Power System Technology
ISSN:1000-3673

Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

A Honeypot-Based Model for Detecting Iot Botnet Attacks Using Separable Convolutional Neural Network and Majority Voting Strategy

Mohsen Mohammadi Aliabadi[1], Maliheh Hashemipour[2*]

1. PhD student, Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran.

2. Assistant Professor, Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran (corresponding author).

Abstract

In recent years, there have been many botnet attacks on Internet of Things devices and the result has been heavy losses to companies and organizations. Each botnet is a group of hosts infected with the same malicious code and controlled by a remote attacker through one or more command and control servers. In this article, a new approach to detect botnet attacks is presented by combining honeypot technology and deep learning. A honeypot is a security tool whose value lies in being discovered and investigated, attacked and compromised. Honeypots can be used in forensics by gathering evidence of attacker activities. The proposed method is a two-stage pattern that in the first step honeypot deceives the attackers and collects their information and behavior in the network. In the second step, relying on machine learning, the collected data is analyzed and malicious samples are distinguished from non-malicious ones. Among machine learning algorithms, methods based on deep learning provide high accuracy, but these algorithms have high computational complexity; They reduce the speed of detection. While detection speed is very important in botnet attacks. To overcome this challenge, a separable convolutional neural network with a group learning approach was proposed in this paper. The proposed method was implemented in Python simulation environment and its efficiency was analyzed in different evaluation indices. Examining the results shows that the proposed method detects 99% of IoT botnet attacks with accuracy. Compared with similar designs, the proposed method has been able to; Improve the accuracy of attack detection.

Keywords: Honeypot, botnet, Internet of Things, separable convolutional network, group learning.

Power System Technology
ISSN:1000-3673

Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

Introduction

Today, due to the increasing progress of technology and the expansion of social networks and sites, information theft or the spread of fake news is expanding day by day and becoming a social problem [1]. Due to this large number of active users, the attention of cybercriminals has been directed to these networks [2]. Bots are one of the ways to steal information from social networks [3]. Botnets are one of the most important threats in the cyber space [4]. Botnets are a network of infected computers that are under the command of one or more bot administrators and execute their commands [5]. When a host computer is infected by bot binary malware, it becomes an actual bot and can execute bot manager commands [6]. In simpler words, a botnet is a set of systems connected to the Internet that has been placed under the authority of a foreign entity called the boss or commander through a malicious software (bot) [3, 7]. The primary purpose of botnets is to carry out destructive activities or attack under the control of a commander [8]. The malicious software used to create botnets is usually a Trojan, which, in addition to its normal activity, provides cooperation with the commander without the knowledge of the system owner [9]. Nowadays, the growth of botnets has turned the special attention of security research [10]. The level of botnet power and its evaluation is one of the most important challenges faced by researchers and managers of large and medium-sized organizations [11, 12]. Monitoring attacks carried out by bot networks still have challenges of uncertainty during the attack [13]. The main problem with botnets is that they perform these actions secretly [14], that is, until we specifically look for them, we will be unaware of their presence in the system, and as long as they remain in the victim's system, the victim's system It will not be able to resist against non-implementation of botnet owner's orders [15]. With the development of network bandwidth and computing power of machines, distributed computing is widely used today. In this regard, hackers also use this concept to carry out more powerful attacks.[16]

Recently, different botnets have been proposed for all types of networks. One of these areas is the Internet of Things [17, 18]. Considering the wide range of areas and equipment connected to internet networks, as well as the desire of the general public and the equipment manufacturing companies for intelligence and integrated communication and remote control as a feature, we see that these equipments, which are defined in the definitions and dimensions Applied to the Internet of Things, they are interpreted as victims of attacks and security disturbances and are exploited and have created a serious concern for security communities [19]. These threats and attacks are increasing every day and affect wider dimensions. Botnets are among the things that seriously threaten the Internet of Things and by using the vulnerability of the Internet of Things, they can attack service providers as well as hosts.[1]

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

One of the prominent techniques to identify a vulnerable device in the Internet of Things network is honeypot [20]. Honeypot is a new and highly dynamic technology [21]. This system is a trap that attracts attackers and keeps them away from the main network. Honeypots mislead attackers by simulating different services and operating systems and obtain information about them[22]. The difference between honeypots and other technologies is that honeypots detect unknown attacks while security technologies detect signature attacks [23]. Using Honeypot technology Along with other artificial intelligence tools, it has been able to; Help improve the security of the Internet of Things [24]. One of the most promising approaches in this field is the use of machine learning [25]. Such methods have the ability to detect new bots that have not been observed before.

Machine learning is a branch of artificial intelligence that uses different algorithms and techniques to extract useful information from raw data [26]. Machine learning methods are suitable in the analysis and prediction of large data, because it is impossible to try to manually process a large amount of data without the support of machines [27]. Machine learning in computer science tries to solve problems not only mathematically but also algorithmically [28]. In fact, learning and building algorithms that can learn from data sets and predict outcomes [29]. Machine learning has provided us with intelligent disease detection tools, intelligent abnormality detection tools, intrusion detection tools, self-driving cars, effective web search, human voice recognition, image recognition and many more, and we live our daily lives without To know that we are using them [30]. Machine learning consists of two stages: learning and prediction. Supervised, unsupervised, semi-supervised and reinforcement learning are some popular types of machine learning.

- Supervised methods: Supervised algorithms are trained on a predefined dataset, which then facilitates its ability to reach an accurate conclusion when presented with new data [31, 32].

- Unsupervised methods: In unsupervised methods, a set of data is given to the algorithm without any labels so that it can find patterns and relationships between the data [33].

– Semi-supervised methods: Semi-supervised learning uses labeled and unlabeled data for training [30].

- Reinforcement methods: Reinforcement learning algorithms learn in an interactive environment by trial and error using feedback from their actions and experiences [30].

Deep learning is a relatively new approach in machine learning that has shown significant results in discovering the hidden knowledge of raw data. Deep learning is considered a subset of machine learning in which, based on multi-level learning, in a hierarchical structure of features or concepts of higher levels, concepts and features of lower levels are defined, and

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

also low-level concepts can also help define higher-level concepts. In simpler words, the main goal of deep learning is to intelligently extract features during several learning stages.

In this article, an attempt will be made to distinguish the malicious flow from the normal flow in the Internet of Things by using Hanbpot technology and analyzing the features related to botnet attacks and deep learning. Among the different deep learning methods, convolutional neural networks have been used more for such problems[34]. Meanwhile, different methods such as recurrent neural networks [35], short-term memory networks [36] and gate recurrent networks [37] have also been used for such problems. Although convolutional networks have high capabilities, high computational complexity makes it impossible to use them in tasks that require high detection speed; used [38]. Detection of botnet attacks in the Internet of Things should be done in the shortest possible time due to the high importance of user information security [39]. To solve the challenge of high computational overhead of convolutional networks, a separable architecture for convolutional networks has recently been proposed [40]. In this architecture, to reduce the number of parameters of the convolutional network, two convolution operations called point convolution and channel-wise convolution are used, which while significantly reducing the parameters, the accuracy remains at the desired level [41]. By reducing the number of parameters, it is also possible to create a deeper network; As a result, accuracy can also increase [42]. There are many methods to create such networks. However, in the general and common mode, the two methods of reducing the number of parameters by inventing a new structure of the convolution layer and compressing the parameters have received more attention from researchers[43].

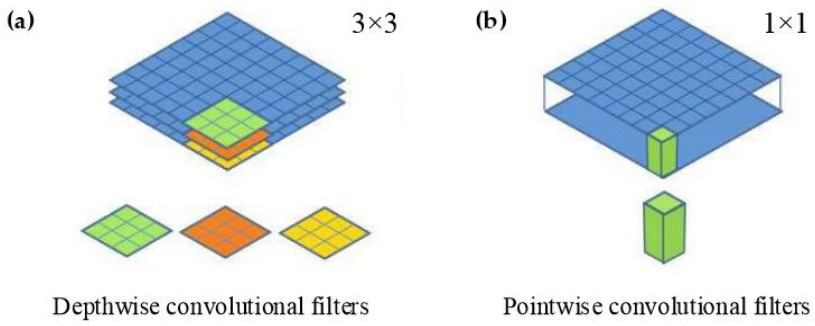


Figure (1) convolution network according to separable channel [44]

But in general, one of the most important disadvantages of convolutional networks is the presence of fully connected layers that include the largest number of learner parameters[45]. These layers are responsible for learning the features extracted by convolutional layers. Also, the last layer of fully connected layers is known as category score calculator [46]. This layer calculates the outputs for each category by a probabilistic function such as Softmax. After that, the network error rate is calculated by a cost function. In order to reduce the amount of network

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

error, the error is propagated into the network and the weights of each neuron in the fully connected layers and the amount of kernels in the convolutional layers are changed by the post-propagation function [47]. Fully connected layers in CNN are computationally heavy and time-consuming[47], on the other hand, they are less accurate than classifiers such as support vector machine, decision tree, random jet flower, etc.[48].

Various experiences of using different machine learning methods, even deep learning, show that there is no single specific algorithm that can be the best and most accurate for all applications [49]. In fact, each algorithm is a special model based on certain assumptions. Sometimes these assumptions are established and sometimes they are violated [50]. Therefore, no single algorithm can work successfully in all conditions and for everyone. To solve this problem, group training method has been introduced. The main motivation for developing such a method is to reduce the error rate [51]. The basic assumption of this methodology is that in the collective mode, the probability of making a mistake in recognizing the category or location of a new sample is much lower than the prediction mode with only one model. When combining independent and different decision makers, since each of these decision makers will perform better than a random guess in the worst case, the probability of making the right decision is enhanced as a result [52].

It seems that the combined use of honeypot technology, separable convolutional networks and basic machine learning algorithms with a group learning approach can increase the accuracy of botnet detection in the Internet of Things. Accordingly, we propose a hybrid classifier for IoT botnet detection, in which convolutional networks and support vector machines are used as a group.

2) research context

The present paper proposes a new and hybrid approach to detect IoT botnet attacks, in which concepts such as IoT, IoT botnet attacks, honeypots, and convolutional neural networks together form an efficient structure to achieve optimal accuracy. In this section, each of these concepts is briefly explained.

1-2) Internet of things and security index

The Internet of Things is a network of electrical equipment and sensors connected to each other in order to exchange information with each other, which is used for the purpose of remote sensing and control [53]. In this network, the ability to send data through communication networks, either the Internet or intranet, is provided for any entity or object, and a set of systems can be automatically and Intelligent control and management. The Internet of Things uses several other technologies such as wireless sensor network, machine-to-machine

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

communication, robotics, Internet technologies, smart devices, etc. [54]. The Internet of Things has brought many benefits to users. The connected nature of IoT devices means that if one device has a security weakness, it has the potential to affect the security and flexibility of the entire system internationally[55]. This behavior is simply due to the widespread use of devices connected to the Internet of Things. Furthermore, the ability of some IoT-connected devices to be mechanically connected to other devices means that IoT users and developers all have an obligation to ensure that they do not expose other users, as well as the Internet itself, to potential harm. They do not give [56]. Figure (2) shows the uses of the Internet of Things in the current era. In all practical aspects of the Internet of Things, security is considered a vital category.

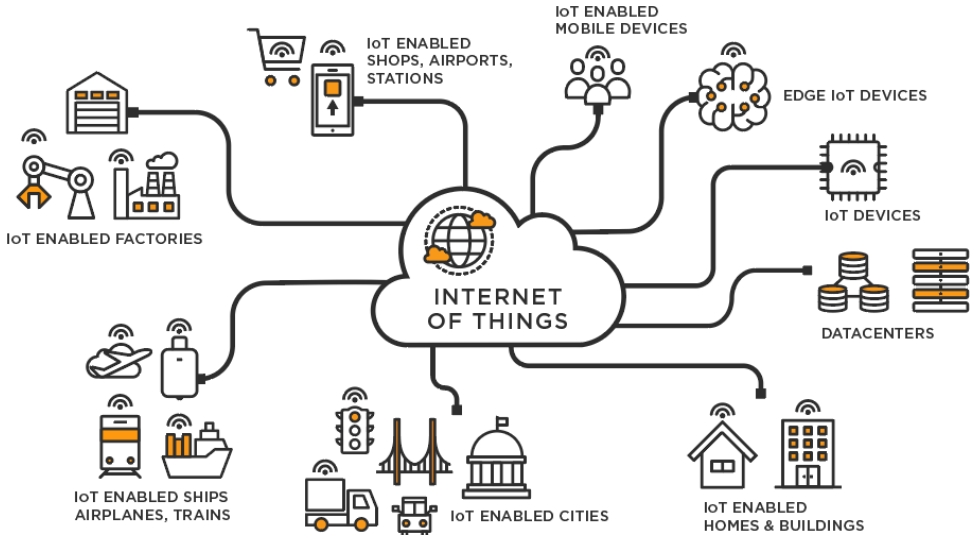


Figure (2) introducing the Internet of Things and its applications

For IoT devices that have limited computing power, memory, radio bandwidth, and resources; It is generally not cost-effective to perform security tasks, especially in large data streams; Or sometimes it is not even possible. This is due to intensive computing requirements and no delay in IoT connections [15].

Cyber security is an important part of the information and resource management framework in today's Internet of Things. Although the Internet of Things increases efficiency and productivity through intelligent and remote control, it also increases the risk of cyber attacks. The following factors contribute to the vulnerabilities of the Internet of Things against cyber attacks.

- Wide distribution of Internet of Things devices from every house to every house

- Wide distribution of Internet of Things in smart power grids

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

- Wide distribution of Internet of Things in smart cars

- also the complexity of protocols used by Internet of Things users [57]

Most current security solutions impose a heavy processing and communication load on IoT devices. This makes them unsuitable solutions for protecting IoT devices, so IoT devices are usually more susceptible to attacks than computer systems. Therefore, investigating the security issues related to Internet of Things devices as well as the Internet of Things environment is always considered as a necessity [15].

2-2) Honey pot

A resource is an information system that has false and unreal information on it and uses its value and false information to try to discover and collect unauthorized and illegal information and activities on the network [58]. In simple words, a honeypot is a computer system or systems connected to a network or the Internet that has false information on it and is intentionally placed in the network to act as a trap and be attacked by a hacker or intruder. and using this information to deceive them and collect information about how they enter the network and the goals they pursue in the network[59].

Honeypots appear like a victim system to the intruder and should behave like one [60]. But at the same time, without informing the intruder, they monitor him with all kinds of control methods and data recording [61]. This information is recorded and can be used later for analysis and used to learn unknown methods of attacks and intrusions. It differs from other similar security systems and technologies in its faster and optimal performance.[62]

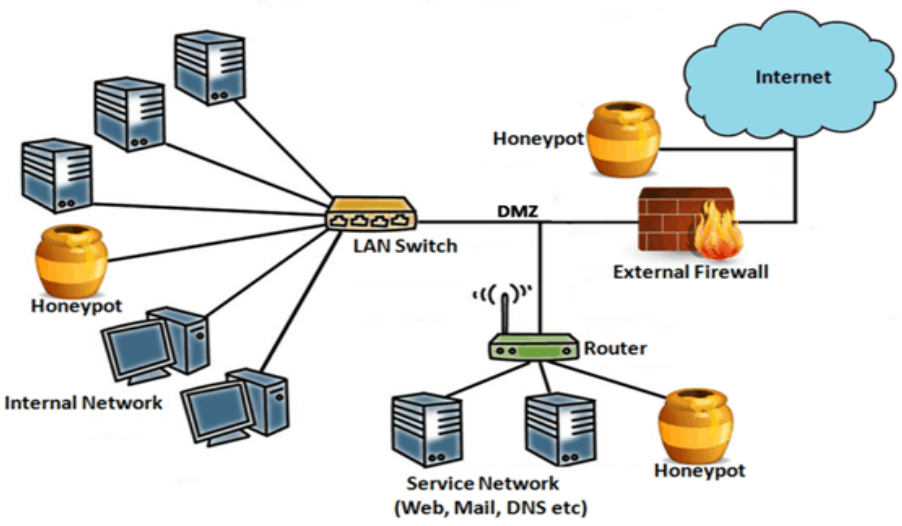


Figure (3) showing a honeypot in a distributed network

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

All these methods are considered inefficient due to the high volume of production data and incorrect data. Honeypots do not act defensively like these systems, that is, they do not wait for the intruder to take the lead in starting the attack. Rather, it tries to collect information about their styles and techniques. Like a firewall, honeypots are not limited to identifying known attacks, and it is a feature of a honeypot to discover new intrusion methods [63]. Honeypots give security analysts the chance to realistically study their adversary [64]. By analyzing how, when, and what hackers are behind rootkits, trojans, and exploits [64] the actual attacks are carried out. Network analysis can suggest and offer better and more efficient ways against such attacks [65]. Implementing strong monitoring on honeypots is not only useful for analysts, but it can also show other possible and potential network attacks [66]. Finally, it can be said that a honeypot is nothing more than a bait, but information is deliberately placed in it, which is tempting for any internal or external attacker, but in reality, what is done is to divert the intruders from sensitive targets. The value of the network is [67].

Honeypots have been created in various shapes and sizes, and collecting them for classification has made it a little difficult [20]. In the rest of this section, three common categories of honeypots are mentioned.

- The first category: This category is called Low-Interaction; Usually, they work with simulated services and operating systems, during which the intruder's activity is limited through the simulator. These types of honeypots are easy to implement. They are easy to use and maintain and cause the least possible risk [68].

- The second category: this category of honeypots, which are also called High Interaction; There are different honeypots; Because they are considered more complex solutions due to dealing with the operating system and real applications. In this category of honeypots, nothing is simulated and everything is real at the disposal of the intruder. In this category, honeypots do not speculate about the intruder's behavior, but provide a real environment for his activity and will learn behaviors that have not been expected so far through Honeypots [68].

- The third category: in this example, by simulating the FTP server, the intruder's login ID and password are recorded and it is possible to access the command lines that he intended and used; He even found out about the cases that the intruder sought to obtain information from [68].

2-3) Botnets and Internet of Things

Botnets are networks formed by taking over a collection of computers called bots [34, 69]. These networks are controlled by one or more attackers with the aim of performing malicious activities [70]. By being placed on the victim's system, this malware takes it under its control

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

and starts spying on the system [71]. Botnets are the most widespread and dangerous threats in cyber attacks, and the reason for this dangerousness is their indiscriminate expansion[72].

The word bot is derived from robot and is actually a malicious binary code that is executed on vulnerable hosts and allows an attacker (known as a bot manager) to remotely access those hosts. guide him with his orders[73]. Botnet also means a network of hosts infected with bots. Sometimes a bot-infected system is called a zombie, and a bot-infected system is called a zombie army. When a computer is infected with a bot, it will no longer be able to resist the commands of the bot manager or refuse to execute them [9]. As a result, the attacker can use the processing power of the captured hosts in a distributed manner for his own benefit and organize various types of attacks in a coordinated manner and with a very high destructive power on the victim. This is while his identity usually remains hidden [3]. The size of a botnet depends on the complexity and the number of computers captured in this botnet [8]. Due to the fact that botnets are made up of different malware technologies, it is not so easy to explain about them and the complexity of their work [16].

The low price of Internet of Things devices has increased their popularity and growth among technology enthusiasts. Cisco [74] predicts that the use of IoT devices may reach more than 29 billion by the end of 2023. However, these devices lack effective security and standards to protect them from attack and control by attackers. One of the most important attack scenarios in IoT is that IoT devices are compromised and added to a botnet. Once an IoT device is infected and compromised, an attacker can take control of it and use it to participate in various attacks. In general, a botnet can be defined as a collection of vulnerable devices that execute malicious code in the form of robots and are controlled by an administrator called a botmaster [75-77]. Typically, a botnet consists of three main components:

- Attacker;

- destructive infrastructure;

- Robots

These components communicate and operate in different botnet architectures. Botnets have a wide range of malicious uses, including email spam distribution, distributed denial-of-service attacks, password cracking, key logging, and cryptocurrency mining [77, 78].

So far, several malwares have been released to target IoT devices and create IoT botnets; has been identified. In this regard, we can mention Mirai, Bashlight, Wirex, Brickerbot Reaper and Hajime attacks [79, 80]. Things to consider in IoT botnet attacks

Many IoT devices, such as webcams and wireless routers, are poorly protected.

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

– Most IoT devices as long as they work properly; are not subject to security checks.

- IoT devices have a suitable capacity to spread attacks to the network. Because IoT devices are designed to require minimal user intervention. Internet of Things devices are a suitable platform for spreading botnet attacks[81].

Today, most of the solutions offered to improve network security require heavy calculations and large memory; Therefore, security in the Internet of Things, which is based on thousands of connected devices and supports massive data; It is considered a big challenge [82]. The volume of data generated by these devices increases exponentially and can contain confidential information. The data generated by the Internet of Things is expected to reach 73.1 ZB by 2025[83]. Figure (4) shows the structure of a botnet attack in the Internet of Things.

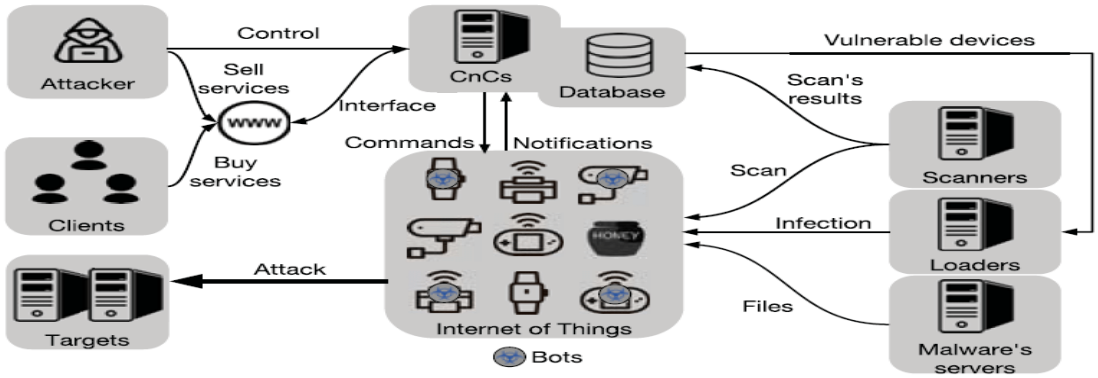


Figure (4) Internet of Things botnet attack

2-4) Convolutional neural network

Convolutional neural networks are prominent algorithms in the field of deep learning that researchers have used in various fields[84]. This algorithm is from machine learning, although it has a relatively high time complexity. But considering its advantages; It encourages researchers to use it [85].

- Provides better results than basic machine learning algorithms in the areas of prediction, classification and estimation.

- It has few parameters to adjust.

- In the convolutional neural network, a set of connections can have the same weight; This can reduce many parameters.

- Sampling in convolutional neural network can be done by preserving useful information [86].

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

Several structures of convolutional networks have been presented, all of which seek to improve the machine learning process. However, the main components of convolutional neural networks are the same [87]. Figure (5) shows the general structure of a convolutional neural network. In the following, the main implementation of this algorithm is introduced.

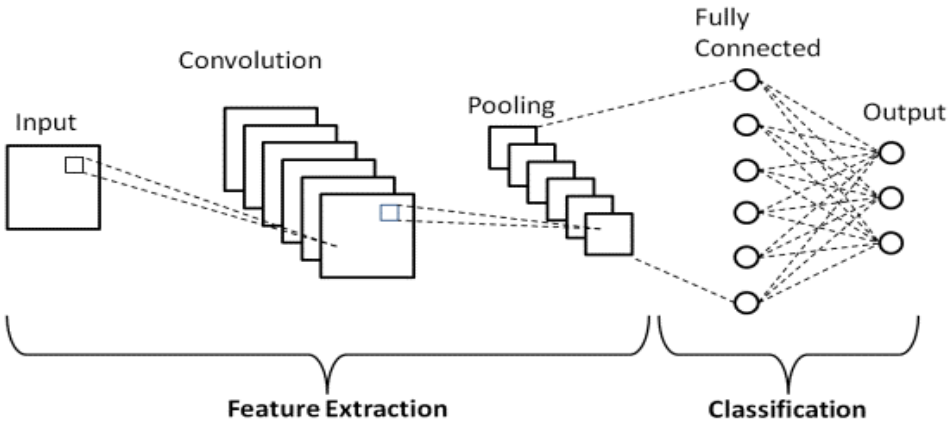


Figure (5) General structure of a convolutional neural network [88]

- Convolution layer: This layer is used to extract features from the input. Convolutional neural network uses different filters for this purpose. In this process, the length of each filter is modeled with a constant value k and its height with h [87].

- Pooling layer: In convolutional neural networks, a pooling layer should be used after each convolution layer to reduce the size of intermediate features [87].

- Activator function: The activator function is one of the main elements of convolutional neural networks and its use causes all neurons to be inactive at the same time. This means that only part of the neurons of the network are active at a time. Faasaz function thins the network and only learns the important features[87].

- Fully connected layer: This layer is located after the last pooling layer and maps two-dimensional intermediate features to one-dimensional vectors to continue the learning process. The fully connected layer is responsible for recognizing the classes it has [87].

3) Previous works

In the field of detection of IoT botnet attacks, different studies have been done in recent years. In this section, some of the performed works are mentioned:

In [89], using the honeypot framework and machine learning, a model for detecting DDoS botnet attacks in the Internet of Things is proposed. In this paper, the data generated by

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

Honeypot in the Internet of Things is used as a dataset for effective and dynamic training of a machine learning classification model. This approach can be considered a constructive start to combat zero-day DDoS attacks; This type of attack has recently become an important challenge in the field of Internet of Things security.

In [71], a model for detecting and analyzing the behavior of botnets using honeypot and classification techniques is presented. In this article, researchers believe that botnets can be identified using honeypots and their behavior can be analyzed using machine learning algorithms. Accordingly, they use Honeypot to collect network data and rely on this data to extract network traffic flow. Network flow is used to analyze traffic behavior caused by hosts. In this case, the hosts are generally botnets. Behavioral analysis is also done to find botnet attack patterns using machine learning. For the process of machine learning, several algorithms such as decision tree, logistic regression, support vector machine and random forest have been examined and the results of the experiments show that by relying on the honeypot structure and machine learning patterns, the traffic belonging to Detected a botnet.

In [90], a model for detecting advanced botnet attacks in the Internet of Things is proposed, which is based on intelligent and honeypot techniques. In this article, researchers have extracted the behavioral characteristics of botnet attacks after collecting data from honeypot and using logistic regression algorithm to diagnose and predict attacks. According to the results of the tests, it can be expected that the proposed security architecture will be used in intercepting large botnet attacks. Because the analysis of tests shows that the model proposed in the article has promising accuracy in identifying attacks.

In [91], using deep learning, an intelligent mechanism for detecting IoT botnet attacks is proposed. The data set used in this article is the N-BaIoT set and the accuracy, correctness, learning and F1 indicators have been used to evaluate the convolutional model. Examining the results shows that the proposed method of the article can detect different botnet attacks with 99% accuracy.

In [92], a machine learning-based approach to detect mobile botnets is presented. In this article, researchers have used machine learning algorithms to identify unusual network behaviors. They implemented their approach on a dataset that contains 13 families of mobile botnets and normal programs, and in this regard, they extracted the desired features by relying on statistical methods. Investigations in the mentioned evaluation criteria show that the proposed approach of the article obtains very good results in mobile botnet detection, especially the criteria of false positive rates and true positive detection rate.

In [38], an approach based on deep learning is presented to identify botnet activities in Internet of Things equipment and consumer networks. Deep learning is a sub-branch of machine

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

learning and is based on a set of algorithms that are trying to model high-level abstract concepts in the data. This process is done using a deep graph that has several processing layers consisting of several layers of linear transformations and They are non-linear, they model. In other words, it is based on learning to display knowledge and features in model layers. The model proposed by researchers in this article is BLSTM-RNN botnet detection, which uses a labeled data set in the training process. Investigations show that although the proposed model has high accuracy in the detection process, the amount of calculations and processing time is long.

In addition to the works mentioned in [72], a machine learning-based model for botnet detection is proposed, in which the process of training algorithms is done using a labeled data set. In this article, researchers use accuracy assessment criteria. , remembering and working accuracy of different machine learning algorithms in bot detection process have checked. The results of the surveys show that machine learning-based techniques always produce good results in botnet detection. But among all the reviewed algorithms, the random forest algorithm has the best accuracy with more than 90%

4) The proposed method

In recent years, there have been many botnet attacks on Internet of Things devices and the result has been heavy losses to companies and organizations. Therefore, considering the sensitivity of the issue, several approaches have been proposed to detect botnet attacks. Recently, researchers have been able to reduce the vulnerability of the network to some extent by using honey pot and the information obtained by it. Honeypots are a relatively new technology in the field of security. A honeypot is a security tool whose value lies in being discovered and investigated, attacked and compromised. Honeypots can be used to detect attacks, malware, slow attacks, decoys, and investigate attacker activity. Honeypots can also be used in criminology by collecting evidence of the attacker's activities. In this article, an efficient approach will be proposed to improve the security level of Internet of Things by using honeypot and machine learning.

The proposed method is a practical approach that will be implemented in the Python environment. This approach includes two general phases. In the first phase, by using the cowrie honeypot, the network attackers are misled and their information is saved. This system is a trap that attracts attackers and keeps them away from the main network. In the second phase, by analyzing the information obtained by Honeypot, the process of detecting botnet attacks on the Internet of Things network is carried out. The second phase is an approach based on machine learning and deep learning, which consists of a multi-step process. In the first stage, the pre-processing operation is done on the information obtained in Honeypot. The purpose of the pre-processing operation is to improve the data. In this section, operations such as replacing

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

missing data, normalizing data, and dividing data are performed. The data normalization operation is based on three normalization modes: quantitative, interval and literal. The purpose of data segmentation is to group data into training and testing data. In the next step, the pattern extraction operation is performed. The purpose of this section is to extract patterns that increase the accuracy of detection systems. In this article, convolutional neural networks have been used to extract the pattern. The purpose of convolutional neural networks is to extract patterns hidden in features. Convolutional neural networks are composed of convolutional, integrated and fully connected layers for pattern extraction. After the pattern extraction operation, classification algorithms have been used to classify the data. In this article, nearest neighbor classifiers, decision tree and support vector machine are used for data classification, which determine the final data class with the majority vote strategy.

The information in figure () shows that the detection of botnet attacks in the second phase includes three general steps. In the first stage, the data is pre-processed. In the second stage, pattern-finding operation is done by convolutional neural networks. In the third stage, the classification operation is performed by relying on group training and majority vote strategy by three classifications: nearest neighbor, decision tree and support vector machine. In the following, each of the desired sections is described.

1-4) Collecting botnet information with honeypot

In the proposed plan, machine learning methods will be used to identify the attacker's performance and detect the attack. For this purpose, the information received by Honeypot is first processed in the form of text logs. Then, based on the model that is formed to detect the attack; The received information is analyzed. Honey Pot is recommended by Cowrie; which will be launched by the Linux virtual machine. In this virtual machine, peripheral tools necessary to collect information and display it are installed and run. The log files will be processed by programs developed in python language and the result will be displayed.

Cowrie Honeypot is an open source honeypot. This tool is developed based on a script from another honeypot called Kippo. This moderately interactive honeypot is capable of simulating several Linux tools with a standard bash user interface. Cowrie Honeypot lacks any analysis and blocking tools to identify and disable malware. This honeypot is able to save (log) all communications that are established at the network level. For this, it manages and logs all incoming communications. Stores and responds to incoming commands in detail. This honeypot shows the attacker or malware by creating conditions similar to real tools in order to succeed in finding a real tool with security holes. Malware or an attacker, with the idea that he has succeeded in identifying a vulnerable tool, implements his plan to infiltrate, send malicious files, extract information, etc. Cowrie's honeypot provides cybersecurity analysts with the

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

information necessary to identify methods and patterns of attack and destruction by fully storing the functions of any type of malicious or non-malicious communication. At the same time, it locks the attacker and the malware in a closed environment that has no way out. Since Cowrie stores all communications and information exchanged, the log files produced by it contain a lot of information. The high volume of this information has made the work of investigation and conclusion very difficult and even impossible.

On the other hand, the widespread use of well-known honeypots such as Cowrie has made this tool easily recognized by malware. When the malware detects the honeypot, it removes it from the attack list and does not perform any information exchange or operation. For example, common network scanning and identification tools such as nmap are now able to identify many commercial and open source honeypots, including Cowrie. Among these, we can mention malware like Aisuru. This malware detects the Cowrie honeypot and reports it to its central control (C&C) server so that they can be removed from the list of attacked addresses in future attacks. In this thesis, the Cowrie honey pot is first examined, installed and implemented in full detail. Then the main methods of identifying this honeypot are shown and methods to deal with them and prevent its identification are presented.

2-4) Pre-processing

As mentioned in the previous sections, pre-processing consists of three methods: missing data correction, normalization and segmentation. Each of these operations is described below.

A) Correction of missing data: As the name suggests, missing data refers to data that some of its values are not available. In order to replace these values, attention is paid to the type of feature. Figure (7) shows the method of replacing missing data.

Figure (7): Missing data correction methods

As shown in the figure above, in order to replace missing data values, it is first determined what kind of feature it is. If the feature is continuous features, the average method is used to replace missing values, but if the feature is discrete, maximum repetition is used to replace missing values. In this case, the most repeated value is considered as the replacement value.

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

b) Normalization: One of the important and fundamental parts of pre-processing operations is related to data normalization. Data normalization has a direct effect on the efficiency of diagnosis algorithms. Therefore, in this study, three normalization methods are used which are given in figure (8).

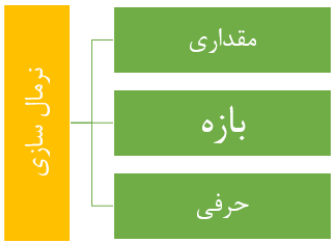


Figure (8): Data normalization methods

As shown in the figure above, data normalization consists of three quantitative, interval and literal methods. In the letter normalization method, a unique number is assigned to each letter feature, finally, the letter features are converted into numerical features. In the value normalization method, the attribute values change from one interval to another. In the following relation, the normalization operation is shown.

$$F_{norm} = \frac{f - lb}{ub - lb} * (ub^* - lb^*) + lb^* \quad (1)$$

In the above relationship, F_norm represents the value of the feature after the normalization operation, f represents the value of the feature after the normalization operation, lb represents the minimum value of the feature before the normalization operation, ub represents the maximum value of the feature before the normalization operation. So, lb^* represents the minimum feature value after the normalization operation and ub^* represents the maximum feature value after the normalization operation. In interval normalization, feature values are divided into smaller intervals and a unique number is assigned to each interval.

c) Data segmentation: As mentioned in the previous section, the purpose of data segmentation is to group data into training and testing data. In order to divide the data, the methods shown in figure (7) are used.

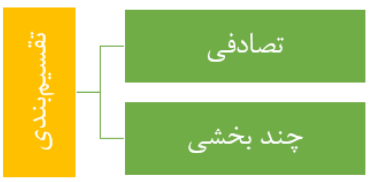


Figure (9): Distribution of data

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

As shown in the figure above, in order to divide the data into training and testing data, two random and multi-part methods are used, and the multi-part method is used when the volume of data is be low.. In this research, the random method was used to divide the data. In the random method, the data are divided into two categories, training and testing, with a percentage of 70 to 30, where 70% of the data is related to the training data and 30% of the data is related to the training data. It is a test.

3-4) pattern finding

One of the important parts of the proposed method is pattern finding. The purpose of pattern finding is to extract hidden relationships between features so as to increase the accuracy of detection systems. In this research, deep learning networks are used for data modeling, and the advantages of using deep learning networks for data modeling are shown in Figure (10).

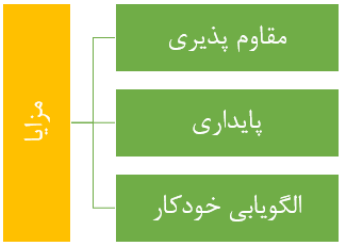


Figure (10): data modeling

As shown in the figure above, the advantages of deep learning networks compared to other pattern finding methods such as appearance, texture pattern finding, etc. include robustness, stability and automatic pattern finding. The most important feature of deep learning networks is the automatic pattern finding of features. Therefore, the efficiency of deep learning networks is higher. Also, deep learning networks are resistant to outliers and noisy data and can obtain correct answers in noisy environments. Unlike other pattern-finding algorithms, deep learning networks do not reduce the efficiency of these networks with the increase in the volume of data. In the figure below, the process of identifying classes in deep learning networks is shown.

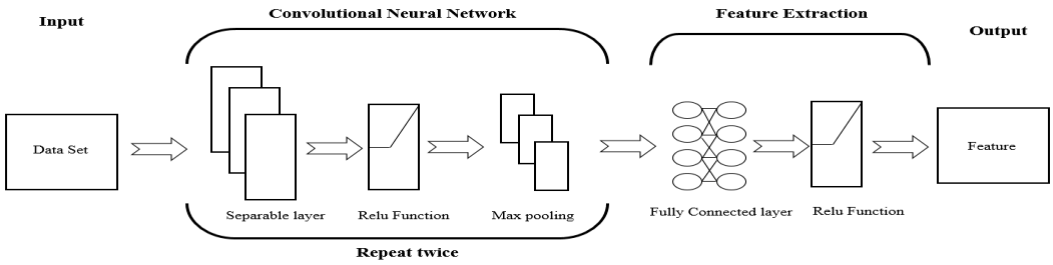


Figure (11): pattern extraction by convolutional neural networks

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

As shown in the figure above, in order to extract the pattern, the data set is given to convolutional neural networks and finally the extracted features are given to the user as output. In this process, convolution, integration and fully connected layers have been used to extract the pattern. In the following, each of the desired sections will be explained.

c) Fully connected layer: The task of this layer is to convert feature matrices into feature vectors. In this case, each cell related to the feature matrix is placed in a house of the feature vector. To better understand this issue, consider the following image.

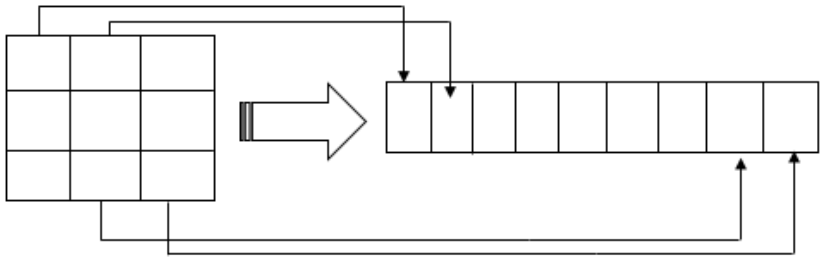


Figure (16): Converting feature matrix to feature vector

4-4) Classification

As mentioned in the previous section, three basic classifications have been used to classify botnets. The classifiers used in this research include nearest neighbor, decision tree and support vector machine. In the figure below, the operation of data classification by basic algorithms is shown.

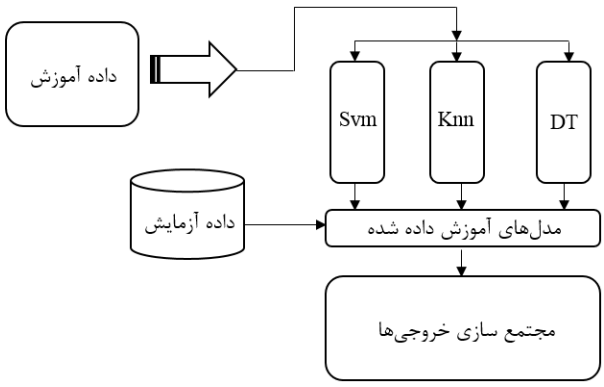


Figure (16): data classification

As shown in the figure above, training data is given to each classifier. And based on the training data, the desired models are made. After building the desired model, test data is given to each classification. Each classification is based on the education he had. It has a diagnosis for each

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

sample. Finally, the desired outputs are stored in the matrix as an integration matrix so that the majority vote operation is done based on this matrix.

4-5) Composition of class

In this research, the majority vote was used to combine the results. Table (1) shows the operation of the majority vote. In this table, three categories of three samples have been categorized.

Table (1): An example for group learning

	Knn Output	Output DT	Output Svm
Example 1	1	2	1
Example 2	2	1	2
Example 3	3	3	3

In the majority voting strategy, each of the models (machine learning algorithms) independently recognize the class of the test sample (botnet or not). In the following, the votes of the models are counted to determine the class of the sample and the class that has the most votes; The sample belongs to it[93]. Table (2) is the result of the classification process for the three test samples reviewed in Table (1); shows

Table (2): majority vote strategy in group learning

Samples	Output of the majority vote
Example 1	1
Example 2	2
Example 3	3

As shown in the figure above, a class with the highest value is selected as the final class.

5) Evaluation

In this section, firstly, the characteristics of the simulation environment are examined from the software and hardware points of view. After introducing the characteristics of the simulation environment, the packages used in this research to simulate the proposed method are given. . After the introduction of the used packages, the evaluation parameters and the description of the data set are given. Finally, at the end of the research, a comparison between the proposed method and other evaluation methods is given based on the criteria of precision, accuracy,

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

recall and F criterion. In the following, the explanations related to each of the desired sections are given.

1-5) research dataset

The research dataset is a standard and publicly available collection that was published in 2018 in order to conduct research in the field of detecting botnet attacks in the Internet of Things. This data set is known by the abbreviation N_BaIoT and was collected by monitoring the attacks carried out on 9 IoT devices. In this data set, three different modes are considered for the samples. Accordingly, each sample belongs to one of three classes: Mirai, BASHLITE, and normal traffic. Based on the data contained in the N_BaIoT dataset, among the 849,234 monitored samples, 17,936 samples are related to healthy data and 831,298 samples are related to botnet attacks.

In this data set, each of the Mirai and BASHLITE attacks includes a subset of attacks. BASHLITE attacks include five categories of scan, spam, udp, tcp and combo attacks. Mirai attacks also include scan, udp, ack, syn and udpplain attacks. Table (3) introduces the IoT botnet attacks in the N_BaIoT dataset.

Table (3) Introduction of IoT botnet attacks in N_BaIoT data set

explanation	BASHLITE	Mirai	attack
Network scanning for vulnerable devices	✓	✓	Scan
Sending spam information	✓	×	unwanted
UDP flood	✓	✓	Udp
TCP flooding	✓	×	TCP
Sending spam data and opening a connection to a specified IP address and port	✓	×	combined
K flood	×	✓	Ak
Flood Syn	×	✓	Syn
UDP flooding with fewer options, optimized for higher packets per second	×	✓	Udp plain

2-5) simulation environment

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

In this research, to evaluate the proposed method, an environment with the following specifications has been used, and these specifications are given in Figure (17).

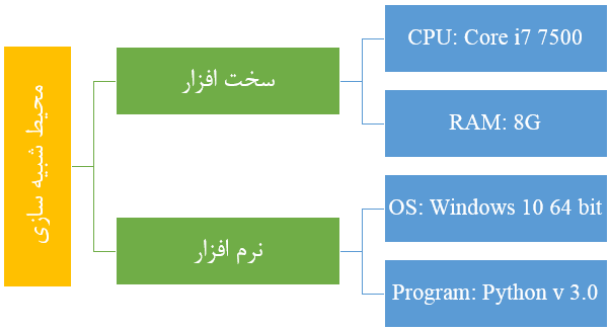


Figure (17): Characteristics of the simulation environment

3-5) Packages used

Table (4) shows the packages used in this project to simulate the proposed method, which is given below.

Table (4): Packages used in this research

Package name		**Application**
Google.Colab		**To connect Google Kolb to Google Drive**
Pandas		**To work with Excel files**
Numpy		**To work with arrays**
Model Selection		**To divide the data into training and test data**
Utils		**To convert vector classes to column classes**
Keras	Layers	**To use deep learning network layers**
	Model	**To make the model**
	Loss	**To set the error calculation algorithms**
	Optimizer	**To adjust the weighting algorithms**
Sklearn	Svm	**To use the support vector machine algorithm**

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

	Tree	**To use the decision tree algorithm**
	Knn	**To use the nearest neighbor algorithm**
	Enssemble	**To use the majority vote algorithm**
	Metrics	**To calculate the evaluation criteria**

4-5) evaluation indicators

In this research, classification criteria have been used to evaluate the proposed method. The classification criteria used in this research include precision, accuracy, recall and F criteria. These criteria are given below.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}} \quad (2)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (3)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (4)$$

$$\text{F Measure} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} * \text{Recall}} \quad (5)$$

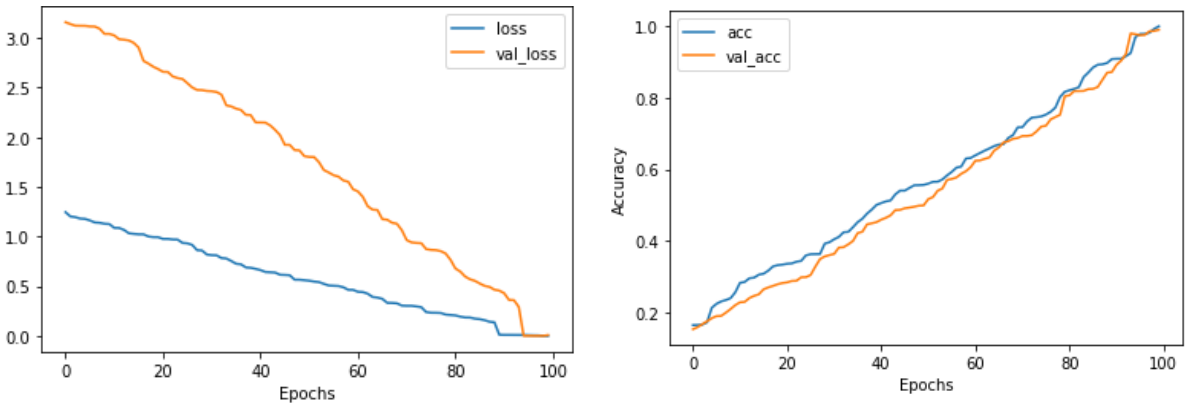
In the above relationship, TP represents the number of samples whose real class is non-attack, but the proposed method incorrectly detects an attack, FP represents the number of samples whose real class is attack, but the proposed method The mistake of their class has been recognized as non-attack. FN represents the number of samples whose real class is non-attack, but the proposed method mistakenly recognized their class as attack, and finally TN represents the number of samples whose real class is attack and the method Proposition has also correctly identified their class as an attack.

5-5) Test results

Examining the execution of experiments shows that the proposed approach has been able to; Detects IoT botnet attacks with better accuracy. Figure (18) shows the convergence of accuracy and error with the proposed model. In these charts, the higher the accuracy and the lower the error rate; It shows the efficiency of the method.

Power System Technology
ISSN:1000-3673

Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024



Accuracy convergence graph in the proposed method. Error reduction graph in the proposed method

Figure (18) process of detection of botnet attacks in the proposed method

Also, the results of the proposed method based on the criteria of accuracy, correctness, recall and F criteria are given in table (5), which are as follows:

Table (5): The results of the proposed method based on classification criteria

	accuracy	accuracy	recall	F-criterion
Suggested method	99	99	99	99

As shown in the table above, the accuracy of the proposed method on the botnet dataset is very accurate. Table (6) shows the results of accuracy, recall and F criteria for different classes.

Table (6): The results of the proposed method for separate classes

class	accuracy	recall	F-criterion
Begin	100	100	100
Ecobee Thermosta	100	99	99
Doorbell	100	100	100
Baby Monitor	100	100	100
Security Camera	99	99	99
Webcam	99	100	99

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

As shown in the table above, the effectiveness of the proposed method in identifying the first, third and fourth classes has been the most accurate and it has been able to correctly recognize the samples in these classes. Figure (19) shows a comparison between the accuracies of each class.

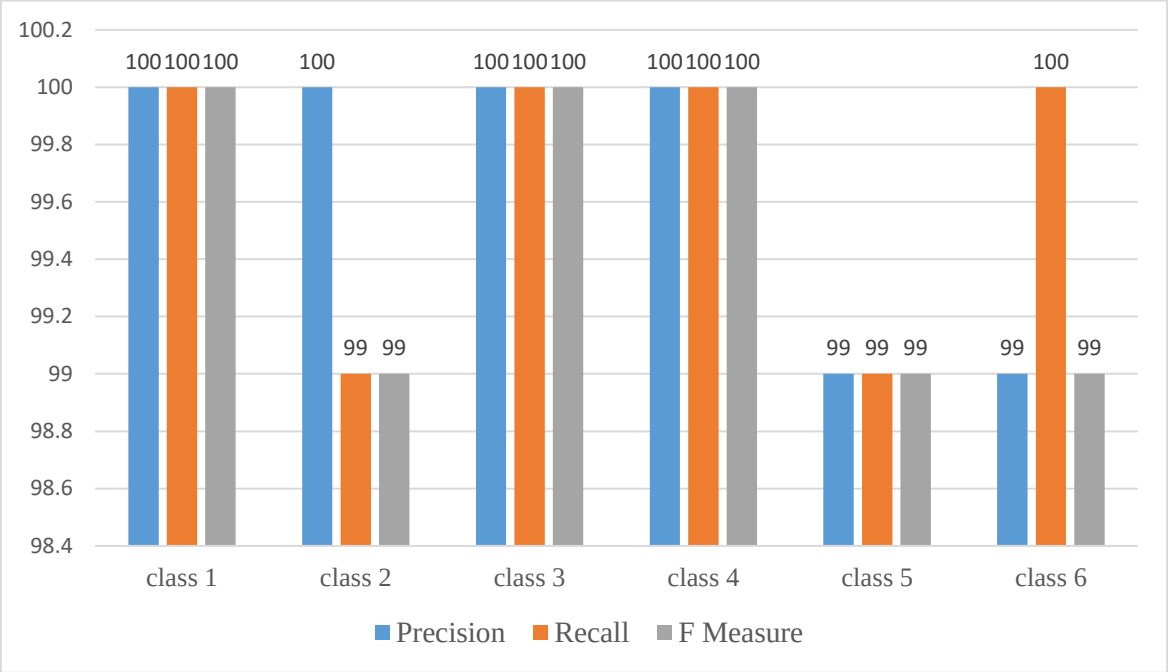


Figure (19): The results of the proposed method for different classes

5-6) Comparison with previous researches

In this section, the results of the proposed method are given with the results stated in the reference article based on the F criterion, and these results are given in Table (7).

Table (7): Comparison of the proposed method and reference results based on the F criterion

		Doorbell	Baby Monitor	Security Camera	Webcam
reference	Gaussian NB	95	84	88	98
	Bernoulli NB	91	93	83	99
	Multinomial NB	1	1	1	1
Suggested method		1	1	99	99

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

As shown in the table above, the accuracy of the proposed method is higher than the methods described in the reference article. In the basic article, each attack is given as a separate class and in binary form to the evaluation methods, while in the proposed method, the data is given in full and in multiple classes, hence the criterion F in Two classes are lower than the multidimensional Bayesian results criteria. If the results of the proposed method are also considered in binary form, the accuracy of the proposed method is also 100% because in this case the attacks do not have common behaviors and the algorithm only needs to detect one attack.

6) Conclusion discussion

Today, botnets are known as one of the most important threats to the Internet infrastructure. Each botnet is a group of hosts infected with the same malicious code and controlled by a remote attacker through one or more command and control servers. These techniques help the attacker to periodically and dynamically change the location of their command and control servers and prevent their addresses from being blacklisted. Meanwhile, the newness of the Internet of Things and its security challenges have caused attackers to carry out massive attacks on it. In recent years, there have been many botnet attacks on Internet of Things devices and the result has been heavy losses to companies and organizations. Several approaches have been proposed to detect botnet attacks; Some have proposed deep learning approaches for this purpose. Some have also used basic machine learning algorithms. In the meantime, some have investigated hybrid approaches such as the combination of meta-heuristic algorithms and machine learning in order to improve the accuracy of diagnosis and reduce the computational complexity of diagnosis. But in recent years, researchers have been able to reduce the vulnerability of the network to some extent by using honeypot and the information obtained by it. Honeypots are a relatively new technology in the field of security. A honeypot is a security tool whose value lies in being discovered and investigated, attacked and compromised. From this definition, we can conclude that honeypots are not limited to a specific problem and can have different applications depending on our needs. Honeypots can be used to detect attacks, malware, slow attacks, decoys, and investigate attacker activity. Also, honeypots can be used in criminology by collecting evidence of the attacker's activities. In this article, an efficient approach was proposed to improve the security level of Internet of Things by using honeypot and machine learning. Among the existing approaches, methods based on deep learning offer high accuracy, but these algorithms have high computational complexity; They reduce the speed of detection. While detection speed is very important in botnet attacks. To overcome this challenge, a lightweight convolutional neural network with a group learning approach was proposed in this paper. The proposed method was implemented in the Python simulation environment and its efficiency was analyzed in different evaluation indices. Examining the results shows that the proposed method detects 99% of IoT botnet attacks with accuracy. In

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

comparison with similar plans, the proposed method has been able to; Improve the accuracy of attack detection. The reason for the superiority of the proposed design is the modeling of features by deep learning networks and the improvement of the convolution layer by the Separable layer.

Refrences:

[1] T. N. Nguyen, Q.-D. Ngo, H.-T. Nguyen, and N. L. Giang, "An Advanced Computing Approach for IoT-Botnet Detection in Industrial Internet of Things," IEEE Transactions on Industrial Informatics, 2022.
[2] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based IoT-botnet attack detection with sequential architecture," Sensors, vol. 20, no. 16, p. 4372, 2020.
[3] K. Alieyan, A. ALmomani, A. Manasrah, and M. M. Kadhum, "A survey of botnet detection based on DNS," Neural Computing and Applications, vol. 28, no. 7, pp. 1541-1558, 2017.
[4] L. K. Musambo, M. K. Chinyemba, and J. Phiri, "Identifying Botnets Intrusion & Prevention–A Review," Zambia ICT Journal, vol. 1, no. 1, pp. 63-68, 2017.
[5] Y. Xing, H. Shu, H. Zhao, D. Li, and L. Guo, "Survey on botnet detection techniques: Classification, methods, and evaluation," Mathematical Problems in Engineering, vol. 2021, 2021.
[6] X. Li, J. Wang, and X. Zhang, "Botnet Detection Technology Based on DNS," Future Internet, vol. 9, no ,4 .p. 55, 2017.
[7] A. Kumar, M. Shridhar, S. Swaminathan, and T. J. Lim, "Machine learning-based early detection of IoT botnets using network-edge traffic," Computers & Security, vol. 117, p. 102693, 2022.
[8] A. H. Lashkari, G. D. Gil, J. E. Keenan, K .Mbah, and A. A. Ghorbani, "A survey leading to a new evaluation framework for network-based botnet detection," in Proceedings of the 2017 the 7th International Conference on Communication and Network Security, 2017, pp. 59-66: ACM.
[9] K. Wang, C. Y. Huang, L. Y. Tsai, and Y. D. Lin, "Behavior-based Botnet detection in parallel," Security and Communication Networks, vol. 7, no. 11, pp. 1849-1859, 2014.
[10] S. Bagui, X. Wang, X. Wang, and S. Bagui, "Machine learning based intrusion detection for IoT botnet," International Journal of Machine Learning and Computing, vol. 11, no. 6, pp. 399-406, 2021.
[11] R. Abu Khurma, I. Almomani, and I. Aljarah, "IoT Botnet Detection Using Salp Swarm and Ant Lion Hybrid Optimization Model," Symmetry, vol. 13, no. 8, p..2021 ,1377
[12] S. Lee, A. Abdullah, N. Jhanjhi, and S. Kok, "Honeypot Coupled Machine Learning Model for Botnet Detection and Classification in IoT Smart Factory–An Investigation," in MATEC Web of Conferences, 2021, vol. 335, p. 04003: EDP Sciences.
[13] H. A.-B. Hashim, M. M. Saudi, and N. Basir, "A systematic review analysis of root exploitation for mobile botnet detection," in Advanced Computer and Communication Engineering Technology: Springer, 2016, pp. 113-122.

Power System Technology
ISSN:1000-3673

Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

[14] S. Lee, A. Abdullah, N. Jhanjhi, and S. Kok, "Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning," PeerJ Computer Science, vol. 7, p. e350, 2021.
[15] M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri, and L. Cheng, "Internet of Things botnet detection approaches: Analysis and recommendations for future research," Applied Sciences, vol. 11, no. 12, p. 5713, 2021.
[16] G. Kirubavathi and R. Anitha, "Botnet detection via mining of traffic flow characteristics," Computers & Electrical Engineering, vol. 50, pp. 91-101, 2016.
[17] I. Ali et al., "Systematic literature review on IoT-based botnet attack," IEEE Access, vol. 8, pp. 212220-212232, 2020.
[18] H. Zhao, H. Shu, and Y. Xing, "A Review on IoT Botnet," in The 2nd International Conference on Computing and Data Science, 2021, pp. 1-7.
[19] A. K. Shukla and S. Dwivedi, "Discovery of Botnet Activities in Internet-of-Things System Using Dynamic Evolutionary Mechanism," New Generation Computing, pp. 1-29, 2022.
[20] M. Amal and P. Venkadesh, "Review of Cyber Attack Detection: Honeypot System," Webology, vol. 19, no. 1, 2022.
[21] F. Ja'fari, S. Mostafavi, K. Mizanian, and E. Jafari, "An intelligent botnet blocking approach in software defined networks using honeypots," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 2, pp. 2993-3016, 2021.
[22] V. Crespi, W. Hardaker, S. Abu-El-Haija, and A. Galstyan, "Identifying botnet IP address clusters using natural language processing techniques on honeypot command logs," arXiv preprint arXiv:2104.10232, 2021.
[23] N. Mcinnes and G. B. Wills, "The VoIP PBX Honeypot Advance Persistent Threat Analysis," in IoTBDS, 2021, pp. 70-80.
[24] A. Marinakis, "A Systematic Comparison of Default based Versus Hardened IoT Systems Using Honeypots :Master Thesis| Supervisor: Maria Papadaki," ed, 2021.
[25] S. Hao, D. Liu, S. Baldi, and W. Yu, "Unsupervised detection of botnet activities using frequent pattern tree mining," Complex & Intelligent Systems, pp. 1-9, 2021.
[26] O. El Kouari, H. Benaboud, and S. Lazaar, "Using machine learning to deal with Phishing and Spam Detection: An overview," in Proceedings of the 3rd International Conference on Networking, Information Systems & Security, 2020, pp. 1-7.
[27] I. Sofi, A. Mahajan, and V. Mansotra, "Machine learning techniques used for the detection and analysis of modern types of ddos attacks," learning, vol. 4, no. 06, 2017.
[28] A. Tripathy, A. Agrawal, and S. K. Rath, "Classification of sentiment reviews using n-gram machine learning approach," Expert Systems with Applications, vol. 57, pp. 117-126, 2016.
[29] J. Tang, C. Deng, and G.-B. Huang, "Extreme learning machine for multilayer perceptron," IEEE transactions on neural networks and learning systems, vol. 27, no. 4, pp. 809-821, 2016.
[30] S .R. Salkuti, "A survey of big data and machine learning," International Journal of Electrical & Computer Engineering (2088-8708), vol. 10, no. 1, 2020.

Power System Technology
ISSN:1000-3673

Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

[31] P. P. Shinde and S. Shah, "A review of machine learning and deep learning applications," in 2018 Fourth international conference on computing communication control and automation (ICCUBEA), 2018, pp. 1-6: IEEE.
[32] V. Nasteski, "An overview of the supervised machine learning methods," Horizons. b, vol. 4, pp. 51-62, 2017.
[33] M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, and A. J. Aljaaf, "A systematic review on supervised and unsupervised machine learning algorithms for data science," Supervised and unsupervised learning for data science, pp. 3-21, 2020.
[34] S. Hosseini, A. E. Nezhad, and H. Seilani, "Botnet detection using negative selection algorithm, convolution neural network and classification methods," Evolving Systems, vol. 13, no. 1, pp. 101-115, 2022.
[35] !!!INVALID CITATION !!! {}.
[36] M. M. Salim, S. K. Singh, and J. H. Park, "Securing Smart Cities using LSTM algorithm and lightweight containers against botnet attacks," Applied Soft Computing, vol. 113, p. 107859, 2021.
[37] S. I. Popoola, R. Ande, K. B. Fatai, and B. Adebisi, "Deep bidirectional gated recurrent unit for botnet detection in smart homes," in Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics: Springer, 2021, pp. 29-55.
[38] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the internet of things using deep learning approaches," in 2018 International Joint Conference on Neural Networks (IJCNN), 2018, pp. 1-8: IEEE.
[39] H. Alkahtani and T. H. Aldhyani, "Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications," Security and Communication Networks, vol. 2021, 2021.
[40] G. Hu, K. Wang, and L. Liu, "Underwater Acoustic Target Recognition Based on Depthwise Separable Convolution Neural Networks," Sensors, vol. 21, no. 4, p. 1429, 2021.
[41] K. Shaheed et al., "DS-CNN: A pre-trained Xception model based on depth-wise separable convolutional neural network for finger vein recognition," Expert Systems with Applications, vol. 191, p. 116288, 2022.
[42] K. Shaheed, A. Mao, I. Qureshi, Q. Abbas, M. Kumar, and X. Zhang, "Finger-vein presentation attack detection using depthwise separable convolution neural network," Expert Systems with Applications, vol. 198, p. 116786, 2022.
[43] S. I. Prottasha and S. M. S. Reza, "A classification model based on depthwise separable convolutional neural network to identify rice plant diseases," International Journal of Electrical & Computer Engineering (2088-8708), vol. 12, no. 4, 2022.
[44] T. Zhang and X. Zhang, "High-speed ship detection in SAR images based on a grid convolutional neural network," Remote Sensing, vol. 11, no. 10, p. 1206, 2019.
[45] P. Dhar, V. K. Garg, and M. A. Rahman, "Enhanced Feature Extraction-based CNN Approach for Epileptic Seizure Detection from EEG Signals," Journal of Healthcare Engineering, vol. 2022, 2022.
[46] J. A. Nasir, O. S. Khan, and I. Varlamis, "Fake news detection: A hybrid CNN-RNN based deep learning approach," International Journal of Information Management Data Insights, vol. 1, no. 1, p. 100007, 2021.

Power System Technology
ISSN:1000-3673

Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

[47] Y. Li, Z. Hao, and H. Lei, "Survey of convolutional neural network," Journal of Computer Applications, vol. 36, no. 9, pp. 2508-2515, 2016.
[48] A. Kirchner and C. S. Signorino, "Using Support Vector Machines for Survey Research," Survey Practice, vol. 11, no. 1, p. 2715, 2018.
[49] A. Rezaei, "Using ensemble learning technique for detecting botnet on IoT," SN Computer Science, vol. 2, no. 3, pp. 1-14, 2021.
[50] T.-J. Liu, T.-S. Lin, and C.-W. Chen, "An Ensemble Machine Learning Botnet Detection Framework Based on Noise Filtering," Journal of Internet Technology, vol. 22 ,no. 6, pp. 1347-1357, 2021.
[51] A. Bijalwan, N. Chand, E. S. Pilli, and C. R. Krishna, "Botnet analysis using ensemble classifier," Perspectives in Science, vol. 8, pp. 502-504, 2016.
[52] H. M. Gomes, J. P. Barddal, F. Enembreck, and A. Bifet, "A survey on ensemble learning for data stream classification," ACM Computing Surveys (CSUR), vol. 50, no. 2, p. 23, 2017.
[53] U. Z. A. Hamid, H. Zamzuri, and D. K. Limbu, "Internet of vehicle (IoV) applications in expediting the implementation of smart highway of autonomous vehicle: A survey," in Performability in Internet of Things: Springer, 2019, pp. 137-157.
[54] S. Enshaeifar et al., "The internet of things for dementia care," IEEE Internet Computing, vol. 22, no. 1, pp. 8-17, 2018.
[55] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," Computer Networks, 2018.
[56] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," IEEE Wireless Communications, vol. 26, no. 5, pp. 92-98, 2019.
[57] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," IEEE Access, vol. 9, pp. 1039 ,103926-06 .2021
[58] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. ,2383-2351 .2021
[59] W. Tian, M. Du, X. Ji, G. Liu, Y. Dai, and Z. Han, "Honeypot detection strategy against advanced persistent threats in industrial internet of things: a prospect theoretic game," IEEE Internet of Things Journal, vol. 8, no. 24, pp. 17.2021 ,17381-372
[60] W. Tian, M. Du, X. Ji, G. Liu, Y. Dai, and Z. Han, "Contract-based incentive mechanisms for honeypot defense in advanced metering infrastructure," IEEE Transactions on Smart Grid, vol. 12, no. 5, pp. 4259-4268, 2021.
[61] K. Ramakrishnan, P. Gokul, and R. Nigam, "Pandora: An IOT based Intrusion Detection Honeypot with Real-time Monitoring," in 2021 International Conference on Forensics, Analytics, Big Data, Security (FABS), 2021, vol. 1, pp. 1-7: IEEE.
[62] M. Başer, E. Y. Güven, and M. A. Aydın, "SSH and Telnet Protocols Attack Analysis Using Honeypot Technique:* Analysis of SSH AND TELNET Honeypot," in 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021, pp. 806-811: IEEE.

Power System Technology
ISSN:1000-3673
Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

[63] A. Z. Tabari, X. Ou, and A. Singhal, "What are Attackers after on IoT Devices? An approach based on a multi-phased multi-faceted IoT honeypot ecosystem and data clustering," arXiv preprint arXiv:2112.10974, 2021.
[64] T. Ovasapyan, V. Nikulkin, and D. Moskvin, "Applying Honeypot Technology with Adaptive Behavior to Internet-of-Things Networks," Automatic Control and Computer Sciences, vol. 55, no. 8, pp. 1104-1110, 2021.
[65] S. Touch and J.-N. Colin, "A Comparison of an Adaptive Self-Guarded Honeypot with Conventional Honeypots," Applied Sciences, vol. 12, no. 10, p. 5224, 2022.
[66] S. Kandanaarachchi, H. Ochiai, and A. Rao, "Honeyboost: Boosting honeypot performance with data fusion and anomaly detection," Expert Systems with Applications, vol. 201, p. 117073, 2022.
[67] J. G. Surber and M. Zantua, "Intelligent Interaction Honeypots for Threat Hunting within the Internet of Things," in Journal of The Colloquium for Information Systems Security Education, 2022, vol. 9, no. 1, pp. 5-5.
[68] A. Matta, G. Sucharitha, B. Greeshmanjali, M. P. Kumar, and M. N. S. Kumar, "Honeypot: A Trap for Attackers," The New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm, pp. 91-101, 2022.
[69] A. Alharbi, W. Alosaimi, H. Alyami, H. T. Rauf, and R. Damaševičius, "Botnet attack detection using local global best bat algorithm for industrial internet of things," Electronics, vol. 10, no. 11, p. 1341, 2021.
[70] M. Wazzan, D. Algazzawi, A. Albeshri, S. Hasan, O. Rabie, and M. Asghar, "Cross Deep Learning Method for Effectively Detecting the Propagation of IoT Botnet," Sensors, vol. 22, no. 10, p. 3895, 2022.
[71] M. Banerjee, "Detection and behavioral analysis of botnets using honeynets and classification techniques," Distributed Denial of Service Attacks: Concepts, Mathematical and Cryptographic Solutions, vol. 6, p. 131, 2021.
[72] X. Hoang and Q. Nguyen, "Botnet detection based on machine learning techniques using DNS query data," Future Internet, vol. 10, no. 5, p. 43, 2018.
[73] J. van Roosmalen, H. Vranken ,and M. van Eekelen, "Applying deep learning on packet flows for botnet detection," in Proceedings of the 33rd Annual ACM Symposium on Applied Computing, 2018, pp. 1629-1636: acm.
[74] C. public, "Cisco Annual Internet Report (2018–2023)," 2021).
[75] P. Beltrán-García, E. Aguirre-Anaya, P. J. Escamilla-Ambrosio, and R. Acosta-Bermejo, "IoT botnets," in International Congress of Telematics and Computing, 2019, pp. 247-257: Springer.
[76] H. Alzahrani, M. Abulkhair, and E. Alkayal, "A multi-class neural network model for rapid detection of IoT botnet attacks," Int. J. Adv. Comp. Sci. Appl, vol. 11, no. 7, pp. 688-696, 2020.
[77] E. Bertino and N. Islam, "Botnets and internet of things security," Computer, vol. 50, no. 2, pp. 76-79, 2017.
[78] S. Dange and M. Chatterjee, "IoT Botnet: the largest threat to the IoT network," in Data Communication and Networks: Springer, 2020, pp. 137-157.
[79] A. Costin and J. Zaddach, "Iot malware: Comprehensive survey, analysis framework and case studies," BlackHat USA, vol. 1, no. 1, pp. 1-9, 2018.

Power System Technology
ISSN:1000-3673

Received: 16-06-2024 Revised: 12-07-2024 Accepted: 07-08-2024

[80] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," Telecommunication systems, vol. 73, no. 1, pp. 3-25, 2020.
[81] Z. Shao, S. Yuan, and Y. Wang, "Adaptive online learning for IoT botnet detection," Information Sciences, vol. 574, pp. 84-95, 2021.
[82] J. A. Stankovic, "Research directions for the internet of things," IEEE internet of things journal, vol. 1, no. 1, pp. 3-9, 2014.
[83] S. S. S. Sugi and S. R. Ratna, "Investigation of machine learning techniques in intrusion detection system for IoT network," in 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 1164-1167: IEEE.
[84] R. Yamashita, M. Nishio, R. K. G. Do, and K .Togashi, "Convolutional neural networks: an overview and application in radiology," Insights into imaging, vol. 9, no. 4, pp. 611-629, 2018.
[85] S. Sakib, N. Ahmed, A. J. Kabir, and H. Ahmed, "An overview of convolutional neural network: its architecture and applications," 2019.
[86] I. Goodfellow, Y. Bengio, and A. Courville, Deep learning. MIT press, 2016.
[87] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, "A survey of convolutional neural networks: analysis, applications, and prospects," IEEE transactions on neural networks and learning systems, 2021.
[88] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa, and M. Driss, "An efficient approach based on privacy-preserving deep learning for satellite image classification," Remote Sensing, vol. 13, no. 11, p. 2221, 2021.
[89] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. :1024-1019 IEEE.
[90] V. A. Memos and K. E. Psannis, "AI-Powered Honeypots for Enhanced IoT Botnet Detection," in 2020 3rd World Symposium on Communication Engineering (WSCE), 2020, pp. 64-68: IEEE.
[91] J. Kim, M. Shim, S. Hong, Y. Shin, and E. Choi, "Intelligent detection of iot botnets using machine learning and deep learning," Applied Sciences, vol. 10, no. 19, p. 7009, 2020.
[92] V. G. da Costa, S. Barbon, R. S. Miani, J. J. Rodrigues, and B. B. Zarpelão, "Detecting mobile botnets through machine learning and system calls analysis," in 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1-6: IEEE.
[93] C. Zhang and Y. Ma, Ensemble machine learning: methods and applications. Springer, 2012.