, vol. 21, no. 4, p. 1113, 2021.

[10] Balasubramanian, V., Zaman, F., Aloqaily, M., Al Ridhawi, I., Jararweh, Y. and Salameh, H.B., "A mobility management architecture for seamless delivery of 5G-IoT services", In ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1–7, IEEE, May, 2019.

[11] Otoum, Y., Liu, D. and Nayak, A.,"DL-IDS: a deep learning–based intrusion detection framework for securing IoT", Transactions on

Emerging Telecommunications Technologies, vol. 33, no. 3, p. e3803, 2022.

[12] Smys, S., Basar, A. and Wang, H., "Hybrid intrusion detection system for internet of things (IoT)", Journal of ISMAC, vol. 2, no. 04, pp. 190–199, 2020.

[13] Sandhu, K.S., Lozada, D.N., Zhang, Z., Pumphrey, M.O. and Carter, A.H., "Deep learning for predicting complex traits in spring wheat breeding program", Frontiers in Plant Science, vol. 11, p. 613325, 2021.

[14] Mighan, S.N. and Kahani, M., "A novel scalable intrusion detection system based on deep learning", International Journal of Information Security, vol. 20, no. 3, pp. 387–403, 2021.

[15] Rodríguez, E., Valls, P., Otero, B., Costa, J.J., Verdú, J., Pajuelo, M.A. and Canal, R., "Transfer-Learning-Based Intrusion Detection Framework in IoT Networks", Sensors, vol. 22, no. 15, p. 5621, 2022.

[16] Yadav, N., Pande, S., Khamparia, A. and Gupta, D., "Intrusion detection system on IoT with 5G network using deep learning", Wireless Communications and Mobile Computing, 2022.

[17] Bhor, H.N. and Kalla, M.,"TRUST-based features for detecting the intruders in the Internet of Things network using deep learning", Computational Intelligence, vol. 38, no. 2, pp. 438–462, 2022.

[18] Khan, M.A., Khan, M.A., Jan, S.U., Ahmad, J., Jamal, S.S., Shah, A.A., Pitropakis, N. and Buchanan, W.J., "A deep learning-based intrusion detection system for mqtt enabled iot", Sensors, vol. 21, no. 21, p. 7016, 2021.

[19] Ge, M., Syed, N.F., Fu, X., Baig, Z. and Robles-Kelly, A., "Towards a deep learning-driven intrusion detection approach for Internet of Things", Computer Networks, vol. 186, p. 107784, 2021.

[20] Qiu, H., Dong, T., Zhang, T., Lu, J., Memmi, G. and Qiu, M., "Adversarial attacks against network intrusion detection in iot systems", IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10327–10335, 2020.

[21] Islam, N., Farhin, F., Sultana, I., Kaiser, M.S., Rahman, M.S., Mahmud, M., Hosen, A.S. and Cho, G.H., "Towards machine learning based intrusion detection in IoT networks", Comput. Mater. Contin, vol. 69, no. 2, pp. 1801–1821, 2021.

[22] Alkahtani, H. and Aldhyani, T.H., "Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms", Complexity, 2021.

[23] Zeeshan, M., Riaz, Q., Bilal, M.A., Shahzad, M.K., Jabeen, H., Haider, S.A. and Rahim, A., "Protocol-Based Deep Intrusion Detection for DoS

and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets", IEEE Access, vol. 10, pp. 2269–2283, 2021.

[24] Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G. and Robles-Kelly, A., "Deep learning-based intrusion detection for IoT networks. In 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC), pp. 256–25609, IEEE, December, 2019.

[25] Thamilarasu, G. and Chawla, S., "Towards deep-learning-driven intrusion detection for the internet of things", Sensors, vol. 19, no. 9, p. 1977, 2019.

[26] Li, D., Deng, L., Lee, M. and Wang, H., "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning", International journal of information management, vol. 49, pp. 533–545, 2019.

[27] Shone, N., Ngoc, T.N., Phai, V.D. and Shi, Q., "A deep learning approach to network intrusion detection", IEEE transactions on emerging topics in computational intelligence, vol. 2, no. 1, pp. 41–50, 2018.

[28] Yang, X., Peng, G., Zhang, D. and Lv, Y., "An Enhanced Intrusion Detection System for IoT Networks Based on Deep Learning and Knowledge Graph", Security and Communication Networks, 2022.

[29] Nguyen, X.H., Nguyen, X.D., Huynh, H.H. and Le, K.H., "Realguard: A lightweight network intrusion detection system for IoT gateways", Sensors, vol. 22, no. 2, p. 432, 2022.

[30] Rahman, M.A., Asyhari, A.T., Wen, O.W., Ajra, H., Ahmed, Y. and Anwar, F., "Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection", Multimedia Tools and Applications, vol. 80, no. 20, pp. 31381–31399, 2021.

[31] Alkadi, O., Moustafa, N., Turnbull, B. and Choo, K.K.R., "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks", IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9463–9472, 2020.

[32] Basati, A. and Faghih, M.M., "APAE: an IoT intrusion detection system using asymmetric parallel auto-encoder", Neural Computing and Applications, pp. 1–21, 2020.

[33] Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., Kavianpour, S. and Idris, N.B., "Intrusion detection system for the internet of things based on blockchain and multi-agent systems", Electronics, vol. 9, no. 7, p. 1120, 2020.

[34] Almogren, A.S., "Intrusion detection in Edge-of-Things computing", Journal of Parallel and Distributed Computing, vol. 137, pp. 259–265, 2020.

[35] Abdel-Basset, M., Hawash, H., Chakrabortty, R.K. and Ryan, M.J., "Semi-supervised spatiotemporal deep learning for intrusions detection in IoT networks", IEEE Internet of Things Journal, vol. 8, no. 15, pp. 12251–12265, 2021.

[36] Li, B., Wu, Y., Song, J., Lu, R., Li, T. and Zhao, L., "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems", IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5615–5624, 2020.

[37] Balakrishnan, N., Rajendran, A., Pelusi, D. and Ponnusamy, V., "Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things", Internet of things, vol. 14, p. 100112, 2021.

[38] Qazi, E.U.H., Almorjan, A. and Zia, T.,"A One-Dimensional Convolutional Neural Network (1D-CNN) Based Deep Learning System for Network Intrusion Detection", Applied Sciences, vol. 12, no. 16, p. 7986, 2022.

[39] Antunes, M., Oliveira, L., Seguro, A., Veríssimo, J., Salgado, R. and Murteira, T.,"Benchmarking Deep Learning Methods for Behaviour-Based Network Intrusion Detection", In Informatics, Vol. 9, No. 1, p. 29. MDPI, March, 2022.

[40] Wang, Y., Wang, J. and Jin, H., "Network Intrusion Detection Method Based on Improved CNN in Internet of Things Environment", Mobile Information Systems, 2022.

[41] Fatani, A., Dahou, A., Al-Qaness, M.A., Lu, S. and Elaziz, M.A., "Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system", Sensors, vol. 22, no. 1, p. 140, 2021.

[42] Derhab, A., Aldweesh, A., Emam, A.Z. and Khan, F.A., "Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering", Wireless Communications and Mobile Computing, 2020.

[43] Zhao, L., Su, C., Huang, H., Han, Z., Ding, S. and Li, X., "Intrusion detection based on device-free localization in the era of IoT", Symmetry, vol. 11, no. 5, p. 630, 2019.

[44] Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., Zhao, Y. and Cui, L., "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion", Measurement, vol. 154, p. 107450, 2020.

[45] Fu, X., Zhou, N., Jiao, L., Li, H. and Zhang, J., "The robust deep learning–based schemes for intrusion detection in Internet of Things environments", Annals of Telecommunications, vol. 76, no. 5, pp. 273–285, 2021.

[46] Ullah, I., Ullah, A. and Sajjad, M., "Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks", IoT, vol. 2, no. 3, pp. 428–448, 2021.

[47] Jothi, B. and Pushpalatha, M., "WILS-TRS—A novel optimized deep learning based intrusion detection framework for IoT networks", Personal and Ubiquitous Computing, pp. 1–17, 2021.

[48] Zhang, Y., Li, P. and Wang, X., "Intrusion detection for IoT based on improved genetic algorithm and deep belief network", IEEE Access, vol. 7, pp. 31711–31722, 2019.

[49] Idrissi, I., Azizi, M.M. and Moussaoui, O., "A lightweight optimized deep learning-based host-intrusion detection system deployed on the edge for IoT", International Journal of Computing and Digital System, 2022.

[50] Dahou, A., Abd Elaziz, M., Chelloug, S.A., Awadallah, M.A., Al-Betar, M.A., Al-qaness, M.A. and Forestiero, A., "Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm", Computational Intelligence and Neuroscience, 2022.

[51] Tharewal, S., Ashfaque, M.W., Banu, S.S., Uma, P., Hassen, S.M. and Shabaz, M., "Intrusion detection system for industrial Internet of Things based on deep reinforcement learning", Wireless Communications and Mobile Computing, 2022.

[52] de Souza, C.A., Westphall, C.B., Machado, R.B., Sobral, J.B.M. and dos Santos Vieira, G., "Hybrid approach to intrusion detection in fog-based IoT environments", Computer Networks, vol. 180, p. 107417.

[53] Yang, Y., Zheng, K., Wu, C. and Yang, Y., "Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network", Sensors, vol. 19, no. 11, p. 2528, 2019.

[54] Sangeetha, S.K., Mani, P., Maheshwari, V., Jayagopal, P., Sandeep Kumar, M. and Allayear, S.M., "Design and Analysis of Multilayered Neural Network-Based Intrusion Detection System in the Internet of Things Network", Computational Intelligence & Neuroscience, 2022.

[55] Albulayhi, K., Smadi, A.A., Sheldon, F.T. and Abercrombie, R.K., "IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses", Sensors, vol. 21, no. 19, p. 6432, 2021.
[56] Shareena, J., Ramdas, A. and AP, H., "Intrusion detection system for iot botnet attacks using deep learning", SN Computer Science, vol. 2, no. 3, pp. 1–8, 2021.

Biographies

Selvam Ravindran completed Bachelor in Computer Science and Engineering from Muthayammal Engineering College, Rasipuram, Anna University, Chennai. Master in Computer Science and Engineering from Kumaraguru College of Technology, Anna University, Coimbatore. I am pursuing a Doctor of Philosophy at SRM University Kattankulathur Campus, Chennai. I have 11 years of Experience as an Assistant professor in the Computer Science and Engineering Department for various Engineering Colleges, I published 1 International Journal and 5 more National conferences.

Velliangiri Sarveshwaran obtained his bachelor's degree in computer science and engineering from Anna University, Chennai. Master in Computer

Science and Engineering from Karpagam University, Coimbatore, and Doctor of Philosophy in Information and Communication Engineering from Anna University, Chennai. Currently, he is working as an assistant professor at the SRM Institute of Science and Technology, Kattankulathur Campus, Chennai. He was a member of the Institute of Electrical and Electronics Engineers (IEEE) and the International Association of Engineers (IAENG). He has been serving as reviewer of IEEE Transactions, Elsevier, Springer, Inderscience, and other reputed Scopus-indexed journals. He is specialized in network security and optimization techniques. He published in more than 60 international journals and presented at more than 10 international conferences. He also serves as a technical program committee chair and conference chair at many international conferences. He served as book series editor of "Artificial Intelligence for Sustainability" in CRC Press. He also serves as an area editor for the EAI Endorsed Journal of Energy Web and an academic editor in the Journal of Wireless Communication and Mobile Computing.