Analysis on Deep Learning and Machine Learning Techniques to Mitigate Botnet Attacks in Robots and IoT Devices

Dr Monika G[1] Prof Dr Divya Midhun[2] Prof. (Dr.) Mohammad Israr[3]

[1]PDF, Dept of Computer science Lincoln University College, pdf.monika@lincoln.edu.my, monikagphd@gmail.com

[2]Supervisor, Lincoln University College, divya@lincoln.edu.my

[3]Co-Supervisor, Lincoln University College, president@maaun.edu.ng

Abstract The proliferation of the Internet of Things (IoT) and robotic systems has opened new avenues for automation and connectivity, but it has also introduced significant cybersecurity challenges. This research focuses on bot detection techniques for IoT and robotic environments, emphasizing the integration of advanced machine learning (ML) and deep learning (DL) methods. By analyzing network traffic data and leveraging anomaly-based detection systems, this study proposes strategies to enhance security against bot attacks in IoT and robotic systems. Datasets such as NSL-KDD, CICIDS2017, IOTID20, and ROSIDS23 were explored to understand the nature of bot attacks and evaluate the proposed detection framework. Various methodology are analysed and to narrow down the research to mitigate Botnet Attacks in Robots and IoT Devices

1. Introduction The rapid growth of IoT and robotics in applications such as smart homes, healthcare, industrial automation, and autonomous vehicles has created a highly interconnected ecosystem. However, this increased connectivity has also made these systems vulnerable to bot-based attacks, such as distributed denial-of-service (DDoS) and botnet attacks, which disrupt operations and compromise data integrity. Detecting and mitigating such attacks is crucial for ensuring system reliability and security.

This paper aims to address bot detection in IoT and robotic systems by leveraging advanced ML and DL techniques. The research highlights the limitations of traditional intrusion detection systems (IDS) and proposes novel methods for anomaly-based bot detection using publicly available datasets.

2. Background IoT and robotic systems operate on multi-layered architectures, including perception, transport, and network layers. These layers are vulnerable to various attacks, including jamming, spoofing, and flooding. Bots exploit these vulnerabilities to launch coordinated attacks, often targeting the resource-constrained nature of IoT devices and robotic middleware like the Robot Operating System (ROS).

Traditional IDS methods, such as signature-based and rule-based systems, are often ineffective against sophisticated bot attacks due to their inability to detect novel threats. Anomaly-based IDS, which identifies deviations from normal behavior, has emerged as a more promising approach, particularly when integrated with ML and DL techniques.

3. Research Question How can machine learning and deep learning techniques be effectively utilized to detect and mitigate bot attacks in IoT and robotic systems while addressing the limitations of traditional intrusion detection methods?

4. Methodology

4.1 Datasets Four datasets were analyzed to develop and evaluate the proposed bot detection framework:

- **NSL-KDD:** A benchmark dataset that addresses the limitations of the KDDCup99 dataset, focusing on DDoS, R2L, and U2R attacks. Any one of the four main categories can apply to the simulated attacks.

  1. DoS (Denial of Service): IT captured the moment when the server was overloaded with more requests than it could process. For instance Teardrop, Neptune, and Smurf attacks are examples of this.
  2. Probe: To take advantage of a known vulnerability, the hacker searches the network. Satan, ipsweep, and Nmap attacks are a few examples.
  3. R2L (remote to local) attacks: they involve the attacker delivering packets to the victim's computer in an attempt to obtain local access to unauthorized data. Eject, load module, and Perl assaults are a few examples.
  4. U2R (User to Root): the attacker uses his normal account to gain core access to the system in order to take advantage of security flaws. FTP_write, password guessing, and imap attacks are a few examples.

CICIDS2017: Contains real-world network traffic with attack types such as botnet and DDoS. This dataset serves as a standard for network traffic analysis. It was created in a simulated setting at the University of New Brunswick's Canadian Institute for Cybersecurity (CIC) [128]. It offers dependable regular and malicious network flows and has 80 network functions. Five days were spent gathering the data. The dataset's CSV files were created from pcap files using ISCXFlow meter. Based on the SSH, FTP, HTTP, and email protocols, it then retrieved the typical and anomalous behavior. In addition to the benign (normal) instances, it includes the 11 attack class instances. The four assault categories—Botnet, DoS, Firewall, and Port Scan—combine the 11 attack types.2.
The simulated attacks can be classified as either "BENIGN," "Botnet," "DoS," "Firewall," or "Port Scan."
1. Botnet: A botnet attack is a network formed by computers infected with malware. Without being aware of their owners, the attacker attempts to carry out nefarious actions. This generates DDoS attacks and can be done remotely. The computers are under the authority of the bot masters.
2. DoS: An assault known as a denial of service. Because it doesn't take a lot of bandwidth, this attack is simple to execute. Additionally, because it takes longer to finish an HTTP request, it is difficult to detect.
3. Firewall: This is an Internet-based sub-attack category rather than a major attack. Thus, the term "firewall." FTP-Patator, SSH-Patator, and infiltration (similar to Probe) make up the attack. The attacker seeks to take total control of the system and obtain remote access.
4. Port Scan: The Nmap utility does this. In order for attackers to get access to the system, this assault gathers information. The operating system, active devices, and port status are only a few of the critical details the attacker might discover about the linked devices.

Table 1: CICIDS2017 Attack samples

Attack category	Attack instances
Benign(Normal)	2036840
DoS	320260
Botnet	4065
PortScan	57440
Firewall	8588

IOTID20: Specifically designed for IoT systems, including botnet and spoofing attacks. Raw network packet files produced by the IOTID [131] dataset are used in the IOTID20 [130]. The dataset is openly accessible and was produced for scholarly purposes. Two intelligent home devices—the EZVIZ Wi-Fi camera (C2C Mini O plus 1080P) and the NUGU (NU 100) AI-based speaker—as well as several PCs and smartphones were linked via a WI-FI router to create the IoT network. Nmap tools were used to mimic attacks such as Man in the Middle, DoS, scanning, and spoofing. The following four categories apply to the simulated attacks. "Dos," "Mirai," "Scan," and "MITM ARP."

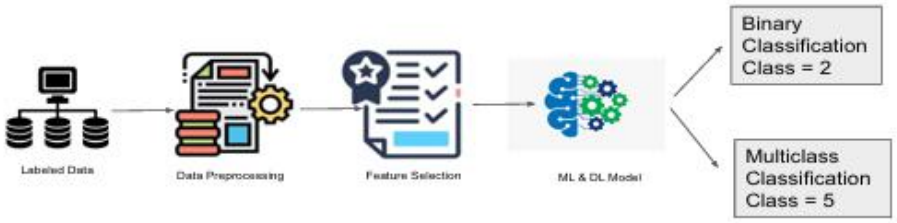
Table 2:IOTID20 Sample attacks

Attack category	Attack instances
Benign(Normal)	38598
Dos	59390
Mirai	230788
Scan	56744
MITM ARP Spoofing	25868

1. DoS: When a single source or end node experiences malicious activity, it might lead to a denial of service assault. By preventing other devices from accessing the target server, the attacker attempts to overload it.
2. Mirai: The attacker attempts to create a network of remotely controlled bots using the victim's software.
3. Scan: Throughout the procedure, the attacker attempts to alter the data. As they scan the devices, they attempt to collect

the data by hardware.
4. MITM ARP Spoofing: A common hacking technique is the man-in-the-middle attack. The attacker controls the traffic by positioned between the connections of two servers.

Fig. 1 Methodology Pipeline



ROSIDS23: Focused on ROS environments, featuring attacks like subscriber flooding and unauthorized publish. The ROSIDS23 dataset was gathered from network traffic in pcap format from autonomous operated robotic systems. The CI-CFlowMeter was used to extract traffic features from the gathered pcap data [1]. Four security threats are included in the dataset: DoS, subscriber flood, unauthorized publish, and unauthorized subscribe. The last of these assaults is a generic network security attack, whereas the first three are specialized to ROS. Details of the suggested dataset are provided in Table 3.

Table 3 ROSIDS23 Dataset details

'he details of the proposed dataset: ROSIDS23 dataset.

Dataset name:	ROSIDS23
Dataset type:	Multi-class
A total number of features:	83
Number of the classes:	5
List of the class labels:	Benign, DoS, Unauthorized Publish, Unauthorized Subscribe, Subscriber Flood

The ROSIDS23 dataset is multi-class; each row includes a label field, eighty-three characteristics, and a timestamp. Benign, DoS, unauthorized publish, unauthorized subscribe, and subscriber flood are the five possible values for the label field. There are many records in the dataset that fall into different categories. With 62,511 cases, the benign records—which indicate safe and non-malicious instances—make up the largest group among these. There are 31,0 0 0 incidents of Denial of Service (DoS) assaults and 30,064 instances of Subscriber Flood assaults. Unauthorized publish and unauthorized subscribe are two more categories that draw attention to particular security issues. Unauthorized subscription includes 5289 records and refers to situations in which unauthorized parties listen to or subscribe to a network or data exchange. However, 7817 data fall within the category of unauthorized publication, which includes situations in which material is published or distributed by unapproved parties. A comprehensive picture of the dataset's makeup is given by Fig. 2, which displays the quantity of each type of record in the dataset.

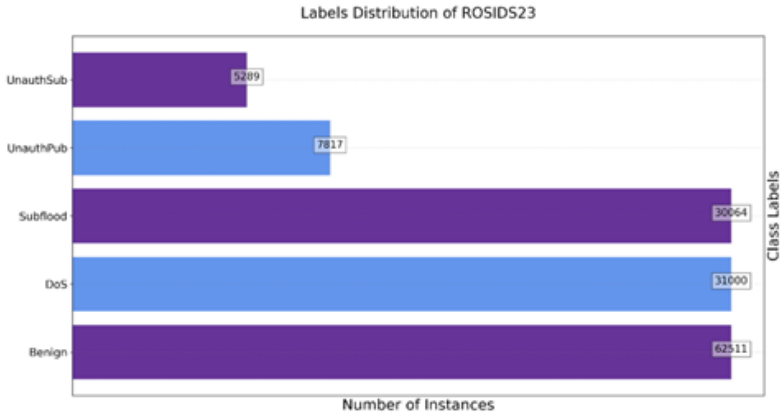


Fig 2: Graphical representation of the dataset

4.2 Detection Model

LR, or logistic regression
One statistical approach for binary classification issues is logistic regression. It uses the sigmoid function to assess the likelihood that a given input belongs to a specific class. A decision threshold, often 0.5, is used to assign a class label after the sigmoid function transfers input values to a probability range between 0 and 1. Although logistic regression is easy to understand and performs well with data that can be divided into linear segments, it has trouble with intricate, nonlinear relationships.

LDA, or linear discriminant analysis
LDA is a supervised learning algorithm that maximizes class separation by projecting data onto a lower-dimensional space. In contrast to logistic regression, LDA makes the assumption that all classes have equal covariance and a Gaussian (normal) distribution. By optimizing the ratio of inter-class variation to within-class variance, it determines the best linear boundary between several classes. LDA performs well when assumptions are met and in high-dimensional spaces, but it may not operate well when class distributions are significantly non-Gaussian.

KNN, or K-Nearest Neighbors
A new data point is classified using the majority vote of its k nearest neighbors by the non-parametric, instance-based KNN learning method. Although other metrics, such as the Manhattan or Hamming distances, can be utilized, the Euclidean distance is typically used to measure the distance between points.

Benefits: Easy to use, requires no training, and performs well with tiny datasets.
Cons: Requires adjusting the k-value for best results; computationally costly for large datasets; susceptible to noise and irrelevant features.
Trees for Regression and Classification (CART)
A decision tree method called CART is applied to jobs involving both regression and classification. By choosing the best feature and threshold value that minimizes impurity (as determined by the Gini index or entropy), it recursively divides the dataset into homogenous groups.
Benefits include handling category and numerical data, capturing non-linear relationships, and being interpretable.
Cons: Needs pruning to enhance generalization; prone to overfitting; sensitive to slight changes in data (high variance).
SVM, or support vector machine
SVM is a potent supervised learning technique that maximizes the margin between classes by identifying the ideal hyperplane for classification.
SVM determines the hyperplane with the largest margin for data that is linearly separable.
It projects non-linearly separable data into a higher-dimensional space where it becomes linearly separable using kernel functions (such as RBF, polynomial, and sigmoid kernels).
Benefits include robustness against overfitting, effectiveness even with tiny datasets, and good performance with high-dimensional data.
Cons: Needs careful adjustment of parameters like C (regularization) and kernel type; computationally costly for huge datasets.

4.4 Additional Techniques

PCC-CNN
The goal of our concept is to create a lightweight and effective IDS. Convolutional neural networks (CNNs) are the best classification model, and our model selects features using the Pearson Correlation Coefficient (PCC). One popular feature selection method is the PCC, which is a filter-based algorithm [142]. Numerous IDS have applied this feature selection technique to different dataset variations [143,144]. The computational efficiency of a filter-based technique is one of its advantages [145]. CNN is trained using the properties that PCC has identified (see fig. 3).

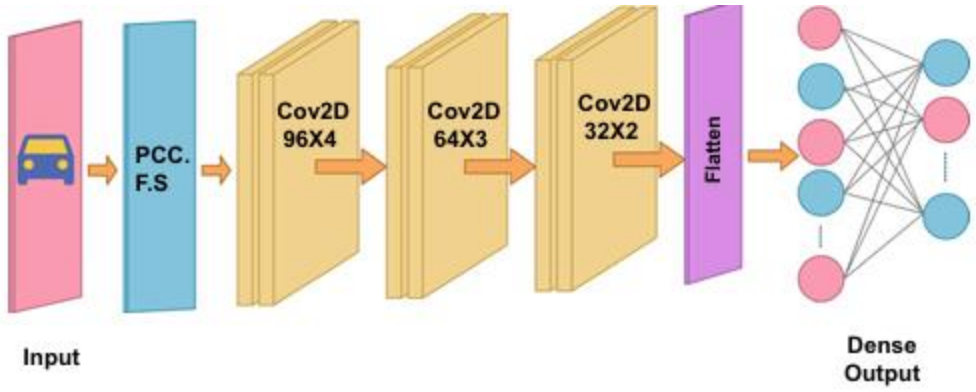


Fig3 PCC- CNN Model

The most advanced model for classification tasks is CNN. In order to identify features and apply them to classification, it applies a number of filters to the data. The input, hidden, and output layers make up CNN. Convolutional layers that apply an activation function come first in the input layer. Finally, fully connected layers carry out classification after the hidden layer's pooling layers lower the feature dimensionality by scaling down the data.
Three convolution layers, each measuring 96 times by 4, 64 times by 3, 32 times by 2, and a rectified linear unit activation function (RELU) are included in the CNN model. A linear function called RELU will output zero if the input is negative or the input directly if it is positive. The values from the previous layer are transformed into one dimension by the flattening layer. With the exception of the final one, which employs the Softmax activation function, three dense layers with 512,128,32, and 2 were applied using RELU activation. The output will be normalized in probabilistic form with the aid of Softmax. The values are viewed in non-linear form via the dense layers. The last layer's parameter values are adjusted by the adaptive moment estimation (Adam) optimizer. Whether the intended results are binary or multiclass determines whether the number class parameter is set to 2 or 5. Since the output is in categorical labels, the loss function was based on sparse categorical cross-entropy. 64 batch sizes and five epochs were used to train the model for binary and multiclass classification.

Comparison with Existing Systems: Traditional IDS models such as Signature-Based IDS and Rule-Based IDS struggle to detect unknown threats, often yielding high false positive rates. Previous ML models, such as Decision Trees and SVM, demonstrated detection accuracies between 85% and 95%, but they lacked the ability to generalize well across different datasets. The proposed PCC-CNN model, with over 99% accuracy, significantly outperforms these traditional methods in both accuracy and robustness. Furthermore, hybrid models incorporating LSTM and Autoencoders have shown improvements in sequential pattern detection, further reducing false positives.

6. Discussion The study highlights the effectiveness of deep learning-based IDS in addressing the limitations of traditional methods. The PCC-CNN model's ability to handle imbalanced datasets and extract meaningful features from high-dimensional data makes it a suitable choice for IoT and robotic systems. However, challenges such as real-time detection and scalability in large-scale deployments need further exploration.

7. Conclusion This paper presents a comprehensive framework for bot detection in IoT and robotic systems using anomaly-based IDS and advanced DL techniques. The integration of PCC and CNN proved effective in identifying bot attacks with high accuracy and low false alarm rates. Future work will focus on implementation and enhancing the model's resilience against adversarial attacks.

References

1. Kyriazis D, Varvarigou T, White D, Rossi A, Cooper J. "Sustainable smart city IoT applications: Heat and electricity management & Ecoconscious cruise control for public transportation,". IEEE 14th International Symposium on "A World of

Wireless, Mobile and Multimedia Networks" (WoWMoM). Madrid, Spain. 2013;2013:1–5. https://doi.org/10.1109/WoWMoM.2013.6583500.

2. Shanzhi Chen, et al. A vision of IoT: Applications, challenges, and opportunities with china perspective''. IEEE Int Things J. 2014;1(4):349–59.

3. Malche Timothy, Maheshwary Priti. "Internet of Things (IoT) for building smart home system." 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.

4. Fotios Zantalis, et al. A review of machine learning and IoT in smart transportation''. Future Int. 2019;11(4):94.

5. Mezghani Emna, Exposito Ernesto, Drira Khalil. A model-driven methodology for the design of autonomic and cognitive IoT-based systems: Application to healthcare. IEEE Trans Emerg Topics Comput Intel. 2017;1(3):224–34.

6. Zhao Ji-chun et al. "The study and application of the IOT technology in agriculture." 2010 3rd international conference on computer science and information technology. Vol. 2. IEEE, 2010.

7. Ou Qinghai et al. "Application of internet of things in smart grid power transmission." 2012 third FTRA international conference on mobile, ubiquitous, and intelligent computing. IEEE, 2012.

8. Bichi BY, Islam SU, Kademi AM, Ahmad I. An energy-aware application module for the fog-based internet of military things. Discov Internet Things. 2022;2(1):4.

9. Khanna A, Kaur S. Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. Wireless Pers Commun. 2020;114:1687762. https://doi. org/10.1007/s11277-020-07446-4.

10. Saba T, Saba T, et al. Real-time anomalies detection in the crowd using convolutional extended short-term memory network. J Inform Sci. 2021. https://doi.org/10.1177/01655515211022665.

11. Khanna Abhishek, Kaur Sanmeet. Internet of things (IoT), applications and challenges: a comprehensive review. Wirel Pers Commun. 2020;114:1687–762.

12. Kraijak Surapon, Tuwanut Panwit. "A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends." 11th international conference on wireless communications, networking and mobile computing (WiCOM 2015). IET,

2015.

13. Schneider S. The industrial internet of things (iiot) applications and taxonomy. Internet Things Data Anal Handb. 2017;41–81.

14. Khan WZ, et al. Industrial internet of things Recent advances enabling technologies and open challenges. Comput Electr Eng. 2020;81: 106522.

15. Li Shan, Iqbal Muddesar, Saxena Neetesh. "Future industry internet of things with zero-trust security." Information Systems Frontiers 2022;1–14.

16. Ahmad I. Discover Internet of Things editorial, inaugural issue: Welcome from Editor-in-Chief. Discov Internet Things. 2021;1:1–4.

17. Alkahtani H, Aldhyani THH, Al-Yaari M. Adaptive anomaly detection framework model objects in cyberspace. Appl Bionics Biomech.2020;6660489:14.

18. Tang M, Alazab M, Luo Y. Big data for cybersecurity: vulnerability disclosure trends and dependencies. Inst Electr Electron Eng Trans Big Data. 2019;5(3):317–29.

19. Zerihun BM, Olwal TO, Hassen MR. Design and Analysis of IoT-Based Modern Agriculture Monitoring System for Real-Time Data Collection. In: Computer Vision and Machine Learning in Agriculture, vol. 2. Singapore: Springer Singapore; 2022. p. 73–82.

20. AL-Sarawi Shadi, Anbar Mohammed, Abdullah Rosni, AI Hawari Ahmed B. Internet of things market analysis forecasts,2020-2030. Worlds4, 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability, IEEE,2020, 978-1-7281-6823-4/20