International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Survey on BotShield Dual-Stage AI System for Detection of IOT Botnet Attacks

Mrs. Manjusha Mane [1], Prof. Arti Abhishek Bhise[2]

[1] *Computer Engineering & SKN college of engineering, Pune*
[2] *Computer Engineering & SKN college of engineering, Pune*

Abstract - The Internet of Things (IoT) and the exponential growth in Internet usage have made cyber threats—especially IoT-based botnet attacks—much more sophisticated and dangerous. Firewalls and antivirus software are examples of traditional cybersecurity solutions that are no longer sufficient to address these changing threats. We examine and suggest BotShield, a dual-stage intrusion detection system (IDS) that uses machine learning to detect and stop IoT botnet activity in real time, as a solution to this problem. The first stage involves anomaly detection, which monitors network traffic for abnormal patterns that could signal early botnet activity. The second stage uses classification algorithms to accurately differentiate between benign and malicious traffic. To improve model performance, our approach uses feature selection, normalization procedures, and strong preprocessing techniques. Experimental validation on standard IoT botnet datasets demonstrates high accuracy, low false-positive rates, and real-time detection capability, making BotShield a scalable and efficient solution for modern IoT network security.

Keywords: Intrusion Detection System, NIDS, Machine learning, Convolutional Neural Network, Host-based Intrusion Detection System.

1.INTRODUCTION

In addition to offering previously unheard-of ease and efficiency, the quick growth of connected devices and IoT systems has also revealed serious cybersecurity flaws. Botnet assaults are increasingly targeting these systems, which can jeopardize service availability, confidentiality, and integrity. Because traditional security systems are static and unadaptable, they are unable to handle these attacks. In order to monitor, identify, and notify users of any threats, intrusion detection systems, or IDS, have become an essential part of protection. A variety of assaults, such as malware incursions, unauthorized access, privilege escalation, and data exfiltration, can be detected by IDS technologies. A dual-phase IDS based on machine learning techniques is presented in this study with the goal of detecting and thwarting botnet threats in Internet of Things environments. The first phase involves anomaly detection, which identifies deviations from normal behavior. Classification methods are used in the second phase to verify whether the anomalies are real attacks. By fusing the advantages of both approaches, this integrated system is intended to provide real-time monitoring, early danger detection, and increased accuracy.Facial aging significantly affects the accuracy of recognition systems, as human faces undergo subtle to pronounced transformations over time. Traditional facial recognition models often underperform when verifying identities across large age gaps, necessitating the development of synthetic aging frameworks. These systems generate age-progressed or age-regressed images while preserving identity, thus enabling more robust recognition over time.

Synthetic aging approaches harness deep learning architectures—especially GAN-based models—to simulate aging effects like wrinkles, skin sagging, or facial structure shifts. These synthetically generated images are instrumental in training models to recognize individuals across varying age spans. Beyond identity preservation, these techniques are also critical in ensuring fairness across age groups and other demographic factors.

This paper surveys the latest advancements in synthetic face aging, focusing on their role in enhancing the robustness and fairness of facial recognition systems.

2. Existing Work

The goal of is to look into these databases and show that the proposed model can correctly classify and identify malicious nodes. A deep attempting to learn paradigm for unauthorized access is presented in this article, as is a comparison of the system model's implementation across three significant network attack datasets [1]. Based on the results, the model performed best with NSL-KDD, Newcastle University, and CSE-CIC-IDS2018. NSL-KDD, UNSW-NB15 and CSE-CIC-IDS2018 model result was obtained for these variables.

A comparison is made between the anomaly-based network intrusion detection models of deep learning and machine learning, as stated in [2]. A look at the datasets used in the study was followed by a review of previous research on ML and DL IDS. In addition, performance results of ML and DL models were presented, contrasted, and debated with the help of the KDD-99 dataset. Last but not least, the authors suggest crucial areas for additional research. According to [3] in-deep learning-based intrusion detection system Ability to withstand adverse attacks. In order to train intrusion detection systems against malicious attack samples from the UNSW-NB 15 dataset, the system employs the min-max (or saddle-point) method. The

system uses the maximum method to produce adversarial examples that generate high loss and attack deep neural networks. The system says that adversarial attack methods made for binary domains can be used in continuous environments and misclassify in different ways. Finally, the system demonstrates that feature reduction based on principle component analysis (PCA) may improve the resilience of an intrusion detection system (IDS) utilizing a deep neural network (DNN).

According to [4], a comprehensive experimental study using a variety of binary is presented to reduce error and increase detection frequency. Additionally, numerous studies on intrusion detection systems have made use of out-of-date datasets like the Kddcup'99 dataset. Because the old dataset does not include them, the majority of them were unable to achieve the potential accuracy of identifying incursions with current invasions. Therefore, the goal of this research is to create a hybrid anomaly classification of IDS utilizing Deep Learning (DL) and Binary Algorithms (BA) as an optimizer, with the most current dataset for intrusion detection testing dubbed "CICIDS2017". Accuracy, recall, precision, confusion matrix, sensitivities, specific, and cost error (DNN and Binary Algorithms) are a few of the outcomes that have been analyzed and obtained for the hybrid version of DNN. According to [5] A new deep neural network architecture is designed to train adaptable and efficient intrusion detection models by merging an unsupervised stage for multi-channel feature learning with just a supervised step leveraging feature relationships on cross channels. The objective is to determine whether class-specific characteristics of network flows can be learned and incorporated into the fundamental characteristics to enhance model accuracy. Specifically, two autoencoders are trained independently every day, and attack flows in the unsupervised stage. Because the top layer of these autoencoders' decoders reconstructs samples in the same space as the input, each network flow can be represented as a multi-channel sample. Two additional feature vectors could be created using this method. In the supervised step, parametric convolution of multiple channels is used to learn how one channel affects the others. A wireless sensor network (WSN), as stated in [6], is made up of a number of sensor nodes that are scattered throughout the location of interest at random. Because the sensor nodes are mostly placed in harsh and open environments, they are very susceptible to assaults, necessitating the use of an efficient intrusion detection system (IDS). Machine learning (ML) methods are becoming increasingly popular in the development of IDS, particularly for energy-constrained WSN. The DA mostly uses the OMLP method to figure out the bias and weights of the MLP. The use of DA makes it possible to select the values of connection weights with greater efficiency, which improves detection performance. As stated in [7], CNN and RNN are two deep learning methods utilized in the creation of an intelligent detection system for the purpose of identifying a variety of network intrusions. The system also uses a number of evaluation matrices to evaluate the performance of the proposed solution. The system compares the results of the suggested solution to choose the optimum model for the network intrusion detection system.

According to [8] Their harmful activities may go unnoticed because their digital trace is hidden in huge log data dumps. This survey aims to provide a comprehensive explanation of the issue statement by focusing on Insider Threat Detection Using Deep Learning. The foundation was laid by the terms and definitions of insider threat detection. Deep Learning has been chosen as the method that should be used to address this issue statement because it has been demonstrated to perform better than traditional Machine Learning algorithms when dealing with complex data from a variety of sources. In addition, this study investigates the challenges that were encountered and the ways in which they have paved the way for subsequent research. However, due to its distributed and open design, which makes it susceptible to intrusions, privacy and security concerns are significant obstacles to the effective adoption of cloud computing. Cloud computing's open and dispersed features are more tempting to prospective hackers. Because of the openness of cloud computing, traditional intrusion detection technologies are often useless. This investigation examines how deep learning can be utilized to implement innovative intrusion detection systems that make use of a believe adaptive security model. Network security is one of the most pressing issues in contemporary research and business, according to Paper[10]. Network and data security are based on intrusion detection systems (IDSs). To achieve maximum detection accuracy, various IDS methods have been utilized over time. One of the most promising IDS strategies for identifying existing and emerging threats is machine learning. The different machine learning methods used to implement Network-based Intrusion Detection Systems are investigated in this article (NIDS).

3. METHODOLOGY

The study develops and evaluates machine learning and deep learning-based models for network intrusion detection using a quantitative, experimental approach. Preprocessing and analysis of several benchmark datasets are part of this study.

- Developed IDS models using machine learning and deep learning.
- Evaluation with numerous performance metrics.
- Analysis of model performance across many datasets.

Three crucial datasets are used in this study to train and evaluate intrusion detection models, such as NSL-KDD, UNSW-NB15, and CSE-CIC-IDS2018. The data undergoes normalization, encoding, and cleaning. Models for deep learning and machine learning are being developed. Both hybrid and optimized models are enhanced by the Dragonfly Algorithm, Binary Algorithms, and min-max optimization. Common metrics including accuracy, precision, recall, and F1-score are used to assess models.

4. CONCLUSION

Intrusion Detection Systems are critical for protecting against modern cyber threats, particularly in IoT environments. The complexity and volume of these threats necessitate sophisticated and adaptable security solutions. This work examined various recent contributions to the field and presented BotShield, a dual-phase IDS that combines anomaly detection and categorization with AI-based approaches. Our approach strikes a balance between early detection and accurate classification, resulting in a strong framework for IoT security. We show that by using advanced optimization algorithms and evaluating over different datasets, such hybrid models can greatly increase network intrusion detection effectiveness. However, issues such as adversarial attacks, model drift, and real-time processing remain open for future investigation.

ACKNOWLEDGEMENT

I would like to express my heartfelt appreciation to my guide for his constant support, insightful suggestions, and encouragement during the preparation of this survey paper. His invaluable guidance and thoughtful feedback played a significant role in the successful completion of this work.

REFERENCES

1. Amaizu, Gabriel Chukwunonso, et al. "Investigating Network Intrusion Detection Datasets Using Machine Learning." 2020 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2020
2. Abdel-Wahab, Mohab Sameh, Ahmed M. Neil, and Ayman Atia. "A Comparative Study of Machine Learning and Deep Learning in Network Anomaly-Based Intrusion Detection Systems." 2020 15th International Conference on Computer Engineering and Systems (ICCES). IEEE, 2020
3. Abou Khamis, Rana, M. Omair Shafiq, and Ashraf Matrawy. "Investigating Resistance of Deep Learning-based IDS against Adversaries using min-max Optimization." ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020.
4. Atefi, Kayvan, Habibah Hashim, and Touraj Khodadadi. "A Hybrid Anomaly Classification with Deep Learning (DL) and Binary Algorithms (BA) as Optimizer in the Intrusion Detection System (IDS)." 2020 16th IEEE International Colloquium on Signal Processing \& Its Applications (CSPA). IEEE, 2020.
5. Andresini, Giuseppina, et al. "Multi-channel deep feature learning for intrusion detection." IEEE Access 8 (2020): 53346-53359.
6. Amaran, Sibi, and R. Madhan Mohan. "An Optimal Multilayer Perceptron with Dragonfly Algorithm for Intrusion Detection in Wireless Sensor Networks." 2021 5th International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2021.
7. Ashraf, Javed, et al. "Novel deep learning-enabled lstm autoencoder architecture for discovering anomalous events from intelligent transportation systems." IEEE Transactions on Intelligent Transportation Systems (2020).
8. Al-Emadi, Sara, Aisha Al-Mohannadi, and Felwa Al-Senaid. "Using deep learning techniques for network intrusion detection." 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE, 2020.
9. Al Makdi, Khalid, Frederick T. Sheldon, and Abdullah Abu Hussein. "Trusted Security Model for IDS Using Deep Learning." 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS). IEEE, 2020.
10. Ahmed, Lubna Ali Hassan, and Yahia Abdalla Mohamed Hamad. "Machine Learning Techniques for Network-based Intrusion Detection System: A Survey Paper." 2021 National Computing Colleges Conference (NCCC). IEEE, 2021.