INTERNATIONAL JOURNAL OF CURRENT ADVANCED RESEARCH
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 13; Issue 12; December 2024; Page No.3383-3390
DOI: http://dx.doi.org/10.24327/ijcar.2024.3390.1720

Research Article

HYBRID MACHINE LEARNING MODEL FOR EFFICIENT BOTNET ATTACK DETECTION IN IOT ENVIRONMENT

Munimanda Premchander[1], B.Bhanu Rekha[2], A.Akshaya[3]and D.Manisha[4]
Assistant Professor [1] and UG Student [2,3,4]
Department of it, Malla Reddy Engineering College for Women (UGC-Autonomous),
Maisammguda, Hyderabad, Telangana-500100

ARTICLE INFO

Article History:

Received 18th October, 2024
Received in revised form 8th November, 2024
Accepted 20th November, 2024
Published online 28th December, 2024

Key words:

Botnet attack detection, stacking, cyber-attacks,stacked ensemble, deep learning, IoT.

ABSTRACT

Cyber attacks are growing with the rapid development and wide use of internet technology. Botnet attack emerged as one of the most harmful attacks. Botnet identification is becoming challenging due to the numerous attack vectors and the ongoing evolution of viruses. As the Internet of Things (IoT) technology is developing rapidly, many network devices have been subject to botnet attacks leading to substantial losses in different sectors. Botnets pose serious risks to network security and deep learning models have shown potential for efficiently identifying botnet activity from network traffic data. In this research, a botnet identification system is proposed based on the stacking of artificial neural network (ANN), convolutional neural network (CNN), Machine Learning Models, and recurrent neural network (RNN) (ACLR). The experiments are conducted by employing both the individual models, as well as, the proposed ACLR model for performance comparison. The UNSW-NB15 dataset is used for botnet attacks and contains nine different attack types including 'Normal', 'Generic', 'Exploits', 'Fuzzers', 'DoS', 'Reconnaissance', 'Analysis', 'Backdoor', 'Shell code' and 'Worms'. Experimental results indicate the proposed ACLR model gains 0.9698 testing accuracy showing that it is successful in capturing the intricate patterns and characteristics of botnet attacks. The proposed ACLR model's k values (3, 5, 7, and 10) for a K-fold cross-validation accuracy score is 0.9749 indicating that the model's robustness and generalizability are demonstrated by k = 5. In addition, the proposed model detects botnets with a high receiver operating characteristic area under the curve (ROC-AUC) of 0.9934 and a precision-recall area under the curve (PR-AUC) of 0.9950. Performance comparison with existing state-of-the-art models further corroborates the superior performance of the proposed approach. The results of this research can be helpful against evolving threats and enhance cyber security procedures

INTRODUCTION

The rise of Internet technology led to its rapid and wide adoption by the masses for daily, social, cultural, and institutional activities. Similar to other technologies, the internet also has negative uses where people are targeted to steal their money or personal information. Botnet attack The associate editor coordinating the review of this manuscript and approving it for publication was Ali Kashif Bashir . detection is a crucial component of cyber security, largely because it aids in preventing and reducing a variety of online security risks. Security experts can protect networks and data from harmful activities, such as distributed denial of service (DDoS) assaults, data breaches, and malware distribution, by identifying and destroying botnets. Early identification not only minimizes possible damage but also preserves network effectiveness and user confidence in digital services. Additionally, it promotes cyber resilience, guarantees adherence to legal and regulatory standards, and supports innovation in the continuous struggle against globally advancing cyber threats. Deep learning-based botnet detection uses powerful machine learning models to quickly find and categorize harmful botnet activity in the network data. Quickly identifying and counteracting the cyber dangers posed by botnets, aids organizations in protecting their systems and data. Such attacks have happened on both individuals and groups in a variety of ways to obtain financial advantage. One of the most well-known forms of assault is

*Corresponding author: **Munimanda Premchander**

Department of it, Malla Reddy Engineering College for Women (UGC-Autonomous), Maisammguda, Hyderabad, Telangana-500100

ransomware, which targets a person and locks their data until they pay the ransom demanded by the attacker. The attackers utilize botnets to assault huge organizations. Due to its success in fending off the growing menace of botnets, botnet detection employing deep learning algorithms has attracted a lot of interest recently. Network traffic analyzers based on deep learning have become an effective tool for spotting and reducing botnet activity. These analyzers use deep learning models to automatically extract pertinent information from unprocessed packet data. The first few packets in a flow's headers are specifically extracted and examined to look for patterns and traits typical of botnet traffic. Using convolutional neural network (CNN) and autoencoder, it is possible to identify malicious botnet traffic independent of the architecture of the underlying botnet [1]. Autoencoders are used to teach the network how to rebuild its input to learn the fundamental form of network traffic data. This method aids in spotting peculiar patterns that point to botnet activity. By identifying spatial connections and hierarchical representations, CNNs on the other hand excel in the analysis of structured data, such as network traffic. Researchers and practitioners in the field of botnet detection have made tremendous progress in identifying and reducing botnet risks because of the strength of deep learning algorithms. These techniques have produced encouraging results in precisely classifying and identifying botnet traffic, allowing for proactive defenses against botnet attacks [2]. Botnet identification using deep learning algorithms has proven to be a promising method for lessening the threat of botnets. It has been suggested that deep learning-based network traffic analyzers can successfully detect and counteract botnet activity. Bidirectional long-short-term memory recurrent neural networks (BLSTM-RNN) are a famous example of how deep learning is being used in botnet identification. BLSTM-RNN models are well suited for analyzing network traffic and spotting trends connected to botnet activity because they are excellent at collecting both the past and future context of sequential data [3]. There are various benefits to using deep learning algorithms for botnet identification. First of all, these algorithms are capable of learning and adapting automatically to the changing characteristics of botnets, allowing them to recognize novel and previously unknown botnet behaviors. Second, these algorithms can find hidden patterns and anomalies that would not be noticeable using conventional detection techniques by extracting characteristics from raw data packets. Deep learning models can also handle enormous amounts of network traffic data quickly, making it possible to detect botnet activity in real-time or almost real-time. The security and integrity of networks and devices depend on the ability to detect botnet activity. Because they can be used for spam distribution, distributed denial of services (DDoS) attacks, and theft of data, botnets offer a serious threat. By utilizing deep learning algorithms in botnet detection, researchers and practitioners expect to increase the accuracy and efficacy of detection approaches and enable proactive protection strategies against botnet attacks [4]. The topic of botnet identification is facing additional difficulties as a result of the proliferation of Internet of Things (IoT) devices. The possible presence of a few devices becoming infected by botnet viruses can have disastrous effects because there are billions of connected devices worldwide. The size and diversity of IoT networks present challenges for traditional botnet detection methods, underscoring the necessity for cutting-edge solutions. Deep learning techniques for botnet identification have become more popular in this field. The challenge of botnet detection in IoT networks is to efficiently detect and reduce the presence of botnets. This problem is solved by deep learning algorithms, which automatically extract relevant features from unprocessed packets [5]. To properly detect new botnet behaviors, however, the detection models must be capable to adapt and update in the present as botnets continue to develop and adopt complex evasion strategies. Real-time or nearly real-time detection of botnet activity is made possible by deep learning algorithms' capacity to handle massive volumes of network traffic data effectively. Scalable deep learning architectures that can manage the high-dimensional and dynamic nature of IoT traffic data are difficult to develop and put into practice. The generalization of detection models across various botnet topologies and variants is the focus of the problem statement. To ensure robustness and adaptability in the face of changing botnet threats, deep learning algorithms must be able to learn and detect botnet activities regardless of the underlying network structure [6]. Deep learning techniques for botnet identification have several benefits. They offer automatic and perceptive systems to deal with the diversifying and increasingly sophisticated dangers posed by botnets. These methods have the potential to accurately detect both well-known and newlydiscovered botnet activity by utilizing deep neural networks. Additionally, the ability to extract features from packet headers enables effective analysis of network data, making it possible to detect botnet behaviors in real-time [7]. However, there are still issues with the creation and application of these suggested alternatives. Deep learning techniques are currently being modified to handle encrypted traffic and changing botnet structures. Further research is needed in the areas of generalizability of detection models across various network settings and handling the dynamic nature of botnet behaviors [8]. In this regard, this research proposes a stacked model and makes the following primary contributions: • This research proposes a stacking model ACLR for botnet attack identification to improve security measures for IoT systems. The proposed model utilizes the strengths of artificial neural network (ANN), convolutional neural network (CNN), long short-term memory (LSTM), and recurrent neural network (RNN). • Experiments involve the classification of several attack types, including common ones like normal and generic as well as worms, backdoors, shell code, fuzzers, DoS, reconnaissance, and analysis. For experiments, the dataset is preprocessed involving the removal of null values and label encoding for categorical values necessary for training machine learning models. • The efficacy of the proposed approach is meticulously assessed through a comprehensive set of widely recognized performance evaluation metrics, encompassing accuracy, precision, recall, and the F1 score. In order to add further resilience to the results, the performance is thoroughly verified using k-fold cross-validation, with k values of 3,5, 7, and 10. Moreover, to evaluate the discriminative power of the model, the receiver operating characteristic area under the curve (ROC-AUC) metric is also utilized. In addition, performance comparison with state-of-the-art models is also carried out.

LITERATURE REVIEW

1. N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," Future Gener. Comput. Syst., vol. 100, pp. 779–796, Nov. 2019

Intrusion detection systems (IDSs) that continuously monitor data flow and take swift action when attacks are identified safeguard networks. Conventional IDS exhibit limitations, such as reduced detection rates and increased computational complexity, attributed to the redundancy and substantial correlation of network data. Ensemble learning (EL) is effective for detecting network attacks. Nonetheless, network traffic data and memory space requirements are typically significant. Therefore, deploying the EL approach on Internet-of-Things (IoT) devices with limited memory is challenging. In this paper, we use feature importance (FI), a filter-based feature selection technique for feature dimensionality reduction, to reduce the feature dimensions of an IoT/IIoT network traffic dataset. We also employ lightweight stacking ensemble learning (SEL) to appropriately identify network traffic records and analyse the reduced features after applying FI to the dataset. Extensive experiments use the Edge-IIoTset dataset containing IoT and IIoT network records. We show that FI reduces the storage space needed to store comprehensive network traffic data by 86.9%, leading to a significant decrease in training and testing time. Regarding accuracy, precision, recall, training and test time, our classifier that utilised the eight best dataset features recorded 87.37%, 90.65%, 77.73%, 80.88%, 16.18 s and 0.10 s for its overall performance. Despite the reduced features, our proposed SEL classifier shows insignificant accuracy compromise. Finally, we pioneered the explanation of SEL by using a decision tree to analyse its performance gain against single learners. The continual growth of the Internet of Things (IoT) industry globally can be primarily attributed to the rising number of Internet-connected devices. Technology such as processors, sensors, and communication devices gather, communicate, and act on information about their environs. However, the expansion and adoption of IoT have highlighted security concerns, notably with the protection of data and linked devices in IoT environments. Concerns about security in the IoT have inspired the development of some security solutions. The solutions encompass various tactics that preserve confidentiality, integrity, and data authentication and control IoT network access, privacy, and user-device trust (Santos et al., 2018).

2. O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2019, pp. 1–6.

Adversarial attacks have been widely studied in the field of computer vision but their impact on network security applications remains an area of open research. As IoT, 5G and AI continue to converge to realize the promise of the fourth industrial revolution (Industry 4.0), security incidents and events on IoT networks have increased. Deep learning techniques are being applied to detect and mitigate many of such security threats against IoT networks. Feedforward Neural Networks (FNN) have been widely used for classifying intrusion attacks in IoT networks. In this paper, we consider a variant of the FNN known as the Self-normalizing Neural Network (SNN) and compare its performance with the FNN for classifying intrusion attacks in an IoT network. Our analysis is performed using the BoT-IoT dataset from the Cyber Range Lab of the center of UNSW Canberra Cyber. In our experimental results, the FNN outperforms the SNN for intrusion detection in IoT networks based on multiple performance metrics such as accuracy, precision, and recall as well as multi-classification metrics such as Cohen Cappas score. However, when tested for adversarial robustness, the SNN demonstrates better resilience against the adversarial samples from the IoT dataset, presenting a promising future in the quest for safer and more secure deep learning in IoT networks. As the Internet of Things (IoT) emerges and expands over the next several years, the security risks in IoT will increase. There will be bigger rewards for successful IoT breaches and hence greater incentive and motivation for attackers to find new and novel ways to compromise IoT systems. Traditional methods and techniques for protecting against cyber threats in the traditional internet will prove inadequate in protecting against the unique security vulnerabilities that would be expected in the internet of things [1]. Hence security researchers and professionals would need to evaluate existing processes and improve upon them to create more efficient security solutions to address the security vulnerabilities in the emerging Internet of Things. Managing security challenges in any network involves three broad strategies namely prevention, detection and mitigation. Successful security solutions for IoT networks will need to adopt all three measures. For the scope of this paper, we focus on Intrusion Detection Systems (IDS) and consider deep learning based IDS for detecting and classifying network traffic within an IoT enviroment. Deep learning based IDS have an advantage over conventional anomaly based IDS because they help overcome the challenge of proper feature selections [2]. However, two major challenges of deep learning in security applications are the lack of transparency of the deep learning models [3], and the vulnerability of the deep learning models to adversarial attacks [4]. For the scope of this study, we focus on adversarial vulnerability of the deep learning models. An adversarial attack occurs when an adversarial example is fed as an input to a machine learning model.

3. M. Shahhosseini, H. Mashayekhi, and M. Rezvani, "A deep learning approach for botnet detection using raw network traffic data," J. Netw. Syst. Manage., vol. 30, no. 3, p. 44, Jul. 2022.

Nowadays, hackers take illegal advantage of distributed resources in a network of computing devices (i.e., botnet) to launch cyberattacks against the Internet of Things (IoT). Recently, diverse Machine Learning (ML) and Deep Learning (DL) methods were proposed to detect botnet attacks in IoT networks. However, highly imbalanced network traffic data in the training set often degrade the classification performance of state-of-the-art ML and DL models, especially in classes with relatively few samples. In this paper, we propose an efficient DL-based botnet attack detection algorithm that can handle highly imbalanced network traffic data. Specifically, Synthetic Minority Oversampling Technique (SMOTE) generates additional minority samples to achieve class balance, while Deep Recurrent Neural Network (DRNN) learns hierarchical

feature representations from the balanced network traffic data to perform discriminative classification. We develop DRNN and SMOTE-DRNN models with the Bot-IoT dataset, and the simulation results show that high-class imbalance in the training data adversely affects the precision, recall, F1 score, area under the receiver operating characteristic curve (AUC), geometric mean (GM) and Matthews correlation coefficient (MCC) of the DRNN model. On the other hand, the SMOTE-DRNN model achieved better classification performance with 99.50%99.50% precision, 99.75%99.75% recall, 99.62%99.62% F1 score, 99.87%99.87% AUC, 99.74%99.74% GM and 99.62%99.62% MCC. Additionally, the SMOTE-DRNN model outperformed state-of-the-art ML and DL models. The Internet-of-Things (IoT) paradigm enables physical objects to interconnect and communicate with each other via the Internet [**1**]. The popularity of IoT is fast-growing, and its adoption cuts across different areas of application such as energy, water, transport, defense, health, agriculture, etc. According to Cisco's Annual Internet Report, 14.714.7 billion IoT devices will be connected to the Internet by 2023 [**2**].

4. S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, "BoTShark: A deep learning approach for botnet traffic detection," in Cyber Threat Intelligence, 2018, pp. 137–153

Cybersecurity is seriously threatened by Botnets, which are controlled networks of compromised computers. The evolving techniques used by botnet operators make it difficult for traditional methods of botnet identification to stay up. Machine learning has become increasingly effective in recent years as a means of identifying and reducing these hazards. The CTU-13 dataset, a frequently used dataset in the field of cybersecurity, is used in this study to offer a machine learning-based method for botnet detection. The suggested methodology makes use of the CTU-13, which is made up of actual network traffic data that was recorded in a network environment that had been attacked by a botnet. The dataset is used to train a variety of machine learning algorithms to categorize network traffic as botnet-related/benign, including decision tree, regression model, naïve Bayes, and neural network model. We employ a number of criteria, such as accuracy, precision, and sensitivity, to measure how well each model performs in categorizing both known and unidentified botnet traffic patterns. Results from experiments show how well the machine learning based approach detects botnet with accuracy. It is potential for use in actual world is demonstrated by the suggested system's high detection rates and low false positive rates. An ever-changing threat scenario is accompanied by an increasing complexity in internet architecture. Hackers seek to discover ways to take advantage of weaknesses that may occur in a range of contexts, including devices, data, applications, people, and places. Botnets are a serious concern. There are three components of a botnet: the botmaster, the infected machine, and the administrative server (C and C server). It takes two steps for a botnet to communicate: first, a botmaster sends instructions to the botnet via remote link or directly to the bots. As a result of this, the controlled bots are able to carry out malicious actions after receiving malicious commands [1]. The threat of botnets compromising the fundamental principles of confidentiality, integrity, and availability is becoming increasingly clear as botnets pose an increasing threat to network security. It is especially important to note that distributed denial of service (DDoS) attacks can be launched using botnets that have a negative impact on the availability and performance of a network [2]. In general, botnet detection is done from two different angles: host-based and network-based. An abnormal use of computation resources can be identifies using the first technique. As an example, it monitors abnormally high central processing unit (CPU) usage and memory consumption. An analysis of the bot's network and traffic conditions would be carried out using the later technique [3]. It is advantage is that it can be applied even when communication is encrypted. In contrast, this method is more time-consuming and requires continuous monitoring of all host's resource utilization. The two types of network-based techniques are signature based and anomaly based. An approach based on signature is used to apply deep packet inspection (DPI) to internet protocol (IP) packets. Low false positive rates are a benefit of it. Identifying known botnets is its primary use [4]. The drawback is in concern to identify new patterns of attacks; signatures must regularly be updated. In addition, encryption techniques can conceal the signatures. Anomaly-based techniques can be used to find anomalies based on variables like packet payload size and bot activity. It is more challenging to identify botnet attacks as time goes on due to the frequent changes in botnet behavior [5], [6]. Due to their abilities to detect anomalous traffic patterns, machine learning techniques have become increasingly popular in anomaly-based methods. However, anomaly-based detection generally caused many detection errors due to high false positive rate. Additionally, one significant drawback of traditional machine learning methods is that they demand a lot of work and depend on a time-consuming feature engineering procedure.

5. M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," in Proc. IEEE 24th Pacific Rim Int. Symp. Dependable Comput. (PRDC), Dec. 2019, p. 256.

Internet of Things (IoT) as a paradigm comes with a range of benefits to humanity. Domains of research for the IoT range from healthcare automation to energy and transport. However, due to their limited resources, IoT devices are vulnerable to various types of cyber attacks as carried out by the adversary. In this paper, we propose a novel intrusion detection approach for the IoT, through the adoption of a customised deep learning technique. We utilise a cutting-edge IoT dataset comprising IoT traces and realistic attack traffic, including denial of service, distributed denial of service, data gathering and data theft attacks. A feed-forward neural networks model with embedding layers (to encode high-dimensional categorical features) for multi-class classification, is developed. The concept of transfer learning is subsequently applied to encode high-dimensional categorical features to build a binary classifier based on a second feed-forward neural networks model. We obtain results through the evaluation of the proposed approach which demonstrate a high classification accuracy for both classifiers, namely, binary and multi-class. Internet of Things (IoT) devices are rapidly being adopted in households and businesses alike [1,2]. Recent statistics for IoT device deployment in various domains include; smart cities (28.6%), industrial IoT (26.4%), eHealth (22%), smart homes (15.4%) and smart vehicles (7.7%) [3]. Device usage stats reveal a staggering jump from

15.4B in 2015 to 26.7B in 2019. A common factor for such growth is the ready availability, affordability and convenience in our daily lives, as facilitated by IoT devices. Whilst on one end consumers have benefited from these devices, on the other, critical infrastructures have also been actively deploying IoT devices to help carry out their tasks. A smart electricity meter for instance carries out its functionality of monitoring and reporting consumer energy usage patterns whilst also interacting with household IoT devices such as smart TVs and refrigerators. Advances in IoT technologies have demonstrated various benefits to users. However, IoT devices do come with their host of vulnerabilities that expose these to the omnipotent and ever-evolving cyber threat landscape [4]. The complexities appertaining to the diverse range of IoT protocols in deployment, encumber the process of providing a fool proof and common cybersecurity solution for the IoT. For instance, the MQTT protocol is a commonly deployed application protocol in the IoT, which is lightweight in nature [5]. The protocol facilitates a publish–subscribe approach towards inter-device communication. Communication between an IoT device and a central server takes place through dedicated devices called message brokers. The protocol itself suffers from several vulnerabilities that expose the IoT devices and the system at large to the ever-evolving adversarial threat. Common examples of these include device compromise, data theft, node theft, denial of service, and Man-in-The-Middle (MiTM) attacks [6]. Traditionally, intrusion detection systems were designed to identify malicious attempts by the adversary to penetrate the network and cause harm. Several techniques for intelligent classification of network traffic exist in the literature. Some of these include principal component analysis [7], genetic algorithms [8], Bayesian networks [9], and support vector machines (SVM) [10]. To our knowledge, intrusion detection systems for the IoT through the concept of deep learning, have not yet been thoroughly explored and reported in the literature. In this work, we propose a novel design of an intrusion detection system, based on deep learning-based network traffic classification. The multi-class classifier comprises a feed-forward neural networks model with embedding layers to identify four categories of attacks, namely denial of service (DoS), distributed denial of service (DDoS), data gathering, and data theft, while differentiating traffic of these attack types from routine network traffic. In addition, the encoding of high-dimensional categorical features is extracted through the concept of network embedding and subsequently applied to a binary classifier via a transfer learning-based approach. A preliminary version of this paper can be found in

EXISTING SYSTEM

- To recognize and reduce one of the biggest hazards to systems connected to the internet, cyber security is a crucial duty. Botnets are collections of hacked computers that are coordinated by a master host and used for malicious purposes like spam distribution, DDoS, and data theft. Traditional botnet detection techniques, like anomaly-based identification and signature-based approaches, have trouble identifying unknown botnets, encrypted traffic, and complex evasion strategies used by attackers. Deep learning methods, however, present a more promising strategy for overcoming these difficulties. The authors [10] were the first to employ machine learning for botnet traffic detection. They utilized a CNN model in that regard. Experimental results showthat the accuracy of the training set is 98.62%, the loss is 4.74% and training takes an average of 32 seconds for each epoch. Accuracy is 99.57%, loss is 1.74% and test duration is 10 seconds per epoch for the test set.

- The largest and most destructive internet cybercrimes have involved DDoS attacks. The Mirai botnet was one of the most well-known instances of a DDoS assault using the IoT. A DDoS attack is a kind of cyber-attack in which a hacker temporarily subjugates several compromised systems to attack a particular target and sends concurrent requests to a server for a specific service, overwhelming the server and convincing it to disregard real requests from end users. To create and disseminate a network of robots (botnets) made up of the afflicted IoT devices (bots), Mirai is a piece of malware that infects IoT devices. The attacker (the ‘‘botmaster’’) then instructs the bots to take part in DDoS attacks on Internet targets using a command and control (C&C) server. The research [11] presented a bidirectional LSTM (BLSTM-RNN) approach for botnet attack detection. To determine whether the BLSTM-RNN’s incorporation of contextual data received from the past and future may lead to higher accuracy, the model was compared against a unidirectional LSTM-RNN. With 99%, 98%, and 98% validation accuracy and 0.000809, 0.125630, and 0.116453 validation loss metrics, respectively the findings for Mirai, UDP, and DNS were highly encouraging.

- The research [12] used classifiers such as k-nearest neighbors (KNN), decision tree (DT), AdaBoost (AB), random forest (RF), linear SVM (LSVM), and radial basis functionSVM(RSVM), all of which were applied to the three different sets of DS1 data. The performances obtained by the logistic regression (LR) and Naive Bayes (NB) classifiers were significantly worse. The authors combined the CNN-LSTM model in [13] to identify DDoS attacks using the CICIDS 2017 dataset. Results show a 97.16% accuracy, 97.41% precision, and 99.1% reliability. A domain generation algorithm attack is studied in [14] and an accuracy of 94.9% is reported. Implementation of countermeasures for cyber attacks incurs large costs; so, cost reduction is an important factor in cyber security. Using only 25% of the implementation budget, the proposed model in [15] outperformed cutting-edge IoT botnet detection techniques in terms of accuracy. As a result, it cuts the implementation budget by almost 75%. The research [16] employs CNN and LSTM for botnet attack detection. In comparison to the average validation accuracy, the average training accuracy for DNNBoT1 and DNNBoT2 was 90.71% and 91.44% respectively, for each was 90.54% and 91.24%. A growing trend in recent years is deep learning potential methods for botnet detection. Cyber security is seriously threatened by botnets, which are networks of compromised hosts

used by a master host to conduct malicious operations. In order to effectively address the variety of cyber security issues, popular deep learning methods can be used, including their ensembles and hybrid methods [17].

- An all-encompassing, useful technique for learning realvalued, discrete-valued, and vector-valued functions is the ANN. The research [18] proposed an ANN model and tested it using the CTU-13 dataset. In comparison to support vector machine (SVM), and NB, the model yields better accuracy of approximately 99%. Similarly, an ANN is deployed for automatically identifying DDoS attacks in [19]. Results showed that ANN in particular showed a very good accuracy of 99% and proved to be more effective against DDoS attacks.
- Various CNN models are also utilized for botnet attack detection. A CNN-LSTM model is utilized in [20] for attack detection IoT settings, categorizing and halting network activity by severing wifi connections. CNN layers are utilized to extract features from the input data while LSTM is used for detection. The authors report good results with a specificity of 93% and an F1 score of 100%. The results demonstrate the innovative outcomes of utilizing the CNN-LSTM model in the analysis of regular packets, fuzzing assaults, and flood attacks. The weighted average findings of the author's suggested approach for identifying the botnet on the Provision PT-737E camera were as follows: 88% for camera precision, 87% for recall, and 83% for F1 score. On the Provision PT-838 camera, the system's classification results for botnet assaults and regular packets were 89% for recall, 85% for F1 score, and 94% for accuracy [21].

DISADVANTAGES

- The system doesn't implement the stacking of artificial neural network (ANN), convolutional neural network (CNN) and Machine Learning Models.
- The system doesn't implement the method to find distributed denial of services (DDoS) attacks.

PROPOSED SYSTEM

This research proposes a stacking model ACLR for botnet attack identification to improve security measures for IoT systems. The proposed model utilizes the strengths of artificial neural network (ANN), convolutional neural network (CNN), ML Models and recurrent neural network (RNN).

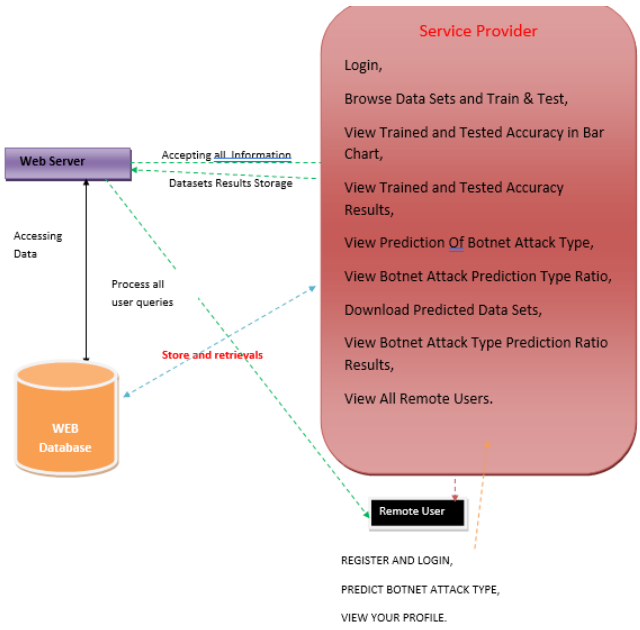
- Experiments involve the classification of several attack types, including common ones like normal and generic as well as worms, backdoors, shell code, fuzzers, DoS, reconnaissance, and analysis. For experiments, the dataset is preprocessed involving the removal of null values and label encoding for categorical values necessary for training machine learning models.
- The efficacy of the proposed approach is meticulously assessed through a comprehensive set of widely recognized performance evaluation metrics, encompassing accuracy, precision, recall, and the F1 score. In order to add further resilience to the results, the performance is thoroughly verified using k-fold cross-validation, with k values of 3,5, 7, and 10. Moreover, to evaluate the discriminative power of the model, the receiver operating characteristic area under the curve (ROC-AUC) metric is also utilized. In addition, performance comparison with state-of-the-art models is also carried out.

ADVANTAGES

- Preprocessing must be completed to make the data ready for the model training and testing. The dataset are loaded, cleaned, modified, and transformed into a form that is appropriate for machine learning models.
- An advanced form of an ANN is CNN, which was created to be particularly effective at processing and analyzing visual data, such as pictures and movies. CNNs are very good at extracting significant patterns and characteristics from datasets.

IMPLEMENTATION

SYSTEM ARCHITECTURE



MODULES

SERVICE PROVIDER

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Browse Data Sets and Train & Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Botnet Attack Type, View Botnet Attack Prediction Type Ratio, Download Predicted Data Sets, View Botnet Attack Type Prediction Ratio Results, View All Remote Users.

VIEW AND AUTHORIZE USERS

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

REMOTE USER

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT BOTNET ATTACK TYPE, VIEW YOUR PROFILE.

RESULT

CONCLUSION

The frequency and intensity of cyber attacks have witnessed a growth lately and botnet attacks have emerged with the potential to cause serious damage. Deep learning-based models have shown potential for automated botnet detection; ensemble models come out as better predictors than individual models. This research proposes a hybrid stacking model, ANN+CNN+LSTM+RNN (ACLR) for botnet detection. The experimental setup involves ACLR implementation in the Google COLAB environment using the UNSW-NB15 dataset. In addition, this research employed ANN, CNN, LSTM, and RNN models for performance comparison with the proposed ACLR model. Experimental results suggest a superior performance of ACLR with a 0.9698 accuracy score while the k-fold cross-validation accuracy score is 0.9749 where the value of k is 3,5,7 and 10, respectively. In addition, increasing the number of layers for the deployed models is observed to produce better performance, however, it comes at the cost of increased computational complexity and higher training time. Among the employed models, the ANN model shows poor performance while LSTM, RNN, and CNN show better results. The comparative findings demonstrate that the proposed approach outperforms ANN, CNN, LSTM, and RNN models in terms of performance and accuracy for the detection of botnets. In comparison to previous models, the suggested ACLR model has the greatest ROC AUC (0.9934) and PR AUC (0.9950) values. Performance analysis with existing models indicates that ACLR can perform better than state-of-the-art models. It is important to note that deep learning algorithms for botnet identification still have limitations such as a lack of labeled statistics on training and the possibility of hostile attacks. To increase the precision, scalability, and robustness of deep learning-based botnet detection systems more research and development in this area are required. The stacking model in the proposed research has been based on four deep learning models which consume more time than the single model in predictions but show more efficient results than the single model. It also necessitates data interchange and synchronization. This demonstrates the significance of carefully balancing model complexity and effectiveness across a range of applications. As it will be totally automated in future research, there should be more training using reinforcement learning, which can be more effective.

References

1. N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, ‘‘Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset,’’ Future Gener. Comput. Syst., vol. 100, pp. 779–796, Nov. 2019.
2. O. Ibitoye, O. Shafiq, and A. Matrawy, ‘‘Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2019, pp. 1–6.
3. M. Shahhosseini, H. Mashayekhi, and M. Rezvani, ‘‘A deep learning approach for botnet detection using raw network traffic data,’’ J. Netw. Syst. Manage., vol. 30, no. 3, p. 44, Jul. 2022.
4. S. Homayoun, M. Ahmadzadeh, S. Hashemi, A. Dehghantanha, and R. Khayami, ‘‘BoTShark: A deep learning approach for botnet traffic detection,’’ in Cyber Threat Intelligence, 2018, pp. 137–153.
5. M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, ‘‘Deep learning-based intrusion detection for IoT networks,’’ in Proc. IEEE 24th Pacific Rim Int. Symp. Dependable Comput. (PRDC), Dec. 2019, p. 256.
6. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H.

Janicke, ‘‘Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,’’ J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102419.

7. T. Hasan, J. Malik, I. Bibi, W. U. Khan, F. N. Al-Wesabi, K. Dev, and G. Huang, ‘‘Securing industrial Internet of Things against botnet attacks using hybrid deep learning approach,’’ IEEE Trans. Netw. Sci. Eng., vol. 10, no. 5, pp. 2952–2963, Sep./Oct. 2023.
8. D. T. Son, N. T. K. Tram, and P. M. Hieu, ‘‘Deep learning techniques to detect botnet,’’ J. Sci. Technol. Inf. Secur., vol. 1, no. 15, pp. 85–91, Jun. 2022.
9. M. Gandhi and S. Srivatsa, ‘‘Detecting and preventing attacks using network intrusion detection systems,’’ Int. J. Comput. Sci. Secur., vol. 2, no. 1, pp. 49–60, 2008.
10. J. Liu, S. Liu, and S. Zhang, ‘‘Detection of IoT botnet based on deep learning,’’ in Proc. Chin. Control Conf. (CCC), 2019, pp. 8381–8385

How to cite this article:

Munimanda Premchander., B.Bhanu Rekha., A.Akshaya and D.Manisha. (2024) Hybrid machine learning model for efficient botnet attack detection in iot environment, *International Journal of Current Advanced Research*, 13(12), pp.3383-3390

****