Journal of Information Systems and Telecommunication
Vol.12, No.3, July-September 2024, 197-207
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

A Survey of Intrusion Detection Systems Based On Deep Learning for IoT Data

Mehrnaz Moudi[1,*], Arefeh Soleimani[1], Amir Hossein Hojjatinia[1]

[1]. Department of Computer Engineering, University of Torbat Heydarieh

Received: 25 Oct 2023/ Revised: 04 Jul 2024/ Accepted: 11 Aug 2022

Abstract

Today, the scope of using the Internet of Things is growing by taking science and technology as the first place in human life, and as these networks get bigger, more data are exchanged. It performs high-speed data exchanges on the Internet and in a pre-defined network. The more the Internet of Things penetrates into people's lives, the more important data it transmits. This causes attackers to draw attention to these data, and Internet of Things network devices that have limited resources are exposed to attacks. With the complexity of hardware and software for the ease of human's use, naturally more intelligent attacks will happen, which is the reason of presenting many methods in this field. For this reason, in this article, we are going to discuss the most important methods used in intrusion detection systems based on deep learning and machine that can identify these interruptions. In this article, we have compared 46 articles from 2020 to 2024 based on the type of dataset used, the type of classification (binary or multi-class) and the accuracy rates obtained from each method, and we have been able to see a comprehensive overview for researchers who intend to work in IoT data security. According to the obtained results, if the proposed method is implemented in binary form, it can achieve better accuracy than multi-class.

Keywords: Internet of Things; Artificial Intelligence; Machine learning; Deep learning; Intrusion Detection Systems.

1-Introduction

We are in the 21st century, where science and technology take the first place in human life. From the past to today, science has made significant progress in various fields in order to improve human comfort. The Internet of Things (IoT) technology is one such advancement in science. Where humans no longer have control over objects and we have a relationship between objects, and the relationship between humans and objects has no meaning. This is one of the signs of increasing the use of artificial intelligence in our earthly world. Today, artificial intelligence and machine learning have penetrated human life so much that the theory can be put forward that increasing the power of artificial intelligence can in some way bring about the well-being of humans and bring about the day when this same artificial intelligence against humans. IoT is not an exception to this rule and has been able to use deep learning algorithms and create a series of artificial neural networks such as CNN[1], RNN, NN[2], LSTM[3], MLP, which are similar to human brain nerves and have a series of weights.

IoT performs high-speed and real-time data exchanges on the Internet and in a pre-defined network [1]. In this network, a set of smart devices that are not limited to a geographical area are exchanging information [2]. Due to the many advantages of IoT, it is used in various government organizations, people's personal lives, health and treatment, industry and military organizations, and transportation and airways and seaways, and depending on the type of data exchanged and their importance as well as to maintain their security, various security protocols are expected for this type of networks [3, 4]. Due to the volume of important generated data that is exchanged based on IoT technology [5], the field of attack and information theft is also provided for hackers and makes the network vulnerable to electronic attacks and security challenges [3]. In the past, traditional methods such as the use of antiviruses and firewalls were used to deal with the security of network objects. However, for example, a smart watch that is connected to the Internet and connected with other devices does not have such a suitable and powerful hardware and processor that can install heavy security programs on it. Due to the hardware and processor limitations of this category of devices, as well as the ability

[1] Convolutional neural networks
[2] Neural Network
[3] Long short-term memory

✉ **Mehrnaz Moudi**
mehrnazmoudi@gmail.com/mmoudi@torbath.ac.ir

to respond quickly, which is one of the most important features of IoT [1], IDS[4] has been provided to monitor the network, the incoming and outgoing traffic from the network. In addition, if abnormal behaviors and anomalies are detected, quickly identify them and find a solution for intrusions. Usually, a group of security experts controls the network of IDS, and the detected flows are reported to the security expert that he provides a series of suggestions to deal with the detected intrusion based on decision-making systems.

Consequently, in order to design practical IDS, we need to know artificial networks based on deep learning so that we can use data mining to obtain the order governing reliable datasets that contain normal conditions and under attack, and the patterns. These datasets are embedded in the data mining science and entered into the desired neural network so that we can identify malicious or normal traffic and make the system resistant to future intrusions. In addition, sometimes the detection of these intrusions and countermeasures require quick action, for example, fire alarm systems, which are extremely important, need to be equipped with more advanced IDS [6]. Generally, when a new method is invented or optimized in this field, they are tested with previously created datasets such as N-BaIoT, IoTID20, NSL-KDD, UNSW-NB15, CICIDS2018 [7-9] and based on a series of parameters such as Accuracy, F-score, Recall, they evaluate the proposed method and compare the results obtained with previous methods.

The reason that many methods have been presented in this field is that with the passage of time and the complexity of hardware and software for the ease of use for humans, naturally more intelligent attacks will happen to these devices. Fundamentally, the ease of using the tool follows complex activities in the background and provides more scope for penetration. One of the best methods that is derived from mathematical calculation principles and has moved towards becoming intelligent is the methods that are based on deep learning [5]. Because in this method, by using multiple hidden layers, we can obtain useful features of network traffic and better detect intrusions. However, due to the amount of unstructured data produced by IoT devices [5], many researches have been conducted to extract the important and key features of the data with the help of deep learning techniques. IDS are used when network intrusion has occurred and we intend to find them, but security protocols such as firewalls and antiviruses prevent malware from entering the network. As a result, the common solutions based on deep learning are still facing many challenges and each of them has a series of disadvantages and limitations and for this reason, new and more optimal methods in this field based on learning are being developed day by day. Deep learning is more reliable than other methods because it can easily extract the important information of the dataset and hence provides better accuracy.

In this article, we have reviewed 46 articles from reputable journals that have presented between 2020 and 2024 in the field of IDS based on deep learning algorithms in IoT and categorized them based on various parameters. For the convenience of researchers, in this article, we examine the different dimensions of IDS and examine the new algorithms that have been presented and compare them. Investigations of ours provide deep learning-based intrusion detection in IoT. To the best of our knowledge, this is the only survey paper that has so far conducted a comprehensive study on deep learning-based security solutions with analytics. As well as this article gives researchers a very important and unique overview compared to other previous reviews. Considering that the methods presented in this field are implemented both in binary and multi-class form, it was necessary for us to let compare the articles in the last 4 years that have studied in the field of intrusion detection from the point of view of being binary and multi-class and see which of these two methods can provide higher accuracy.

In the continuation of the introduction section, we will organize the sections of the article. In section 2, we present a hierarchical view of the subject, in which we have sub-sections that fully explain each area. In section 3, we have examined the solutions and challenges of deep learning and presented a comprehensive table that includes the comparison of methods. Section 4 is our discussion in which we discussed the evaluation parameters of the methods. In conclusion, Section 5, which is the last section, is our conclusion based on the evaluations.

2-Hierarchical View of Intrusion Detection Systems

In this section, we intend to take a hierarchical view of IDS and explain in detail all the components that play a role in creating IDS. For this purpose, first in section A, we have presented the importance of learning data mining science and in section B; we have discussed the applications of artificial intelligence. Then, in section C, it is time to examine machine learning, which we have described its various uses and categories, and next in section D, it is time to get to the core of our article, which is deep learning. Finally, in section E,

[4] Intrusion Detection System

we have discussed the importance of using IDS using deep learning algorithms.

2-1- Details of Data Mining and its salient features

In the past, the use of electronic and digital tools was not as widespread as it is today. Thus, research on the data generated by this tool was not much discussed. The digital age can be called the 1990s, where digital devices produced a huge amount of data [10]. However, today, we see traces of digital in every environment and place we look. Naturally, this widespread use of these devices leads to the production of a series of data in massive volumes. The mass data that is output from these devices contains useful information about the system. This obtained information is often not understandable for humans. In the past, due to the minimal use of digital tools, the output data was also small, and humans used to analyze the data with a superficial look and manual separation. Gradually, with the significant increase in the use of digital tools, data was produced in huge volumes. Therefore, when the time came for these data to be analyzed by humans for better performance, he would get confused and unable to calculate. For this reason, the science of data mining was proposed. Data mining is a process to find anomalies, associations, patterns, changes, structures, correlations and non-correlations in datasets with massive data [10]. Among the most important datasets with large data are N-BaIoT, IoTID20, NSL-KDD, UNSW-NB15, CICIDS2017, CICIDS2018, KDDCup99, MQTT IOT IDS2020, KDD, Bot-IOT, KDD99, MQTT.

Data mining was able to provide a series of methods and methods to human, enabling him to find the law and order governing the data, and this human being analyzed these data through a series of evaluations in order to be able to find the pattern governing these data and classify them [10, 11]. If we can analyze these data generated from digital devices well and find the rules on them, we can optimize the system for the next time in order to reach the goals with more optimal power. The science of data mining was also created in order to be able to extract these ruling patterns from the data by providing a series of methods and methods such as artificial intelligence, deep learning, and so on. For example, a company that operates in the field of investment can perform a series of analyzes to predict the price trend of a stock by analyzing the data obtained from the chart of each stock [10]. On the other hand, in another example, we can refer to the data generated by the IoT. IoT devices produce massive amounts of data in the form of datasets, and it is quite difficult to check each one of them by humans. With the data mining of these datasets, it is possible to find the order governing them and inform IDS. The main data mining techniques include the following:

1. Data cleaning
2. Classification
3. Clustering
4. Regression
5. Prediction
6. Decision trees
7. Neural networks
8. Long-term memory processing

2-2- Details of Artificial Intelligence and its salient features

Artificial intelligence is one of the most interesting research fields in computer science and many researchers have done many activities in this field. It is enough to prove the exactingness of the research field of artificial intelligence that according to the report of the online portal, the statistics of the global market of artificial intelligence software will increase from 9.51 billion dollars in 2018 to 118.6 billion dollars by 2025 [12]. If we want to apply this concept of artificial intelligence, it is better to first separate this word into artificial and intelligence. Intelligence includes the ability to think and learn based on experience, and everything that is made by human thought and intelligence is called artificial [16]. Now, the combination of these two words helps us to understand the main concept of artificial intelligence more clearly. Artificial intelligence is a set of algorithms that are given by humans to a series of robots or programs so that they can learn with the help of these primary algorithms by means of pre-produced data sets and understand the pattern governing the data by repeating and reviewing these algorithms. Eventually they will be able to optimize their performance and make decisions without human intervention according to the educational experience that they have gained in the previous stage and it is no longer necessary for humans to dictate commands to the program or robot one by one.

The techniques used in artificial intelligence are [13]:

- machine learning
- Deep learning
- Decision tree techniques
- Support Vector Machine (SVM)
- Fuzzy Logic
- Genetic algorithm
- Bayesian network
- Clustering techniques

Therefore, in the discussion of identifying intrusions, we can use the techniques used in artificial intelligence, such as machine learning, which means the ability to teach a machine by learning algorithms, and deep learning, which means simulating the neural networks of the human brain, and has many advantages over other techniques are being used for IoT data.

2-3- Details of Machine Learning and its Salient Features

In fact, machine learning is a subset of artificial intelligence. Since it was said in the previous sections, with the help of machine learning algorithms, the system can be enabled to receive and read the data by itself without direct programming, and at the end, the output along with a series of suggestions for better decision-making offer to the user. In general, the basis of machine learning techniques is that they intend to improve performance over time based on previous results [13] and automate processes [14]. Recently, machine learning, like artificial intelligence, has been interested in university research and has been able to solve problems in real-world businesses largely [15]. The main machine learning techniques include the following [13]:

- Neural Network (NN)
- Bayesian network
- Markov model
- Vector machine support

In addition, various types of machine learning [14]:
- Supervised learning
- Unsupervised learning
- Reinforcement learning

2-4- Details Deep Learning and its Salient Features

Deep learning is a more complex part of machine learning. In most definitions, these two concepts are considered the same, but in reality, they are not, and each of them has a series of unique characteristics. As mentioned, deep learning is a set of neural nodes, each of which can be a type of input to a neural network. Generally, deep learning consists of neural networks that have three layers. The first layer is the neural nodes or our inputs to the network and after that, we have hidden layers and finally the output layer, which are considered as inputs for the next layers. The hidden layers extract features of nodes in different ways. In other words, the central core of neural networks are the hidden layers that are placed between the input and output layers and have activation functions. Because in this layer we can extract the features from the inputs in different ways. For example, the hidden layer in convolutional neural networks has a series of multi-dimensional inputs that we can obtain in the hidden layer with the help of a large number of filters important features of the input data. In the traditional methods of machine learning, we had to generate complex hypotheses ourselves, but with neural networks, this happens by automatically repeating the network, and the network learns patterns. With more repetitions, the network becomes more powerful and makes it a powerful tool for effective learning of nonlinear relationships [16]. Certainly, the important point is that we must be careful that the network not to be overfitting. It means that our network repeats the algorithm so much and learns so many models that it can only give the best answer with exactly the same initial dataset and cannot work with other datasets and give us an optimal and appropriate answer since it has learned too much.

Scientists are increasingly developing deep learning algorithms, and each time they have been able to reach new and more optimal records with an accuracy rate close to 100%. For example, testing the classification of 1000 different images, the image classification error rate was reduced to 3.5%, which is higher than human accuracy. Deep learning technology is used in the fields such as speech recognition, image processing, medicine, and IDS in the IoT, etc. [16].

Now that we are familiar with deep learning and neural networks, we intend to use them in IDS. For this purpose, we can use different neural networks such as DCNN[5], DLHNN[6], CNN, Bi-LSTM[7], and LSTM. The basis of all of them is to identify and announce abnormal and malicious behavior by examining the traffic passing through the IoT network. This behavior detection requires us to analyze network traffic and identify malicious behavior patterns. With the help of artificial neural networks, we can extract the characteristics of these traffics and prepare the network against future intrusions. In fact, we teach the IoT network to resist harmful behaviors and prevent interruption in our network. In Fig. 1, in order to summarize our explanations, the three layers of artificial intelligence, machine learning and deep learning along with examples of each have been demonstrated:

AI **Artificial intelligence** A program that can sense, reason, act and adapt	❖ Reactive machine ❖ Limited memory ❖ Theory of mind ❖ Self-awareness
ML **Machine Learning** Algorithms whose performance improve as they are exposed to more data over time	❖ Supervised Learning ❖ Unsupervised Learning ❖ Reinforcement Learning
DL **Deep Learning** Subset of machine learning in witch multi-layered neural networks learn from vast amounts of data	❖ Convolutional Neural Networks ❖ Long Short-Term Memory ❖ Deep Random Neural Network

Fig. 1: Global View of AI, ML, DL

[5] Deep convolutional neural networks
[6] Deep learning-based hybrid neural network
[7] Bidirectional long short-term memory

2-5- Details IDSs and their Salient Features

In this section, we will examine IDS in the IoT. Considering the limited resources of network devices, security is one of the most important challenges. Small devices that rely on weak processors and little storage resources are not capable of supporting many security protocols. On the other hand, these devices may have important data exchanges in the organization, and their low security exposes them to undetermined intrusions. In the past, when IoT was not studied much and only computers were networked together, their ultimate security was to use a firewall and a series of antiviruses [17] such as Kaspersky Internet Security or ESET NOD32 Antivirus. However, with the expansion of the Internet and the advancement of science, devices such as watches, cameras, televisions, etc. have been able to connect to the Internet and exchange data. As a result, it was practically impossible to use antivirus on them. Even the computers that connected to the Internet and carried these two protocols were no longer able to respond to attacks.

It was here that the creation of a system that can monitor the network and check all network details such as bandwidth, throughput, tolerance and network traffic to identify malicious attacks and intrusions was felt. These systems became known as IDS, which were able to detect intrusions to a significant extent using deep learning techniques. IDS can monitor activities between devices connected to a network and send an alert to a network security expert or network administrator whenever a fault is detected [18]. However, due to the dynamic nature of network science and the expansion of their use, over time, the techniques are worn out and unresponsive. For this reason, new articles are presented every year in the field of intrusion detection in the IoT using deep learning techniques, which somehow have been able to provide new and more optimal techniques to deal with intrusions due to the development of network software. It is predicted that the financial losses caused by attacks on the IoT network will be about 20 billion dollars by 2021. In Fig. 2, you can see the taxonomy of IDS for IoT [19].

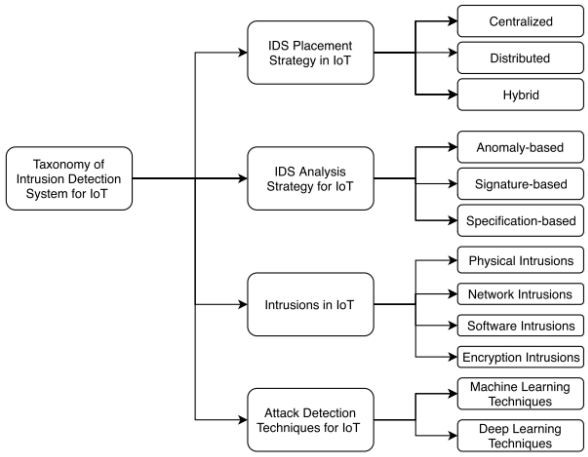

Fig. 2: Taxonomy of IDS for IoT

3- Solutions and Challenges in IoT

In this section, we intend to pay more attention to deep learning. Due to the results of studies, deep learning methods have helped to identify intrusions in the discussion of IoT systems. In the previous sections, we went through a hierarchical view to better understand the importance of deep learning, and now we want to discuss the importance and applications of the solutions that deep learning has made in order to identify intrusions in section A. Section B will address the challenges and limitations that may be in front of us when using deep learning techniques and explain them. Finally, in section C, we have put a complete table of comparison of deep learning and machine learning methods in the past years until now.

3-1-Deep learning as an Ideal Security Solution in IoT

Due to the growing use of the IoT, devices that use this technology are added day by day. Each device has specific software and hardware that follows predetermined standards. This expansion and important data swaps that are exchanged between devices prompt attackers to penetrate the network with various attacks and carry out information theft operations. For example, these important data can be bank account numbers, home addresses, people's ages, users and passwords of logged-in sites, the amount of salary received, etc. Since these devices have no unified and uniform security, they are constantly under attack so that organizations such as IEEE[8] and ETSI[9] are trying to provide an ideal method to identify these intrusions [20]. IoT devices usually come with software solutions that are not sufficient to protect the devices or the network itself [21, 22]. Since the

[8] Institute of Electrical and Electronics Engineers

[9] European Telecommunications Standards Institute

IoT is used in various areas and fields, the security at the software level is weak [23].

Unfortunately, most of the methods proposed by researchers are mostly for small-scale networks and have not been very effective for large-scale networks [20]. Scalability in the IoT and IDS means that the network does not face a decrease in its efficiency with the increase in the number of devices and the increase in the volume of users. Most importantly, it can perform its main task, which is to identify intrusions during attacks. Every network has a series of layers. IoT network is similar. Depending on the type of each layer, we have various malicious attacks. The most important attacks on the IoT are active and passive attacks. Active attacks refer to attacks that occur online during network activity, but passive attacks steal network information without disrupting network activity [20].

There is no 100% solution on how to guarantee security or detect intrusions in the IoT [23], however we can use deep learning methods to solve these problems as much as possible compared to other methods. Therefore, deep learning is especially suitable for data sets in large volumes [24]. Obviously, because billions of devices are connected in the network and exchange data, as a result, datasets are produced in large volumes [20]. Deep learning methods are according to these big datasets. The unique structure of deep learning and machine learning algorithms help IDS to identify malicious operations to the system. For example, if we want to act in a supervised way, it is necessary to train our neural network algorithm, which consists of a number of hidden layers whose purpose is to extract features from the dataset [20], and finally predict after learning. Sort and display the outputs for us in normal or malicious format [25]. Certainly, good progress has been made in the supervised method that the algorithm no longer needs to be trained with primary data and can identify and predict intrusions without learning [26].

As mentioned earlier, with the help of deep learning algorithms in the IoT network, connection between objects or devices is possible without human intervention, and we have connection between objects and objects, and there is no longer a human who can send these connections to the device one by one [27]. For example, imagine a house where all electronic devices are intelligently connected to each other on the Internet and meet each other's needs [28].

3-2-Limitations of using Deep Learning

Limiting the use of resources and not having relatively strong processors and suitable computing resources in most of the IoT devices have caused us to have problems that our most important problems are the memory efficiency and IDS response time. Since new methods and more optimal techniques are presented in deep learning algorithms day by day, there is a need for these optimized algorithms to match the characteristics of the IoT and be able to adapt to the network. But because these methods are new and have not yet been widely used, they cannot be used much for IDS [20].

The next point is to assume that the algorithm is suitable for the network. Since we tried to make the model learn and make decisions on its own, and humans no longer have special access to learn the model, sometimes the volume of data becomes larger and larger over time, and this causes the efficiency of the algorithm to decrease [20]. For example, if the algorithm is trained for a million devices with 10 features, after sometime it may be added to the number of network devices. If another 2 million devices are added, the efficiency of the algorithm will not be the same as before and the accuracy of diagnosis will decrease. In addition to the point that all these events happen online and the increase in the number of devices occurs during network activity. Now imagine a deep learning algorithm that aims to detect intrusions online in an IDS and the size of its network is increasing over time. If the algorithm is not scalable, it will lose its efficiency. On the one hand, the attacker has infiltrated the network, while the network does not have the capacity to accept the new device to process its data, and the result is a devastating event for the network.

One of the important challenges with deep learning is that the wrong and inefficient inputs used to design and learn the model for deep techniques or lack of data for training or non-essential features in hidden layers of IDS have been easily exposed our network to threats and major damages such as hacking and information theft [23].

3-3- Comparison Table

In Table 1, we have compared 46 articles from 2020 to 2024. Each of these articles has its own datasets, methods, accuracies and classifications. The first column contains the authors' name of the references, which have been applied to identify intrusions in the IoT. In the second column, the year of publication for each article is placed. The selection period starts from 2020 to 2024. Generally, in most of the review articles, short periods of 4 years are considered in the discussion of intrusion detection. The reason is that the speed of updating deep and machine learning algorithms is increasing, and the previous methods will soon become outdated. The next column is the number of citations for the mentioned references after their publication. Then, by considering that more devices are added to the IoT network and each hardware device uses more complex software, it is necessary to provide new methods. In the next column, you can see the datasets used by the methods. Datasets are files in .txt or .csv format that contain large matrices. These

matrices consist of a series of rows and columns. Rows are records or network devices, and columns are attributes of network devices. Using the science of data mining, we find the rule governing these datasets. For training and testing a network, the ready-made datasets have been created manually or in reality. In the fifth column, you can see the method used by researchers to identify and predict intrusions in each studied article. In the next column, you can see the accuracy rate obtained from the algorithm. In the last column, we have obtained the type of attack classification based on binary or multi-class. Some articles have used several datasets with different classifications to show their work better, which have been able to obtain acceptable accuracy rates. In this table, different datasets with different methods have been able to obtain high and acceptable accuracy rates. In the next section, we will discuss more details of the following table.

Table 1: Comparison DL/ML Methods

Authors	*Year*	*Dataset*	*Method*	*Accuracy*	*Classification*
Lahsan et al. [7]	2022	NBaIoT	Lightweight autoencoder -KNN	99.00%	Binary
Ullah et al. [8]	2022	IoTID20	DCNN	99.91% & 98.38%	Binary & Multiclass
Kim et al. [29]	2024	IoT Intrusion Bot-IoT	Transfer learning	99.94%	Binary
Osa et al. [30]	2024	CICIDS 2017	DNN	99.68 %	N/A
Psychogyios et al. [31]	2024	UNSW-NB15	LSTM	N/A	Binary
Çavuşoğlu et al. [32]	2024	NSL-KDD	Transfer learning	99.85% 99.83%	Binary & Multiclass
Yang et al. [33]	2024	CICIDS2017	LSTM, CNN & Auto encoder	99.81%	Multiclass
Hnamte et al. [34]	2023	CICIDS2017 CSE-CICDIS2018	Autoencoder and LSTM	99.99% 99.10%	Multiclass
Alenezi et al. [35]	2023	X-IIoTID	K-means	99.79% & 97.10%	Binary & Multiclass
Lilhore et al. [36]	2023	UNW-NB15	LSTM & CNN	94.25%	Multiclass
Figueiredo et al. [37]	2023	CICIDS2017	LSTM	99.00%	Binary
Chaganti et al. [38]	2023	SDN-IoT, SDN-NF-TJ	LSTM	97.70% & 97.10%	Binary & Multiclass
Gupta et al. [39]	2022	NSLKDD	DLHNN- HCSGA MinK-means	99.52%	Binary
Basatsi at al. [40]	2022	KDDCup99 CICIDS2017 UNSWNB15	DFE – CNN	N/A & 99.92% 98.98% & 99.31% 100% & 99.96%	Binary & Multiclass
Sagu et al. [41]	2022	UNSWNB15 & CloudStor	Bi-LSTM -GRU	84.83% & 84.73%	Binary
Idrissi et al. [42]	2022	MQTTIOT-IDS2020	DL-HIDS	99.74	N/A
Sobhanzadeh et al. [43]	2022	NBaIoT	WCC & SVM	100% & 96.70%	Binary & Multiclass
Malik et al. [44]	2022	MedBIoT & Chris Dataset & HCRL	KNN	98.00% & 99.00% & 98.00%	N/A
Diddi et al. [45]	2022	CICDDoS2019	CNN	99.75% & 99.99%	Binary & Multiclass
Idrissi et al. [46]	2021	BotIoT	CNN	99.94%	Multiclass
Alkahtani et al. [47]	2021	IoTID20	CNN-LSTM & mix both	CNN = 96.60% LSTM = 99.82% CNN-LSTM = 98.80%	Multiclass

Liu et al. [48]	2021	NSLKDD	DSSTE+LSTM	81.78%	Multiclass
Ashraf at al. [49]	2021	UNSWNB15	LSTM Autoencoder	98.00%	Binary
Borisenko et al. [50]	2021	CICIDS2018	LSTM	94.00%	Multiclass
Hai et al. [51]	2021	CICIDS2017	LSTM	99.55%	Binary
Ts et al. [52]	2021	KDD	Bi LSTM	99.70%	Binary
Mighan et al. [53]	2021	UNB ISCX 2012	SVM and LSTM	99.49%	Binary
Jia et al. [54]	2021	KDD & NSLKDD	IE-DBN	98.12% & 98.79%	Multiclass
Biswas et al. [55]	2021	BotIOT & NSL	LSTM-GRU	99.76% & 99.14%	Binary
Laghrissi et al. [56]	2021	KDD99	LSTM	98.88%	Binary
ElSayed et al. [57]	2021	InSDN	CNN	97.50%	Binary & Multiclass
Joshi at al. [58]	2021	CTU13	ANN	99.94%	Binary
Sethi et al. [59]	2021	NSLKDD	Reinforcement/ML	96.50%	Multiclass
Mendonça et al. [60]	2021	DS2OS & CICIDS2017	SET	99.00% & 99.00%	Multiclass
Hussain et al. [61]	2021	MQTTset	DT	99.47%	Binary
Vaccari et al. [62]	2021	MQTTset	RF	99.68%	Binary
Imrana et al. [63]	2021	NSLKDD	BiLSTM	94.26% & 91.36%	Binary & Multiclass
Khan et al. [64]	2021	UNSWNB15	LSTM	98.88%	Binary
Parra et al. [65]	2020	NBaIoT	DCNN & LSTM	94.30% & 93.58	N/A
Latif et al. [66]	2020	UNSWNB15	DRaNN	99.41%	Multiclass
Roopak et al. [67]	2020	CISIDS2017	CNN & LSTM	99.03%	Binary
Smys et at al. [68]	2020	UNSWNB15	HCNN	98.60%	Multiclass
Kasongo et al. [69]	2020	UNSWNB15	WFEU-FFDNN	99.66% & 99.77%	Binary & Multiclass
Li et al. [70]	2020	NSLKDD	CNN	86.95% 81.33%	Binary & Multiclass
Khamis et al. [71]	2020	UNSWNB15	CNN	96.00%	Multiclass

4- Table Discussion

In this section, we will discuss Table I. This table gives us a comprehensive and complete view of the methods of detecting intrusions in the IoT by means of deep learning and machine learning techniques. The reason for choosing this 3-year period is that due to the strange speed of growth of deep learning and machine learning methods in the past years and the optimization and performance of each algorithm compared to the previous algorithm, there is no need to repeat the methods of previous articles. Let us discuss because, for example, the accuracy rate of an article using the CNN method in 2017 was 85%, but the same dataset with the same method in 2021 achieved an accuracy rate of 98%. For this reason, this table has collected the techniques of the day in the field of IoT. Researchers who are looking for ideas and need to quickly get a comprehensive view of the articles published in these three years in the field of IoT and IDS, Table 1 helps them well.

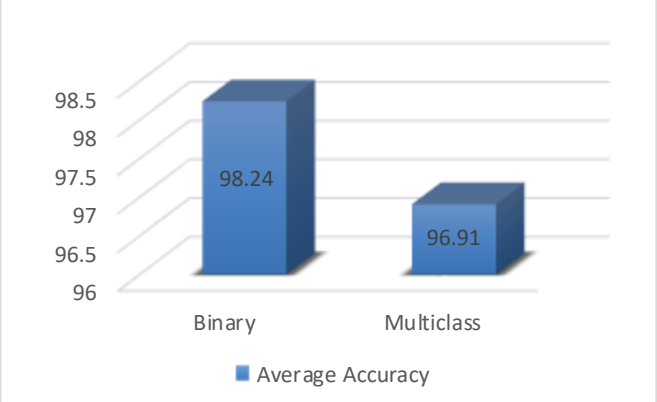

Fig. 3: Average of Accuracy in two classification

As it is known, most of the methods have used convolutional neural networks, which have been able to analyze the input

well and recognize the important features of the input using a series of convolutional layers. As it is evident from Fig. 3, the more evaluations of deep learning and machine algorithms have been done based on binary classifications in these three years, the average accuracy of them is much higher than multi-class classification. Therefore, the average accuracy of the binary and multi-class classification is 98.24% and 96.91%, respectively.

5- Conclusion

In this article, first, we tried to explain concepts such as data mining, which is the main basis of working with data. Moreover, to understand the functioning of an ITDA intrusion detection system, we expressed a hierarchical view of artificial intelligence, which itself consisted of machine learning and deep learning. Finally, we examined the types of IDS in the IoT network, then, we examined the challenges and solutions that deep learning has provided to IDS. This article gives researchers unique overview compared to other previous studies that which of the binary or multi-class form in the research methods can provide higher accuracy in the field of intrusion detection. Referring to Table 1, we found out what as time passes, the popularity of using deep learning methods increases. In provided table (Table 1), we have compiled the accuracy rates of the methods from 2020 to 2024 based on different classifications and we have concluded that binary classification methods have been able to obtain better accuracy rates.

Authors'Contribution

We would like to inform you that to the best of our knowledge, this work does not currently exist in print or otherwise and it will not be submitted until a decision has been made. The contribution of this paper presents a survey of intrusion detection systems based on deep learning for IoT data in the presence of complete various aspects. Mehrnaz Moudi conceived the idea, conducted the experiments, analyzed the results and revised the manuscript. Arefeh Soleimani and Amir Hossein HojjatiNia conducted the experiments and wrote the manuscript. All authors read and approved the final manuscript.

Acknowledgment

This work was financially supported by the University of Torbat Heydarieh under Grant No: 1401/12-154.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications", IEEE internet of things journal, Vol. 4, No. 5, 2017, pp. 1125-1142.

[2] U. Farooq, N. Tariq, M. Asim, T. Baker, and A. Al-Shamma'a, "Machine learning and the Internet of Things security: Solutions and open challenges", Journal of Parallel and Distributed Computing, Vol. 162, 2022, pp. 89-104.

[3] A. Adnan, A. Muhammed, A. A. Abd Ghani, A. Abdullah, and F. Hakim, "An intrusion detection system for the internet of things based on machine learning: Review and challenges", Symmetry, Vol. 13, No. 6, 2021, pp. 1011.

[4] K. Lakshmanna et al., "A review on deep learning techniques for IoT data", Electronics, Vol. 11, No. 10, pp. 1604, 2022.

[5] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review", Applied sciences, Vol. 11, No. 18, 2021, pp. 8383.

[6] T. Hossain, M. Ariful Islam, A. B. R. Khan, and M. Sadekur Rahman, "A Robust and Accurate IoT-Based Fire Alarm System for Residential Use", in International Conference of Computer Networks, Big Data and IoT (ICCBI), 2021, Singapore.

[7] B. Lahasan and H. Samma, "Optimized deep autoencoder model for internet of things intruder detection", IEEE Access, Vol. 10, 2022, pp. 8434-8448.

[8] S. Ullah et al., "A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering", Sensors, Vol. 22, No. 10, 2022, pp. 3607.

[9] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, and T. Baker, "A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT", Journal of Parallel and Distributed Computing, Vol. 134, 2019, pp. 198-206.

[10] P. Prasdika and B. Sugiantoro, "A review paper on big data and data mining concepts and techniques", International Journal on Informatics for Development, Vol. 7, No. 1, 2018, pp. 36-38.

[11] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends", Computer networks, Vol. 51, No. 12, 2007, pp. 3448-3470.

[12] D. Minh, H. X. Wang, Y. F. Li, and T. N. Nguyen, "Explainable artificial intelligence: a comprehensive review", Artificial Intelligence Review, Vol. 55, 2022, pp. 3503-3568.

[13] G. Kumar, K. Kumar, and M. Sachdeva, "The use of artificial intelligence based techniques for intrusion detection: a review", Artificial Intelligence Review, Vol. 34, 2010, pp. 369-387.

[14] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning", Electronic Markets, Vol. 31, No. 3, 2021, pp. 685-695.

[15] A. Paleyes, R.-G. Urma, and N. D. Lawrence, "Challenges in deploying machine learning: a survey of case studies", ACM Computing Surveys, Vol. 55, No. 6, 2022, pp. 1-29.

[16] S. Dong, P. Wang, and K. Abbas, "A survey on deep learning and its applications", Computer Science Review, Vol. 40, 2021, pp. 100379.

[17] S. B. Saad, A. Ksentini, and B. Brik, "A Trust architecture for the SLA management in 5G networks", in IEEE-International Conference on Communications (ICC), 2021, Canada, pp. 1-6.

[18] A. Thakkar and R. Lohiya, "Role of swarm and evolutionary algorithms for intrusion detection system: A survey", Swarm and evolutionary computation, Vol. 53, 2020, pp. 100631.

[19] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges", Archives of Computational Methods in Engineering, Vol. 28, 2021, pp. 3211-3243.

[20] Y. Yue, S. Li, P. Legg, and F. Li, "Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey", Security and communication Networks, Vol. 2021, 2021, pp. 1-13.

[21] J. Porras, J. Khakurel, A. Knutas, and J. Pänkäläinen, "Security challenges and solutions in the internet of things", Nordic and Baltic Journal of Information and Communications Technologies, Vol. 2018, No. 1, 2018, pp. 177-206.

[22] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices", in 21st Asia and South Pacific design automation conference (ASP-DAC), 2016, China, pp. 519-524.

[23] S. Bharati and P. Podder, "Machine and deep learning for iot security and privacy: applications, challenges, and future directions", Security and Communication Networks, Vol. 2022, 2022, pp. 1-41.

[24] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey", IEEE Communications Surveys & Tutorials, Vol. 20, No. 4, 2018, pp. 2923-2960.

[25] J. Franklin, "The elements of statistical learning: data mining, inference and prediction", The Mathematical Intelligencer, Vol. 27, No. 2, 2005, pp. 83-85.

[26] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks", science, Vol. 313, No. 5786, 2006, pp. 504-507.

[27] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems", IEEE Communications Surveys & Tutorials, Vol. 19, No. 4, 2017, pp. 2432-2455.

[28] H. Li, K. Ota, and M. Dong, "Learning IoT in edge: Deep learning for the Internet of Things with edge computing", IEEE network, Vol. 32, No. 1, 2018, pp. 96-101.

[29] H. Kim, S. Park, H. Hong, J. Park, and S. Kim, "A Transferable Deep Learning Framework for Improving the Accuracy of Internet of Things Intrusion Detection", Future Internet, Vol. 16, No. 3, 2024, pp. 80.

[30] E. Osa, P. E. Orukpe, and U. Iruansi, "Design and implementation of a deep neural network approach for intrusion detection systems", e-Prime-Advances in Electrical Engineering, Electronics and Energy, Vol. 7, 2024, pp. 100434.

[31] K. Psychogyios, A. Papadakis, S. Bourou, N. Nikolaou, A. Maniatis, and T. Zahariadis, "Deep Learning for Intrusion Detection Systems (IDSs) in Time Series Data", Future Internet, Vol. 16, No. 3, 2024, pp. 73.

[32] Ü. Çavuşoğlu, D. Akgun, and S. Hizal, "A novel cyber security model using deep transfer learning", Arabian Journal for Science and Engineering, Vol. 49, No. 3, 2024, pp. 3623-3632.

[33] Y. Yang, J. Cheng, Z. Liu, H. Li, and G. Xu, "A multi-classification detection model for imbalanced data in NIDS based on reconstruction and feature matching", Journal of Cloud Computing, Vol. 13, No. 1, 2024, pp. 31.

[34] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A novel two-stage deep learning model for network intrusion detection: LSTM-AE", IEEE Access, Vol. 11, 2023, pp. 37131-37148.

[35] N. Alenezi and A. Aljuhani, "Intelligent Intrusion Detection for Industrial Internet of Things Using Clustering Techniques", Computer Systems Science & Engineering, Vol. 46, No. 3, 2023, pp. 2899-2915.

[36] U. K. Lilhore et al., "HIDM: Hybrid intrusion detection model for industry 4.0 Networks using an optimized CNN-LSTM with transfer learning", Sensors, Vol. 23, No. 18, 2023, pp. 7856.

[37] J. Figueiredo, C. Serrão, and A. M. de Almeida, "Deep learning model transposition for network intrusion detection systems", Electronics, Vol. 12, No. 2, 2023, pp. 293.

[38] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks", Information, Vol. 14, No. 1, 2023, pp. 41.

[39] S. K. Gupta, M. Tripathi, and J. Grover, "Hybrid optimization and deep learning based intrusion detection system", Computers and Electrical Engineering, Vol. 100, 2022, pp. 107876.

[40] A. Basati and M. M. Faghih, "DFE: Efficient IoT network intrusion detection using deep feature extraction", Neural Computing and Applications, Vol. 34, No. 18, 2022, pp. 15175-15195.

[41] A. Sagu, N. S. Gill, P. Gulia, J. M. Chatterjee, and I. Priyadarshini, "A hybrid deep learning model with self-improved optimization algorithm for detection of security attacks in IoT environment", Future Internet, Vol. 14, No. 10, 2022, pp. 301.

[42] I. Idrissi, M. Mostafa Azizi, and O. Moussaoui, "A lightweight optimized deep learning-based host-intrusion detection system deployed on the edge for IoT", International Journal of Computing and Digital System, Vol. 11, No. 1, 2021, pp. 209-216.

[43] Y. Masoudi-Sobhanzadeh and S. Emami-Moghaddam, "A real-time IoT-based botnet detection method using a novel two-step feature selection technique and the support vector machine classifier", Computer Networks, Vol. 217, 2022, pp. 109365.

[44] K. Malik, F. Rehman, T. Maqsood, S. Mustafa, O. Khalid, and A. Akhunzada, "Lightweight internet of things botnet detection using one-class classification", Sensors, Vol. 22, No. 10, 2022, pp. 3646.

[45] S. Diddi, S. Lohidasan, S. Arulmozhi, and K. R. Mahadik, "Standardization and Ameliorative effect of Kalyanaka ghrita in β-amyloid induced memory impairment in wistar rats", Journal of Ethnopharmacology, Vol. 300, 2023, pp. 115671.

[46] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui, and H. El Fadili, "Toward a deep learning-based intrusion detection system for IoT against botnet attacks", IAES International Journal of Artificial Intelligence, Vol. 10, No. 1, 2021, pp. 110.

[47] H. Alkahtani and T. H. Aldhyani, "Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms", Complexity, Vol. 2021, 2021, pp. 1-18.

[48] L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion detection of imbalanced network traffic based on machine learning and deep learning", IEEE Access, Vol. 9, 2020, pp. 7550-7563.

[49] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, "Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems", IEEE Transactions on Intelligent Transportation Systems, Vol. 22, No. 7, 2020, pp. 4507-4518.

[50] B. Borisenko, S. Erokhin, A. Fadeev, and I. Martishin, "Intrusion detection using multilayer perceptron and neural networks with long short-term memory", in Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), 2021, Russia, pp. 1-6.

[51] T. H. Hai and L. H. Nam, "A practical comparison of deep learning methods for network intrusion detection", in International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2021, Malaysia, pp. 1-6.

[52] T. Pooja and P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security", Global Transitions Proceedings, Vol. 2, No. 2, 2021, pp. 448-454.

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

[54] H. Jia, J. Liu, M. Zhang, X. He, and W. Sun, "Network intrusion detection based on IE-DBN model", Computer Communications, Vol. 178, 2021, pp. 131-140.

[55] R. Biswas and S. Roy, "Botnet traffic identification using neural networks", Multimedia Tools and Applications, Vol. 80, 2021, pp. 24147-24171.

[56] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)", Journal of Big Data, Vol. 8, No. 1, 2021, pp. 65.

[57] M. S. ElSayed, N.-A. Le-Khac, M. A. Albahar, and A. Jurcut, "A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique", Journal of Network and Computer Applications, Vol. 191, 2021, pp. 103160.

[58] C. Joshi, R. K. Ranjan, and V. Bharti, "A Fuzzy Logic based feature engineering approach for Botnet detection using ANN", Journal of King Saud University-Computer and Information Sciences, Vol. 34, No. 9, 2022, pp. 6872-6882.

[59] K. Sethi, Y. V. Madhav, R. Kumar, and P. Bera, "Attention based multi-agent intrusion detection systems using reinforcement learning", Journal of Information Security and Applications, Vol. 61, 2021, pp. 102923.

[60] R. V. Mendonca, J. C. Silva, R. L. Rosa, M. Saadi, D. Z. Rodriguez, and A. Farouk, "A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms", Expert Systems, Vol. 39, No. 5, 2022, pp. e12917.

[61] F. Hussain et al., "A framework for malicious traffic detection in IoT healthcare environment", Sensors, Vol. 21, No. 9, 2021, pp. 3025.

[62] I. Vaccari, S. Narteni, M. Aiello, M. Mongelli, and E. Cambiaso, "Exploiting Internet of Things protocols for malicious data exfiltration activities", IEEE Access, Vol. 9, 2021, pp. 104261-104280.

[63] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection", Expert Systems with Applications, Vol. 185, 2021, pp. 115524.

[64] I. A. Khan, N. Moustafa, D. Pi, W. Haider, B. Li, and A. Jolfaei, "An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles", IEEE Transactions on Intelligent Transportation Systems, Vol. 23, No. 12, 2021, pp. 25469-25478.

[65] G. D. L. T. Parra, P. Rad, K.-K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning", Journal of Network and Computer Applications, Vol. 163, 2020, pp. 102662.

[66] S. Latif, Z. Idrees, Z. Zou, and J. Ahmad, "DRaNN: A deep random neural network model for intrusion detection in industrial IoT", in International Conference On UK-China Emerging Technologies (UCET), 2020, Glasgow, UK, pp. 1-4.

[67] M. Roopak, G. Y. Tian, and J. Chambers, "An intrusion detection system against ddos attacks in iot networks", in 10th annual computing and communication workshop and conference (CCWC), 2020, USA, pp. 0562-0567.

[68] S. Smys, A. Basar, and H. Wang, "Hybrid intrusion detection system for internet of things (IoT)", Journal of ISMAC, Vol. 2, No. 04, 2020, pp. 190-199.

[69] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset", Journal of Big Data, Vol. 7, 2020, pp. 1-20.

[70] Y. Li et al., "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion", Measurement, Vol. 154, 2020, pp. 107450.

[71] R. Abou Khamis and A. Matrawy, "Evaluation of adversarial training on different types of neural networks in deep learning-based idss", in International Symposium On Networks, Computers And Communications (ISNCC), 2020, Canada, IEEE, pp. 1-6.