2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS)

DDoS and Botnet Attacks: A Survey of Detection and Prevention Techniques

Pranav S A
Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Ramapuram,
Chennai,India.
ps4174@srmist.edu.in

Sathya Priya S
Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Ramapuram,
Chennai,India.
sathyas6@srmist.edu.in

HariHaran B
Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Ramapuram,
Chennai,India.
hariharb@srmist.edu.in

2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS) | 979-8-3503-6482-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/ADICS58448.2024.10533615

Abstract*—The Internet of Things (IoT) heralds a innovative generation in communication via enabling regular gadgets to supply, receive, and percentage records easily. IoT applications, which prioritise venture automation, aim to present inanimate items autonomy; they promise increased consolation, productivity, and automation. However, strong safety, privateness, authentication, and recuperation methods are required to understand this goal. In order to assemble give up-to-quit secure IoT environments, this newsletter meticulously evaluations the security troubles and risks inherent to IoT applications. It emphasises the vital necessity for architectural changes.The paper starts by conducting an examination of security worries before exploring emerging and advanced technologies aimed at nurturing a sense of trust, in Internet of Things (IoT) applications. The primary focus of the discussion revolves around how these technologies aid in overcoming security challenges and fostering an ecosystem for IoT.

Keywords— AI for DDoS Attack Detection,AI in Botnet Attack Detection, Botnet attacks, Cybersecurity Training and Awareness, DDoS Attack, Deep Neural Network, Enhanced Very Fast Decision Tree (EVFDT), Entropy-based DDoS, Internet of Things (IoT), Intrusion Prevention System (IPS),Machine Learning, Network Security Enhancement, Non-Machine Learning Approaches ,One-Class SVM for DDoS Detection, Random Forest, SkyShield, Support Vector Machines (SVM).

I. INTRODUCTION

The blended impact of big data, new industry technology, and the pervasive effect of cloud services and the Internet of Things (IoT) has revolutionised a number of industries in the speedy evolving virtual landscape. In technological know-how, mainly when it comes to community protection, the most critical issues are finding and identifying focused attacks. These problems are vital due to the fact firms are having to deal with the ever-changing strategies utilized by cybercriminals. The volume, complexity, and difficulty of cyberattack detection may be an excessive amount of for human analysts to deal with. Organisations are nonetheless plagued via protection breaches, and the fee of cybercrime is anticipated to upward push. Cyber AI shows up as a effective ally, improving security groups with the capacity to respond greater speedy and expect attacker movements in advance.

The use of intelligence (AI) and deep learning has become widely for their contributions, to the current technological scenario. The integration of AI and deep learning has emerged as a great of advancements particularly in the realm of targeted threat identification.Notably, by microanalyzing AI and deep learning applications, the focus on harmful botnets and distributed denial of service (DDoS) attacks has produced significant outcomes. This technological ability becomes critical because the number of cyberattacks that target organisations worldwide is increasing.

A. Botnet attacks

In today's world of cloud computing the increasing threat of botnet attacks is a concern, for the security of both systems and Internet of Things (IoT) devices. With the emergence of computer architectures such, as always on mobile devices new avenues, for botnet attacks have come to light. A constant evolution of botnet kinds and attack tactics is the result of the widespread use of networked devices and a variety of system platforms. Understanding the nature of botnets, their historical growth, and the numerous mitigation strategies is essential to addressing the growing risk that they pose.[1] A botnet refers to a collection of computers or devices that have been infected on purpose and are controlled by an individual known as the "bot herder" or "botmaster." These compromised entities, referred to as bots or zombies [2] are programmed to carry out activities such, as spreading malware launching distributed denial of service (DDoS) attacks, stealing sensitive data and engaging in other cybercrimes. Given the interconnectivity of computing systems vulnerabilities, across a wide range of devices can be exploited, allowing botnets to thrive in this environment.

Mirai was created with the purpose of carrying out scale distributed denial of service (DDoS) attacks. By utilizing the combined power of compromised devices, the botnet could overwhelm targeted websites or online services by flooding them with an immense amount of traffic. The goal was to disrupt the operations of these services rendering them inaccessible to legitimate users

One notable incident involving [3] Mirai took place in 2016 when it orchestrated a DDoS attack, on Dyn a Domain Name System (DNS) provider. This attack caused internet outages impacting websites and services such, as Twitter, Netflix and Spotify.

B. **DDoS Attack**

In the changing world the threat of Distributed Denial of Service (DDoS) attacks persists and poses a serious risk, to the availability and functionality of crucial online services. These attacks, which aim to overwhelm platforms with traffic

IEEE 979-8-3503-6482-8/24/$31.00 ©2024 IEEE

have become increasingly sophisticated and consequential. Recently there has been an increase in known websites becoming victims of what is commonly referred to as a "service attack." At the core of this trend lies DDoS attacks, where coordinated assaults originate from distributed hosts, across the internet simultaneously.

In 2023 there was an more recent example of the power of DDoS attacks involving GitHub, which is known as one of the worlds software development platforms. During this incident an effective DDoS attack specifically targeted GitHub's infrastructure. The attackers skillfully used a combination of volumetric and application layer attack techniques causing disruptions, to the platforms services and impacting its user community.

GitHub, which plays a role in software development encountered difficulties, in maintaining its services amidst this onslaught. This incident served as a reminder of how DDoS attackers adapt and find ways to bypass mitigation strategies.

II. TYPES OF ATTACK DETECTION METHODS FOR BOTNET AND DDOS

Traditional methods to detect Botnet Attack

1.Monitoring Network Traffic: Collect and analyze data regarding the flow of network activity using tools, like Wireshark, Snort or specialized solutions.

2. Extracting Relevant Features: Retrieve attributes from the network traffic data, such as source/destination IP addresses, ports, protocols, packet sizes, frequency of packets sent/received, etc.

3.Detecting Anomalies: Utilize techniques to detect patterns within the network traffic that could indicate potential botnet attacks.

4. Analyzing Behavioral Patterns: Study the behavior of devices connected to the network in order to identify patterns associated with botnet activity.

5. Identification based on Signatures: Keep track of signatures connected to different botnets in a database, then match signatures with network traffic to find matches.

Machine Learning Method's [4] for Botnet attack

1.Machine Learning: Transforming raw data into a machine learning format using data transformation and preprocessing techniques. Development of a state-of-the-art machine learning model for botnet detection, utilizing the latest emerging techniques. Classification of botnet attacks based on the UNSW-NB15 dataset.

2. Deep Neural Network (DNN) for IoT Attack Detection: Utilizing Deep Neural Network (DNN) [18] for detecting IoT attacks. Testing on datasets like KDD-Cup'99, NSL-KDD, and UNSW NB15, demonstrating high precision rates exceeding 90%). Leveraging deep learning for effective intrusion detection in IoT environments. Employing Synthetic Minority Oversampling Technique (SMOTE) to address imbalanced datasets. Specialized technique for balancing datasets in classification problems where classes are not equally represented. Generating synthetic samples to ensure a more equal class distribution and enhance model performance.

AI Based detection technique

1.Machine Learning Models: One such approach involves employing machine learning models like Support Vector Machines (SVMs), Random Forests and Neural Networks. These models help distinguish between traffic and botnet activity.

2. Real-time Behavioral Analysis: Implemented using advanced bot mitigation tools, like DataDome. These solutions leverage the power of intelligence to analyze behavior in time and identify and block botnet activities.

Traditional Methods to detect DDoS attacks

1.The Enhanced Very Fast Decision Tree (EVFDT):

The Enhanced Very Fast Decision Tree (EVFDT) [5] is designed for cloud-assisted Wireless Body Area Networks (WBAN) with the primary aim of efficiently detecting Distributed Denial of Service (DDoS) attacks within WBANs. This tree-based approach employs distinctive features, including adaptive tie-breaking for determining node splitting thresholds and a lightweight iterative pruning method to effectively manage extreme noise, ultimately achieving a notable balance between high accuracy and lower false alarms in the detection of DDoS attacks. Despite its strengths, such as providing precision in DDoS attack detection, integrating adaptive mechanisms for enhanced performance, and offering a lightweight iterative pruning method to address noise concerns, EVFDT is acknowledged to have limitations, notably its unsuitability for real WBAN testbeds, limiting its performance evaluation. In contrast, the proposed Network Analysis Tree (NAT) serves as a potential solution to address system deficiencies arising from DDoS attacks. NAT adopts a tree-based approach for the systematic detection, prevention, and analysis of DDoS attacks. The methodology operates in a step-by-step fashion, identifying active components, standards, and attributes during attacks to ensure a comprehensive understanding and mitigation of DDoS-induced issues. This approach is strategically positioned to mitigate the challenges posed by DDoS attacks in networked environments.

2. Entropy-based DDoS:

Entropy-based DDoS attack detection relies [6] on minimal packet header data to model legitimate traffic patterns, allowing for resource-efficient and rapid detection. However, challenges arise from fixed thresholds in dynamic attack scenarios, leading to potential oversight of anomalies with similar uncertainty levels. Establishing self-adaptive thresholds proves challenging, restricting the practicality of entropy-based methods. To overcome these limitations, the integration of machine learning techniques is on the rise, aiming to improve detection accuracy and address shortcomings inherent in traditional models.

3. Random Forest for IoT Attack Detection:

In the evolving field of CyberSecurity the renowned machine learning technique called " forest " developed by Leo Breiman and Adele Cutler plays a vital role as a powerful ally. This methodology is highly adaptable and user friendly making it extremely relevant, for addressing both regression and classification challenges in the landscape of Internet of Things (IoT) attack detection.

IEEE 979-8-3503-6482-8/24/$31.00 ©2024 IEEE

Detection Technique	Attack Type	Detection Method	Description
Signature-based	General Network Attacks	Intrusion Prevention System (IPS)	Utilizes predefined attack signatures for identifying malicious activities. Provides a comprehensive defense against a wide range of network attacks.
Signature-based	DDoS Attacks	Entropy-based DDoS	Applies fixed thresholds to detect anomalies in traffic patterns. Efficiently identifies DDoS attacks with minimal packet header data.
Anomaly-based	General Network Attacks	EVFDT	Analyzes individual elements and overall traffic patterns to identify unusual behavior. Specifically tailored for WBANs to detect and counter Distributed Denial of Service
Anomaly-based	DDoS Attacks	Random Forest for IoT	Detects patterns in network traffic that deviate from normal user behavior. Adapts to diverse Internet of Things (IoT) attack patterns, offering flexibility in detection.
Anomaly-based	DDoS Attacks	One-Class SVM for DDoS	Trained on normal user behavior to recognize deviations as anomalies. Focuses on detecting application-layer DDoS attacks by learning from normal user behavior.
Anomaly-based	DDoS Attacks	SkyShield	Utilizes two hash tables to identify anomalies introduced by malicious hosts. Designed for preventing application-layer DDoS attacks, emphasizing HTTP protocol protection.
Hybrid	General Network Attacks	Support Vector Machines (SVM)	Can function in both signature-based (C-SVM) and anomaly-based (OC-SVM) modes. Versatile in addressing various attack types, depending on the model configuration.

Table on Methods to detect DDoS Attack

When it comes to securing IoT systems where threats are rapidly expanding the random forest method proves to be invaluable. By combining the results from decision trees this approach becomes proficient at identifying patterns that signify various types of IoT attacks. The flexibility of forest is especially crucial in dealing with attacks that target IoT devices since it can quickly adapt to emerging threats.

As the interconnectedness within the ecosystem grows there is an increasing demand for mechanisms to detect attacks. The versatility of forest in handling attack scenarios and seamlessly transitioning between regression and classification tasks makes it an ideal tool for safeguarding against evolving threats faced by IoT devices. In particular when it comes to attacks on systems where swift response is crucial the patented nature of random forest aids in synthesizing decision trees thereby enhancing accuracy and efficiency, in detection mechanisms.

Integrating the forest approach into the investigation of attack detection brings a higher level of complexity to the exploration of defense strategies. With the growing number of threats, in the realm utilizing the flexibility and simplicity offered by random forest becomes an intriguing path to strengthen security measures.

4. Support Vector Machines:

Support Vector Machines (SVM) [7] in Intrusion Detection Systems (IDS) for cybersecurity. SVM, a powerful supervised machine learning algorithm, creates a binary classification model to address complex, non-linear problems. The methodology involves two main types: C-SVM, suitable for multiple classes like benign and malicious activities, and OC-SVM, effective for anomaly detection based on normal activity profiles. The Radial Basis Function (RBF) kernel is chosen for its computational efficiency in identifying support vectors. Scaling ensures the significance of parameters, and cross-validation with grid search optimizes free parameters like C to maximize the SVM hyperplane margin. This approach contributes to the development of accurate intrusion detection models, crucial for enhancing cybersecurity defenses.

Methods To detect DDoS Attack

The table above mentioned presents an overview of network security detection methods, including approaches based on anomalies and signatures for different types of attacks. Signature-based techniques, such as IPS, rely on pre-established patterns, whereas anomaly-based techniques, such as EVFDT and Random Forest, look for changes from typical behaviour.For a comprehensive defence against network security threats, hybrid models like SVM combine both strategies; however, specialised tools like One-Class SVM and SkyShield focus on specific threats like DDoS attacks.

1.EVFDT (Enhanced Very Fast Decision Tree): EVFDT is designed specifically for cloud assisted Wireless Body Area Networks (WBAN). Its main objective is to detect Distributed Denial of Service (DDoS) attacks. The methodology includes tie breaking to determine node splitting thresholds and a lightweight iterative pruning technique. This ensures a balance, between accuracy and minimizing false alarms in detecting DDoS attacks.

2. Entropy-based DDoS: To effectively detect traffic patterns, minimal packet header data analysis is employed, However challenges arise when fixed thresholds are used in attack scenario, therefore techniques are explored accuracy.

3. Random Forest for IoT Attack Detection: In the field of attack detection a methodology utilizes decision trees to identify patterns associated with IoT attacks efficiently.[19] This approach adaptability to offers address emerging threats against devices quickly.

4. Support Vector Machines (SVM) in IDS: Support Vector Machines (SVM) play a role in Intrusion Detection Systems (IDS) for cybersecurity. SVM creates a classification model of handling complex non-linear problems effectively. It improves security through approaches such, as C SVM and OC SVM that cater to classes and anomaly detection. The utilization of the Radial Basis Function (RBF) kernel contributes to efficiency.

5.SVM for Application Layer DDoS Detection: A unique model, which employs a single class Support Vector Machine (SVM) can differentiate between users and botnets that carry out Distributed Denial of Service (DDoS) attacks targeting the application layer. Trained on user behavior this SVM is excellent, at identifying patterns by detecting deviations from the established norm.

6. Intrusion Prevention System (IPS): IPS is a critical security apparatus that continuously scans network traffic, identifies known attack signatures, and acts in real time to thwart potential threats. It actively engages in risk mitigation, generating alerts for administrators and taking immediate actions against identified threats to reinforce network defenses.

7. SkyShield DDoS Defense System: SkyShield utilizes a unique approach during the detection phase by analyzing the divergence between two hash tables, known as Sketches. Incorporates protective measures during the mitigation phase, including filtering, whitelisting, blacklisting, and CAPTCHA. Custom datasets are employed for evaluation.

III TYPES OF ATTACK PREVENTION METHODS FOR BOTNET AND DDoS

A. ATTACK PREVENTION METHODS IN BOTNET

1.Cybersecurity Training and Awareness

Educating staff members through regular training sessions on cybersecurity is a fundamental strategy to prevent botnet attacks, particularly those originating from phishing attempts. Feily [8] and Alexander and Wanner [9] underscore the role of social engineering attacks, which rely on deceiving individuals. By enhancing the awareness of employees regarding various social engineering and phishing tactics, organizations empower them to identify and avoid potential threats. Training programs should emphasize the significance of not clicking on unfamiliar links, verifying the legitimacy of emails, and exercising caution when dealing with unknown attachments. This proactive approach establishes a human barrier against the initial stages of botnet intrusion.

2.Network Security Enhancement

Strengthening network security measures is crucial for thwarting botnet attacks effectively. As recommended by Bhandari [10] and Tunggal [11], a key prevention technique involves closing unused ports on the network, reducing the potential points of entry for unauthorized access by bot-masters. Regular updates to firewalls and security configurations are essential to scrutinize and filter suspicious packets within network traffic, addressing the insights provided by Bhandari [10]. Implementing Access Control Lists (ACLs) offers an additional layer of defense by specifying which devices are permitted to communicate within the network, as suggested by Gupta [12]. This strategy restricts the pathways that botnets can exploit, minimizing the risk of unauthorized access through open services or vulnerabilities.

B. ATTACK PREVENTION METHODS IN DDoS

1. SVM

A specialized model utilizing a single-class Support Vector Machine (SVM) was crafted to discern regular users from botnets launching denial-of-service attacks on application layers. Trained exclusively on normal user behavior, this One-Class SVM effectively detects Distributed Denial of Service (DDoS) attacks at the application layer by identifying deviations from the learned norm.[13] Researchers emphasized parameter selection and dataset curation to ensure accurate detection, while fine-tuning SVM parameters, such as kernel type and regularization, optimizes the model's performance in distinguishing between normal and attack traffic. This focused approach leverages the distinctive patterns associated with legitimate user behavior to pinpoint application layer DDoS attacks.

2.IPS

An essential component in ensuring network security is the Intrusion Prevention System (IPS), a critical security apparatus that plays a pivotal role in fortifying defenses against cyber threats. This sophisticated system acts as a vigilant guardian by continuously scanning network traffic, scrutinizing patterns, and identifying known attack signatures. Functioning in real-time, the IPS acts promptly to thwart potential threats, adding an additional layer of protection to the network.

IPS operates by closely monitoring network traffic and leveraging pre-defined attack signatures. These signatures serve as fingerprints for known attack patterns, allowing the system to rapidly identify malicious activities. Simultaneously, the IPS has the capability to detect anomalies, recognizing deviations from established behavioral norms. By actively engaging in this pattern analysis, the IPS ensures a proactive defense mechanism, capable of swiftly responding to emerging threats.

Moreover, the IPS doesn't merely function as a passive observer; it actively engages in risk mitigation. Upon detecting a potential threat, the system generates alerts for administrators, providing them with timely notifications. Furthermore, the IPS is equipped to take immediate and automated actions against identified threats, preventing the escalation of security breaches. By enforcing security policies, the IPS contributes significantly to maintaining the integrity and resilience of the network against dynamic and evolving cybersecurity threats.

3. Skysheild

SkyShield [14] is proposed as a solution for detecting and preventing Distributed Denial of Service

IEEE 979-8-3503-6482-8/24/$31.00 ©2024 IEEE

(DDoS) attacks at the application layer. The system employs a unique approach during the detection phase, utilizing the divergence between two hash tables, known as Sketches, to identify anomalies introduced by malicious hosts. To enhance mitigation, SkyShield incorporates protective measures such as filtering, whitelisting, blacklisting, and CAPTCHA during the mitigation phase. The evaluation of the system involved the use of custom datasets tailored to assess its effectiveness. It is essential to note that SkyShield primarily focuses on the application layer, specifically the HTTP protocol. However, it is acknowledged that potential vulnerabilities may exist if flooding occurs at the network and transport layers, necessitating a comprehensive understanding of the system's limitations and potential impact.

PREVENTION TECHIQUES ON DDoS BOTH TRADITIONAL AND ML METHODS

I Traditional Methods

1.Intrusion Prevention System (IPS): Continuously scans network traffic. Identifies known attack signatures.Acts in real-time to thwart potential threats. Utilizes pre-defined attack signatures as fingerprints. Recognizes anomalies by detecting deviations from behavioral norms. Engages in risk mitigation by generating alerts for administrator's takes immediate and automated actions against identified threats. Enforces security policies to maintain network integrity.

II Machine Learning Methods

1.One-Class SVM for DDoS Detection: Crafted for discerning regular users from botnets in DDoS attacks. Trained exclusively on normal user behavior.Detects anomalies by identifying deviations from the learned norm. Emphasizes parameter selection and dataset curation for accuracy. Fine-tunes SVM parameters for optimal performance. Leverages distinctive patterns associated with legitimate behavior.

2.SkyShield for Application Layer DDoS Prevention: Detects and prevents DDoS attacks at the application layer. Utilizes a unique approach with two hash tables (Sketches) during detection Identifies anomalies introduced by malicious hosts. Incorporates protective measures like filtering, whitelisting, blacklisting, and CAPTCHA during mitigation. Evaluates system effectiveness using custom datasets. Primarily focuses on the application layer, specifically the HTTP [20] protocol. Acknowledges potential vulnerabilities if flooding occurs at network and transport layers, requiring a comprehensive understanding of limitations and potential impact.

III ADVANTAGES AND CHALLENGES FOR ATTACK DETECTION METHODS FOR BOTH BOTNET AND DDoS

1. Machine Learning (ML) for Botnet Attack Detection

Advantages

Efficient Data Processing: Machine learning models are ideal for the high volume of network[17] traffic related to botnet detection as they process large datasets rapidly and efficiently in real time.

Automated Recognition of Patterns: Without the need for human intervention, it is possible to identify complicated and subtle patterns that indicate botnet activity by using machine learning models to automate pattern recognition.

Adaptability to Dynamic Threats: ML models can adapt to evolving attack strategies and changing behaviors, offering a robust defense against dynamic and continually evolving botnet threats.

Challenges

Training Data Requirement: ML models necessitate substantial labeled training data for accurate pattern generalization, posing challenges, particularly for emerging or novel botnet attacks.

Potential for False Positives: ML models may generate false positives, incorrectly identifying benign network behavior as malicious. Balancing false positive reduction without compromising detection accuracy requires careful fine-tuning.

2.Machine Learning (ML) for DDoS Attack Detection

Advantages

Real-Time Capabilities: ML models provide real-time detection capabilities, swiftly identifying and responding to DDoS attacks as they occur.

Advanced Pattern Recognition: ML algorithms excel at recognizing intricate patterns associated with DDoS attacks, enhancing overall detection accuracy.

Challenges

Interpretability Issues: Deep learning models within ML may lack interpretability, making it challenging for cybersecurity analysts to understand decision rationale.

Computational Complexity: Some ML models, especially those using deep learning, may demand significant computational resources, potentially leading to performance issues in resource-constrained environments.

3.Artificial Intelligence (AI) in Botnet Attack Detection:

Advantages

Extensive Behavioral Analysis: AI systems conduct in-depth behavioral analysis, enabling a [16]nuanced understanding of network activities and accurate identification of botnet behaviors.

Accurate Signature Recognition: AI-based[15] systems achieve high accuracy in recognizing and matching signatures associated with known botnets.

Challenges

Complex Deployment Processes: Implementing AI solutions for botnet detection may involve intricate deployment processes, requiring careful integration into existing network infrastructures.

Resource-Intensive Implementations: AI-based solutions can be resource-intensive, demanding significant computing power and storage, posing challenges for certain organizational setups.

4.AI for DDoS Attack Detection

Advantages

Complex Algorithm Usage: AI employs sophisticated algorithms, enhancing detection capabilities, particularly in identifying intricate DDoS attack patterns.

Challenges

Complex Implementations: Deploying and managing AI for DDoS attack detection may require specialized knowledge, making the implementation process intricate.

5.Non-Machine Learning (Non-ML) Approaches - DDoS Attack Detection

Advantages

IEEE 979-8-3503-6482-8/24/$31.00 ©2024 IEEE

Efficient Detection of Established Patterns: Non-ML approaches, like rule-based or signature-based methods, efficiently detect well-established attack patterns.

Prompt Defense via Firewalls: Non-ML methods enable quick defense mechanisms through firewalls, responding rapidly to known attack signatures.

Challenges

Limited Behavioral Analysis Depth: Non-ML approaches may have limitations in analyzing complex and evolving behavioral patterns, potentially leading to a higher likelihood of false negatives for novel attack types.

Less Adaptability to Novel Patterns: These methods may struggle to adapt to new and evolving attack patterns, necessitating regular updates to signature databases.

Research challenges:

Dealing with botnet and DDoS attacks presents a significant challenge for research in the field of IoT security. Novel approaches like transfer learning or the creation of synthetic data are needed to address problems like the lack of data for machine learning models in new attack scenarios. It is necessary to investigate cutting edge algorithms or hybrid approaches in order to reduce false positives in machine learning systems without sacrificing accuracy. It is imperative to develop resource-efficient AI models for scalability in resource-constrained environments in addition to improving interpretability in deep learning models through explainable AI techniques. Simplified integration procedures for artificial intelligence solutions should be a priority, and non-ML approaches require innovations for thorough behavioural analysis. Future research has the chance to create objective metrics and frameworks because prevention techniques currently lack a standardised evaluation framework.

Conclusion:

In conclusion, the paper sheds light on the security challenges in IoT, where connected devices face threats. To tackle these issues, the study suggests using smart technology like machine learning and AI. It discusses different ways to spot and stop attacks, especially those from botnets and DDoS.

The paper starts by talking about the overall safety concerns in IoT and stresses the need for better security plans. It says that using machine learning and AI can make IoT safer. The study looks at different methods to find attacks, putting them into groups based on their features.

There's a good part about botnet attacks, like the Mirai one that caused big problems. The paper talks about usual ways to find attacks, like checking network activity and watching how devices behave. It then talks about fancier methods, like using machines to learn patterns and AI to find problems.

The paper explains the strengths and weaknesses of each method, showing how machine learning and AI can be powerful. It highlights specific models like SVM and Random Forest, which can find both botnet and DDoS attacks.

Preventing attacks is also discussed, including using SVM for a certain kind of attack and a system called SkyShield for another. The paper praises old-school methods like IPS, which keeps an eye on things and acts fast.

To sum it up, blending machine learning and AI is crucial for making IoT safer. The paper gives a full picture of different ways to find and stop attacks, pointing out how adaptable methods like Random Forest and SkyShield are. The paper says it's important to use a mix of old and new ways to stay strong against changing threats in IoT.

References

[1] S. N. T. Vu, M. Stege, P. I. El-Habr, J. Bang, and N. Dragoni, "A Survey on Botnets: Incentives, Evolution, Detection and Current Trends," Future Internet, vol. 13, no. 8, p. 198, Jul. 2021, doi: 10.3390/fi13080198.

[2] K.-K. R. Choo, "Zombies and Botnets," Trends and Issues in Crime and Criminal Justice, vol. 327, no. 1, pp. 1-6, Mar. 2007.

[3] G. Kambourakis, C. Kolias, and A. Stavrou, "The Mirai botnet and the IoT Zombie Armies," presented at MILCOM 2017 - 2017 IEEE Military Communications Conference, Baltimore, MD, USA, 2017.

[4] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, "Botnet Attack Detection in IoT Using Machine Learning," vol. 2022, Article ID 4515642, 2022, doi: 10.1155/2022/4515642.

[5] R. Latif, H. Abbas, S. Latif, and A. Masood, "EVFDT: An Enhanced Very Fast Decision Tree Algorithm for Detecting Distributed Denial of Service Attack in Cloud-Assisted Wireless Body Area Network," vol. 2015, Article ID 260594, 2015, doi: 10.1155/2015/260594.

[6] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," J. Sens. Actuator Netw., vol. 12, no. 4, p. 51, Jul. 2023, doi: 10.3390/jsan12040051.

[7] C. Ioannou and V. Vassiliou, "Network Attack Classification in IoT Using Support Vector Machines," J. Sens. Actuator Netw., vol. 10, no. 3, p. 58, Aug. 2021, doi: 10.3390/jsan10030058.

[8] M. Feily, A. Shahrestani, and S. Ramadass, "A Survey of Botnet and Botnet Detection," in Proceedings of the 2009 Third International Conference on Emerging Security Information, Systems and Technologies, Athens, Greece, 2009, pp. 268-273, doi: 10.1109/SECURWARE.2009.64.

[9] M. Alexander, "Methods for Understanding and Reducing Social Engineering Attacks," SANS Institute, May 3, 2016.

[10] P. Bhandari, "Botnet Detection and Prevention Techniques: A Quick Guide," XenonStack, Jan. 26, 2022.

[11] T. Tunggal, "What is an Open Port? Definition & Free Checking Tools," ,2021.

[12] B. B. Gupta, R. C. Joshi, and M. Misra, "Distributed Denial of Service Prevention Techniques," International

Journal of Computer and Electrical Engineering (IJCEE), vol. 2, no. 2, pp. 268-276, 2010.

[13] C. She, W. Wen, Z. Lin, and K. Zheng, "Application-layer DDoS Detection Based on a One-class Support Vector Machine," International Journal of Network Security & Its Applications (IJNSA), vol. 9, no. 1, pp. 13-26, January 2017, doi: 10.5121/ijnsa.2017.9102.

[14] C. Wang, T. T. N. Miu, X. Luo, and J. Wang, "SkyShield: A Sketch-Based Defense System Against Application Layer DDoS Attacks," IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 559-573, March 2018, doi: 10.1109/TIFS.2017.2758754.

[15] Salim M. M.; Rathore S.; Park, J. H. "Distributed denial of service attacks and its defenses in IoT: a survey," The Journal of Supercomputing, vol. 76, pp. 5320–5363, Jul. 2019, DOI: 10.1007/s11227-019-03067-x.

[16] K. Kaur and J. Ayoade, "Analysis of DDoS Attacks on IoT Architecture," in 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Palembang, Indonesia, 20-21 Sept. 2023, pp. 1-6, IEEE, 2023. doi: 10.1109/EECSI59885.2023.10295766.

[17] F. Hussain et al., "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," IEEE Access, vol. 9, pp. 163412-163430, Nov. 25, 2021. DOI: 10.1109/ACCESS.2021.3131014.

[18] Y. Batham and R. K. Tiwari, "A CNN Deep Learning Technique for Botnet Attack Detection for IoT Application," in 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 19-20 June 2023, pp. 1-5, IEEE, 2023. DOI: 10.1109/ICPCSN58827.2023.00199.

[19] Chanal, P. M., & Kakkasageri, M. S. (2023). "Random Forest Algorithm based Device Authentication in IoT." In 2023 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 14-16 July 2023, pp. 1-6. IEEE. DOI: 10.1109/CONECCT57959.2023.10234738.

[20] Shaaban, A. R., Abdelwaness, E., & Hussein, M. (2019). "TCP and HTTP Flood DDOS Attack Analysis and Detection for Space Ground Network." In 2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Cairo, Egypt, 04-06 September 2019, pp. 1-6. IEEE. DOI: 10.1109/ICVES.2019.8906302.

IEEE 979-8-3503-6482-8/24/$31.00 ©2024 IEEE