Review

Botnet Detection Techniques: A Comparative Study

Mohammad Alauthman *

Posted Date: 6 November 2023

doi: 10.20944/preprints202311.0311.v1

Keywords: Botnet detection; Network traffic analysis; Machine learning; Deep learning Cybersecurity; Adversarial machine learning

Review

Botnet Detection Techniques: A Comparative Study

Mohammad Alauthman *

Department of Information Security, Faculty of Information Technology, University of Petra, Amman, 11196, Jordan; mohammad.alauthman@uop.edu.jo.

* Correspondence: mohammad.alauthman@uop.edu.jo

Abstract: Botnets pose a grave cybersecurity threat, enabling widescale malicious activities through networks of compromised devices. Detecting botnets is challenging given their frequent use of evasion techniques like encryption. Traditional signature-based methods fail against modern botnets capable of zero-day attacks. This paper surveys recent advances applying machine learning for botnet detection based on analysis of network traffic payloads, flows, DNS data, and hybrid feature fusion. Core machine learning models include support vector machines, neural networks, random forests, and deep learning architectures, which extract patterns to separate benign and botnet behaviors automatically. Results demonstrate machine learning's capabilities in identifying heterogeneous botnets using artifacts in network streams. However, challenges remain around limited labeled data, real-time streaming, adversarial evasion, and model interpretability. Promising directions involve semi-supervised learning, adversarial training, scalable analytics, and explainable AI to address these gaps. Beyond the technical aspects, responsible development and deployment of botnet detection systems raise ethical considerations around privacy, transparency, and accountability. With diligent cross-disciplinary collaboration, machine learning promises enhanced, generalizable, and trustworthy techniques to combat the serious threat posed by continuously evolving botnets across the digital ecosystem.

Keywords: botnet detection; network traffic analysis; machine learning; deep learning; cybersecurity; adversarial machine learning

1. Introduction

Recent major botnet attacks, such as Mirai in 2016 and Echobot in 2019, have compromised hundreds of thousands of IoT devices, generating immense DDoS traffic volumes nearing 1Tbps. The scale and impact of these incidents highlight the urgent need for advanced botnet detection capabilities beyond traditional signature-based methods.

A botnet refers to a network of compromised devices, known as bots, controlled by a botmaster through command and control (C&C) channels[1]. Botnets allow cybercriminals to perform malicious activities, including distributed denial-of-service (DDoS) attacks, spamming, click fraud, and data theft [2]. The botmaster can issue commands to the compromised bots to send spam, launch DDoS attacks, or steal credentials. Botnets pose a major cybersecurity threat, with recent estimates of over 6 million active botnet infections globally [3,4].

Detecting botnets is challenging as botmasters frequently modify their C&C protocols and evasion techniques to avoid detection [5]. Existing botnet detection relies on inspecting network traffic payloads, flow-based features, DNS features, or a combination of these data sources. However, encrypted communications obstruct payload-based analysis. Flow-based methods are susceptible to mimicry attacks that manipulate flow features to appear as normal traffic. DNS-based detection can be defeated using domain generation algorithms (DGAs) and fast-flux techniques [2].

Given these challenges, there is significant interest in leveraging machine learning techniques for botnet detection. Machine learning can automatically extract useful features from network traffic to identify botnet anomalies [5,6]. This paper surveys recent research applying machine learning for botnet detection. We categorize detection systems based on the network data used, including payload, flow, DNS, and hybrid data. We also summarize key machine learning algorithms like

SVMs, neural networks, random forests, and deep learning models. Ongoing challenges and future research directions are discussed.

2. Detection approach

2.1. Traffic Payload-Based Detection

Payload-based detection analyzes packet contents to identify signatures or anomalies indicative of botnets. Early systems used deep packet inspection (DPI) to match known botnet signatures defined manually or via regular expressions [7]. However, hand-engineering detection rules is labor-intensive and fail to catch zero-day attacks. This motivated applying machine learning to learn models that separate benign and malicious payloads automatically.

Specific machine learning models for payload-based detection include multilayer perceptrons for general pattern recognition, convolutional neural networks for identifying spatial patterns in packet data, and recurrent neural networks for sequence modelling of network streams. For example,

Mashaleh et al.[8] developed an IoT botnet detection system using convolutional and recurrent neural networks trained on fused packet payload and flow data, achieving 97.3% accuracy. Alsarhan et al. [4] proposed an intrusion detection framework for vehicular networks using SVMs optimized with genetic algorithms (GAs) and particle swarm optimization (PSO). Features were extracted from network traffic payloads. Results showed GAs achieved higher accuracy versus PSO and unoptimized SVMs.

Younisse et al. [9] addressed the lack of labeled multistage attack data by developing a novel kerberoasting attack dataset. Network traffic capturing a realistic attack scenario was processed to extract informative features for each attack stage. The resulting dataset provides valuable data reflecting the sequential steps of an actual attack life-cycle. This can enhance the testing and evaluation of intrusion detection systems against sophisticated multistage attacks. However, only a single attack type was included, and expanding to diverse botnet scenarios could strengthen its utility.

Alslman et al.[10] focused on improving the robustness of payload-based intrusion detection systems against adversarial attacks. They utilized a denoising autoencoder technique to defend SNMP-MIB based botnet detection from multiple white-box and black-box attack types. Testing showed accuracy improved from 68% under attack to 90% with the defense applied. However, their approach concentrated only on protection rather than initial botnet detection capabilities. The study demonstrates the potential of autoencoders to harden payload-based detectors against evasion attempts.

AlMasri et al.[11] addressed the lack of data for supply chain attacks by generating a novel dataset modeling the SUNBURST malware. The concise, practical dataset reflecting observable attack indicators will aid researchers in enhancing defences against this threat vector. However, only one machine-learning algorithm was used to validate the data. The specialized dataset is valuable for evaluating payload analysis methods against supply chain attacks.

Qabalin et al. [12] collected a new payload-based dataset focused on Android spyware detection. Traffic was gathered reflecting spyware installation and operation activities on real devices. Multi-class experiments demonstrated 79% accuracy in identifying the spyware strains. However only random forest was tested as the classifier. The unique dataset advances malware detection research, although more complex models could be evaluated.

A limitation of payload-based detection is the inability to analyze encrypted traffic contents. Botnets increasingly leverage encryption and polymorphism to evade deep packet inspection. Alternative methods to inspect encrypted traffic metadata have been proposed. However, fundamentally, encryption reduces the efficacy of payload-based botnet detection. Table 1 summarizes key papers in this area, their methods, datasets, results, pros, and cons.

Table 1. Summary of flow-based botnet detection papers.

Authors	Method	Dataset	Results	Pros	Cons
Alsarhan et al.[4]	Optimized SVM	Network payload features	Higher accuracy with GA optimization	Meta-heuristic optimization	Focused on vehicular networks
Younisse et al. [9]	Dataset labelling	Kerberoasting attack traffic	Multistage attack dataset	Realistic attack data	Single attack type
Alslman et al. [10]	Denoising autoencoder	SNMP-MIB traffic	Accuracy improved from 68% to 90% under attack	Robust to evasion attacks	The only defence, not detection
AlMasri et al. [11]	J48 ML	Generated SUNBURST data	87.7% F-measure	Novel supply chain attack data	Single ML algorithm
Qabalin et al. [12]	Random forest	Android spyware traffic	79% multi-class accuracy	New spyware dataset	Limited classifiers tested

The highlighted works showcase deep learning, optimization, dataset generation, and robustness techniques for advancing payload-based botnet detection. The machine learning innovations explored include CNN-RNN fusion, autoencoders, and ensemble learning. However, limitations exist around the evaluation of single datasets, focusing on defence rather than initial detection, and testing a few classifier types.

In conclusion, payload analysis continues to be a valuable approach for identifying botnet threats through network traffic monitoring. The surveyed papers demonstrate promising applications of machine learning to enhance detection accuracy, integrity against attacks, and generalizability across evolving botnets. Further research can build on these works by expanding evaluation across diverse, standardized datasets using a broader range of deep learning architectures in an adversarial setting. Advancing payload-based detection will require leveraging the full suite of modern machine-learning capabilities.

2.2. Flow-Based Detection

Network flows encapsulate key traffic statistics like duration, bytes, and timing between packets. Flow-based detection analyzes communication patterns to identify botnet anomalies and cluster similar flows.

Early work focused on hand-selecting flow features to improve botnet classification. Alauthman et al. [1] used a reinforcement learning classifier trained on flow features, including flow duration, average bytes, and average packets per flow. More recent research automates feature engineering using machine learning. Alieyan et al.[2] evaluated various classifiers, including SVMs, Naive Bayes, and decision trees trained on statistical flow features for botnet detection.

A benefit of flow-based detection is the ability to analyze encrypted traffic by relying exclusively on flow metadata. However, flow-based methods remain susceptible to mimicry attacks, which manipulate flows to emulate normal traffic patterns [5]. Defending against flow-based evasion attacks remains an open challenge.

Useful flow features engineered from network traffic include duration, idle time between packets, packet counts, byte counts, byte-per-packet ratios, and variance in packet arrival intervals. Preparing raw flow data for effective machine learning requires careful preprocessing like normalization. Table 2 summarizes key flow-based botnet detection research in terms of methods, datasets, results, advantages, and limitations.

Table 2. Summary of flow-based botnet detection papers.

Authors	Method	Dataset	Results	Pros	Cons
Alauthman et al.[1]	Reinforcement learning	Flow features	Learned classifier	Automated feature learning	Single technique evaluated
Alieyan et al. [2]	SVMs, Naive Bayes, decision trees	Statistical flow features	Compared classifiers	Evaluated multiple models	Focused only on accuracy

The highlighted works showcase reinforcement learning and classical ML algorithms for learning from network flow metadata. Automating feature engineering eliminates manual selection needed in early systems. However, limitations exist around model overfitting and susceptibility to mimicry attacks.

In conclusion, flow-based detection provides a means to monitor botnets, including encrypted traffic, by relying on metadata patterns. The surveyed papers demonstrate initial applications of machine learning to extract useful flow features and comparisons between algorithms. Further research is needed to enhance model generalization and integrity against evasion attempts. Applying deep learning and adversarial training represents promising directions for progress in flow-based botnet detection.

2.3. DNS-Based Detection

The Domain Name System (DNS) offers a key control channel for botnets to locate C&C servers and receive updates. Analyzing DNS traffic can reveal botnet activity through anomalous lookup patterns. Botmasters use domain generation algorithms (DGAs) to create domain names contacting the C&C server randomly. Fast-flux manipulates DNS bindings to change IPs mapped to C&C domains rapidly. These behaviours deviate from legitimate DNS traffic [13].

Machine learning has been applied to detect botnet DNS patterns using domain entropy, query counts, IP diversity, and time-series lookups.

Alkasassbeh & and Almseidin [14] developed a DNS-based botnet detection system comparing multiple machine learning classifiers on DNS tunneling data. Their results showed random forest achieving the highest accuracy for detecting DNS tunnelling compared to algorithms like J48 and multilayer perceptrons. Evaluating multiple classifiers demonstrated machine learning's capability to identify malicious DNS patterns. However, the scope was limited to DNS tunnelling data rather than diverse botnet traffic. Overall, the work highlights the promise of random forest models for DNS-based botnet detection. Extending the approach to other botnet detection tasks and datasets could further establish its capabilities.

Almomani et al. [15] proposed an ensemble-based system using max voting for classifying darknet traffic. Combining random forest, KNN, and gradient boosting classifiers, their approach attained 98.76% accuracy on the CIC-Dark2020 dataset. The ensemble method integrates the outputs from diverse models to improve performance over single classifiers. However, the technique focused exclusively on darknet traffic classification rather than general botnet detection applications. The study indicates that ensemble learning is a valuable strategy for boosting DNS-based botnet detection accuracy. Similar voting ensemble approaches on wider network traffic data could enhance real-world botnet detectors.

A limitation of DNS detection is the ability of advanced botnets to mimic legitimate traffic via domain caching and other evasion tactics. DNS analysis also misses alternative C&C communication methods. Table 3 summarizes key DNS-based botnet detection research.

Table 3. Summary of DNS-based botnet detection papers.

Authors	Method	Dataset	Results	Pros	Cons
Alkasassbeh & Almseidin**[14]**	Multiple classifiers	DNS tunneling data	High RF accuracy	Evaluated multiple models	Limited data

doi:10.20944/preprints202311.0311.v1

Authors	Method	Dataset	Results	Pros	Cons
Almomani et al. **[15]**	Voting ensemble	CIC-Dark2020	98.76% accuracy	Ensemble learning	Darknet traffic focused

The highlighted works demonstrate the effectiveness of ensemble learning and comparative classifier evaluations for improving DNS-based detection. However, limitations exist around darknet specificity and lack of diverse botnet data. In conclusion, DNS traffic analysis provides a valuable detection approach by identifying anomalous lookup patterns. The surveyed papers showcase applications of machine learning, especially ensemble methods, to extract useful DNS features. Further research should focus on expanding evaluation to general botnet datasets and real-world traffic. Applying deep learning for representational DNS data modelling also offers promise. Advancing DNS-based detection will require leveraging the full spectrum of modern machine-learning techniques.

2.4. Hybrid Detection

Hybrid detection combines multiple data sources like payloads, flows, and DNS to improve accuracy. The enriched features provide additional perspectives to identify heterogeneous botnet behavior's.

Alieyan et al. [16] evaluated a hybrid model merging DNS and flow features using various classifiers, including SVMs, Naive Bayes, and decision trees. Mashaleh et al.[8] proposed an early IoT botnet detection framework fusing packet and flow features classified with SVMs, attaining 97.3% accuracy.

A core challenge is the large feature space resulting from merged data sources, risking model overfitting. Careful feature selection is necessary to determine optimal hybrid feature subsets. Complex neural architectures are also required to fuse the diverse data types effectively.

Hybrid systems fuse diverse data sources such as payloads, flows, and DNS to enrich perspectives for detecting heterogeneous botnets. Table 4, summarizes key research on hybrid botnet detection approaches.

Table 4. Summary of hybrid botnet detection papers.

Authors	Method	Dataset	Results	Pros	Cons
Alieyan et al. [16]	SVMs, Naive Bayes, decision trees	DNS + flow features	Compared classifiers	Feature fusion	Focused on accuracy
Mashaleh et al.[8]	SVM classifier	Packet payload + flow data	97.3% accuracy	Deep learning on fused data	Single technique tested

The highlighted works demonstrate classifier comparisons and deep learning models for hybrid detection. Fusing DNS, flow, and payload data improves visibility into diverse botnets. However, limitations exist around single model evaluation and lack of focus on evasion robustness.

In conclusion, hybrid detection leverages complementary data sources to enhance visibility into heterogeneous botnets. The surveyed papers present initial applications of machine learning, including deep neural networks, for fusing and analyzing multi-modal data. Further research should concentrate on robustness against attacks, scalable streaming methods, and emerging deep learning architectures. Advancing hybrid detection requires fully utilizing the latest machine learning innovations.

2.5. Anomaly-based

Almseidin & Alkasassbeh [17] developed an anomaly based IoT botnet detection system using fuzzy rule interpolation. Their approach avoids binary decisions and provides interpretable outputs. Testing on an IoT botnet dataset yielded a 96.4% detection rate. However, fuzzy rule-based methods

doi:10.20944/preprints202311.0311.v1

face challenges with incomplete rule bases. Overall, interpolative fuzzy logic shows promise for enhancing anomaly detection and explainability.

Almseidin et al. [18] also applied fuzzy rule interpolation for detecting phishing website attacks. Their method can handle incomplete rule bases and smooth boundaries between normal and attack traffic. Evaluation on a phishing website dataset achieved 97.58% detection accuracy. While promising, the approach was tailored specifically for phishing attacks rather than general botnet detection. The interpolative reasoning enhanced robustness to rule base gaps.

Alkhamaiseh et al. [19] proposed a multistage one-class SVM model for anomaly-based detection of unknown attacks. Using the SNMP-MIB dataset, their approach combines wrapper and filter feature selection to train the SVM classifiers. In testing, 97% of unknown attacks were successfully detected. However, the multistage SVM model is relatively complex. The study demonstrates the potential of one-class methods for identifying novel attacks.

Almseidin et al. [20] developed an anomaly-based distributed denial-of-service (DDoS) attack detection system using fuzzy inference. Their approach aims to avoid binary decisions and provide human-interpretable outputs. Testing on a DDoS dataset yielded strong results of 96.25% accuracy and a 0.006% false positive rate. Fuzzy logic enhances the IDS alert system by delivering more nuanced attack assessments instead of binary decisions. However, a limitation is that the evaluation was restricted to a single DDoS dataset, and generalizability to other botnet types is unclear. Overall, the paper demonstrates the potential of fuzzy inference systems to improve anomaly-based botnet detection's robustness, explain ability, and precision. The interpolative reasoning capability enables the generating of alerts even with incomplete rule bases. Further research can build on this explainable AI approach for botnet detection across diverse datasets and attack types. Table 5 summarizes key research in this area.

Table 5. Anomaly detection approaches for botnet detection.

Authors	Method	Dataset	Results	Pros	Cons
Almseidin & Alkasassbeh [17]	Fuzzy rule interpolation	IoT botnet data	96.4% detection rate	Handles incomplete rules	Tailored to IoT
Almseidin et al. . [18]	Fuzzy rule interpolation	Phishing website data	97.58% accuracy	Smooths decisions	Specific to phishing
Alkhamaiseh et al. [19]	Multistage one-class SVM	SNMP-MIB data	97% unknown attack detection	Detects new threats	Complex model
Almseidin et al. [20]	Fuzzy inference	DDoS data	96.25% accuracy	Explainability	Single dataset

The highlighted works demonstrate the benefits of explainable models like fuzzy systems and one-class SVMs for detecting anomalies and unknown threats. Key limitations include specificity to attack types and model complexity.

In conclusion, anomaly detection provides an important paradigm for identifying zero-day botnet attacks. The surveyed papers showcase promising applications of interpretable machine learning models to enhance the detection of novel threats. Further research should improve model generalization, integration, and evaluation of diverse, real-world data. Overall, explainable anomaly detection exhibits significant potential for advancing botnet detection systems.

2.6. Machine Learning Algorithms

Key machine learning algorithms applied for botnet detection include:

- Support Vector Machines (SVMs): SVMs are widely used for botnet classification given their ability to handle high-dimensional data and learn complex decision boundaries, especially using kernel functions [4,8,9,15,16].

- Random Forests: Ensemble techniques like random forests overcome overfitting risks on limited samples by training collections of decision trees on bootstrapped data, providing variance reduction and inherent feature selection[15,21].
- Neural Networks: Various neural network architectures have been leveraged, including multilayer perceptrons for traffic analysis [1]
- Deep Learning: Deep neural networks, CNNs, and RNNs/LSTMs have representation learning capabilities useful for large, complex botnet datasets. Autoencoders enable unsupervised pre-training prior to botnet anomaly detection [14].

3. Challenges and Future Directions

Despite progress, key challenges remain in applying machine learning for botnet detection:

- Limited labelled datasets: Generating comprehensive labelled botnet data is difficult given rapid evolution of botnet techniques and privacy concerns with sharing network data [6]. Current datasets have limited diversity. Semi-supervised learning could help improve generalization.
- Adversarial evasion: Machine learning models are vulnerable to adversarial examples crafted to cause misclassification. Evaluating model robustness and adversarial training are important to deploy botnet detection [4].
- Encrypted traffic analysis: Widespread encryption protocols like TLS/SSL reduce the efficacy of payload-based detection. Methods to extract insights from encrypted metadata offer a promising direction [5].
- Real-time detection: Most systems are evaluated offline on static datasets. Enabling real-time detection on live streams requires addressing efficiency and incremental learning challenges [1].
- Explainability: Complex models like deep neural networks lack interpretability. Explainable AI techniques to provide human-understandable reasons for botnet classifications increase trust [12].

Due to the adversarial nature of botnets, models require continual retraining to detect modified botnet behaviors. Advances in adversarial machine learning could improve model robustness and generalization against deceptive attacks. Explaining complex models via methods like LIME and SHAP also enhances model transparency.

4. Discussion

Botnet detection is an important cybersecurity application of machine learning. Intelligent botnets capable of evolving their techniques pose a major threat to organizations and internet infrastructure. Traditional signature-based detection is inadequate against sophisticated botnets using polymorphism, encryption, and evasion tactics. Machine learning is essential for identifying new patterns and anomalies indicative of emerging botnet behaviour. However, effective application of machine learning for botnet detection introduces both research challenges and ethical considerations. On the research side, adversarially robust models must be developed amidst an arms race with increasingly evasive botnets. Scalable streaming algorithms are needed to enable real-time botnet detection on live network traffic. The lack of labeled training data also hampers the development of generalizable models. Responsible data-sharing protocols and synthesis techniques should be explored to generate representative botnet datasets without compromising user privacy. There are also ethical ramifications regarding how botnet detection systems are deployed. Network traffic monitoring and inspection could infringe on reasonable expectations of privacy. Transparent policies and processes should govern use of botnet data. Botnet alerts should be validated before triggering any restrictive actions. Explainable ML methods can increase trust and accountability in botnet response systems. A thoughtful approach balancing security, privacy, and ethics is required to develop machine learning-based solutions that responsibly combat the botnet problem.

5. Conclusion

In conclusion, this survey reviewed recent advances in applying machine learning for botnet detection, categorizing systems based on analysis of network payloads, flows, DNS, and hybrid data fusion. Diverse algorithms have been leveraged, including SVMs, neural networks, random forests, and deep learning models, to automatically extract artifacts that identify botnet behaviors amidst benign traffic. Results demonstrate machine learning's capabilities in surfacing heterogeneous botnet anomalies from monitored network streams. However, open challenges remain concerning limited labeled data, real-time streaming, adversarial evasion, and interpretability. Ongoing innovations in semi-supervised learning, adversarial training, scalable analytics, and explainable AI provide promising directions to address these gaps. Beyond technical research, responsible development and deployment of machine learning for botnet detection also raises ethical considerations around privacy, transparency, and accountability that warrant diligent cross-disciplinary collaboration. Overall, with thoughtful guidance across the machine learning, security, and ethics spheres, sophisticated machine learning techniques hold immense promise to enhance the detection, understanding, and mitigation of serious botnet threats across our increasingly digital world. This review aims to spur collaborative progress at the intersection of machine learning and cybersecurity to responsibly combat the global botnet scourge.

References

1. Alauthman, M.; Aslam, N.; Al-Kasassbeh, M.; Khan, S.; Al-Qerem, A.; Choo, K.-K.R. An efficient reinforcement learning-based Botnet detection approach. *Journal of Network and Computer Applications* **2020**, *150*, 102479.
2. Alieyan, K.; Almomani, A.; Anbar, M.; Alauthman, M.; Abdullah, R.; Gupta, B.B. DNS rule-based schema to botnet detection. *Enterprise Information Systems* **2021**, *15*, 545-564.
3. Lu, W.; Rammidi, G.; Ghorbani, A.A. Clustering botnet communication traffic based on n-gram feature selection. *Computer Communications* **2011**, *34*, 502-514.
4. Alsarhan, A.; Alauthman, M.; Alshdaifat, E.a.; Al-Ghuwairi, A.-R.; Al-Dubai, A. Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing* **2021**, 1-10.
5. Randhawa, R.H.; Aslam, N.; Alauthman, M.; Rafiq, H. Evasion generative adversarial network for low data regimes. *IEEE Transactions on Artificial Intelligence* **2022**.
6. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems* **2019**, *100*, 779-796.
7. Saad, S.; Traore, I.; Ghorbani, A.; Sayed, B.; Zhao, D.; Lu, W.; Felix, J.; Hakimian, P. Detecting P2P botnets through network behavior analysis and machine learning. In Proceedings of the 2011 Ninth annual international conference on privacy, security and trust, 2011; pp. 174-180.
8. Mashaleh, A.S.; Ibrahim, N.F.B.; Alauthman, M.; Almomani, A. A Proposed Framework for Early Detection IoT Botnet. In Proceedings of the 2022 International Arab Conference on Information Technology (ACIT), 2022; pp. 1-7.
9. Younisse, R.; Alkasassbeh, M.; Almseidin, M.; Abdi, H. AN EARLY DETECTION MODEL FOR KERBEROASTING ATTACKS AND DATASET LABELING. *Jordanian Journal of Computers and Information Technology* **2023**, *9*.
10. Alslman, Y.; Alkasassbeh, M.; Almseidin, M. A Robust SNMP-MIB Intrusion Detection System Against Adversarial Attacks. *Arabian Journal for Science and Engineering* **2023**, 1-17.
11. AlMasri, E.; Alkasassbeh, M.; Aldweesh, A. Towards Generating a Practical SUNBURST Attack Dataset for Network Attack Detection. *Computer Systems Science & Engineering* **2023**, *47*.
12. Qabalin, M.K.; Naser, M.; Alkasassbeh, M. Android spyware detection using machine learning: a novel dataset. *Sensors* **2022**, *22*, 5765.
13. Almomani, A.; Al-Nawasrah, A.; Alauthman, M.; Al-Betar, M.A.; Meziane, F. Botnet detection used fast-flux technique, based on adaptive dynamic evolving spiking neural network algorithm. *International Journal of Ad Hoc and Ubiquitous Computing* **2021**, *36*, 50-65.
14. Alkasassbeh, M.; Almseidin, M. Machine Learning Techniques for Accurately Detecting the DNS Tunneling. In Proceedings of the Science and Information Conference, 2023; pp. 352-364.
15. Almomani, A.; Alauthman, M.; Alkasassbeh, M.; Samara, G.; Liu, R.W. A Proposed Darknet Traffic Classification System Based on Max Voting Algorithms. In Proceedings of the International Conference on Cyber Security, Privacy and Networking, 2021; pp. 349-355.

16. Alieyan, K.; Anbar, M.; Almomani, A.; Abdullah, R.; Alauthman, M. Botnets detecting attack based on DNS features. In Proceedings of the 2018 International Arab conference on information technology (ACIT), 2018; pp. 1-4.
17. Almseidin, M.; Alkasassbeh, M. An Accurate Detection Approach for IoT Botnet Attacks Using Interpolation Reasoning Method. *Information* **2022**, *13*, 300.
18. Almseidin, M.; Alkasassbeh, M.; Alzubi, M.; Al-Sawwa, J. Cyber-Phishing Website Detection Using Fuzzy Rule Interpolation. *Cryptography* **2022**, *6*, 24.
19. Alkhamaiseh, A.; Alkasassbeh, M.; Al-Saraireh, J. Unknown Attack Detection Based on Multistage One-Class SVM. In Proceedings of the 2022 International Conference on Emerging Trends in Computing and Engineering Applications (ETCEA), 2022; pp. 1-9.
20. Almseidin, M.; Al-Sawwa, J.; Alkasassbeh, M.; Alweshah, M. On detecting distributed denial of service attacks using fuzzy inference system. *Cluster Computing* **2023**, *26*, 1337-1351.
21. Zhao, D.; Traore, I.; Sayed, B.; Lu, W.; Saad, S.; Ghorbani, A.; Garant, D. Botnet detection based on traffic behavior analysis and flow intervals. *computers & security* **2013**, *39*, 2-16.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.