Artificial Intelligence-Powered Data Analytics against Botnet Attacks: Threat Detection and Ethical Considerations

Ramazan KOCAOĞLU

Ostim Technical University

To Cite This Chapter

Kocaoğlu, R. (2024). Artificial Intelligence-Powered Data Analytics against Botnet Attacks: Threat Detection and Ethical Considerations. In M. Hanefi Calp & R. Bütüner (Eds.), *Current Studies in Data Science and Analytics* (pp. 86-96). ISRES Publishing.

Introduction

In today's digital world, botnet attacks pose serious threats to both individuals and organizations. Botnets allow cyber attackers to carry out large-scale attacks by capturing hundreds of thousands or even millions of devices under a network. These attacks usually involve destructive activities such as DDoS (Distributed Denial of Service), phishing, and spam, causing both financial and operational losses. The ever-increasing size of botnet attacks has necessitated the development of new and powerful methods that can effectively detect and block these threats.

Data analytics and artificial intelligence have the potential to revolutionize the security world in order to protect against botnet attacks (Owen et al., 2022) Data analytics enables tracing and predicting attacks by extracting meaningful patterns from the large amounts of data generated by botnet networks. In addition, artificial intelligence-based methods offer promising solutions to detect botnet attacks with techniques such as behavioral analysis, anomaly detection, and machine learning models. The ability of artificial intelligence to learn over large data sets makes it possible for this technology to adapt to constantly evolving and changing attack techniques.

However, the use of artificial intelligence against botnet attacks raises a number of ethical and technical issues. In particular, issues such as data privacy, the ethical acceptability of artificial intelligence models, and the potential damage that false positives can cause are critical areas that need to be carefully considered when developing such solutions (Stahl, 2021). In addition, how effective existing AI solutions can remain against evolving attack methods is another important element that should be discussed in long-term security strategies.

In this chapter, how AI-supported data analytics methods can be used against botnet attacks, the effectiveness of these technologies in security, the technical and ethical challenges encountered, and future development areas will be evaluated in detail. At the end of the chapter, in light of the solutions offered by artificial intelligence against botnet attacks, recommendations will be presented for future directions and the development of healthier solutions in this field.

Botnet Attacks and Threat Detection with Data Analytics

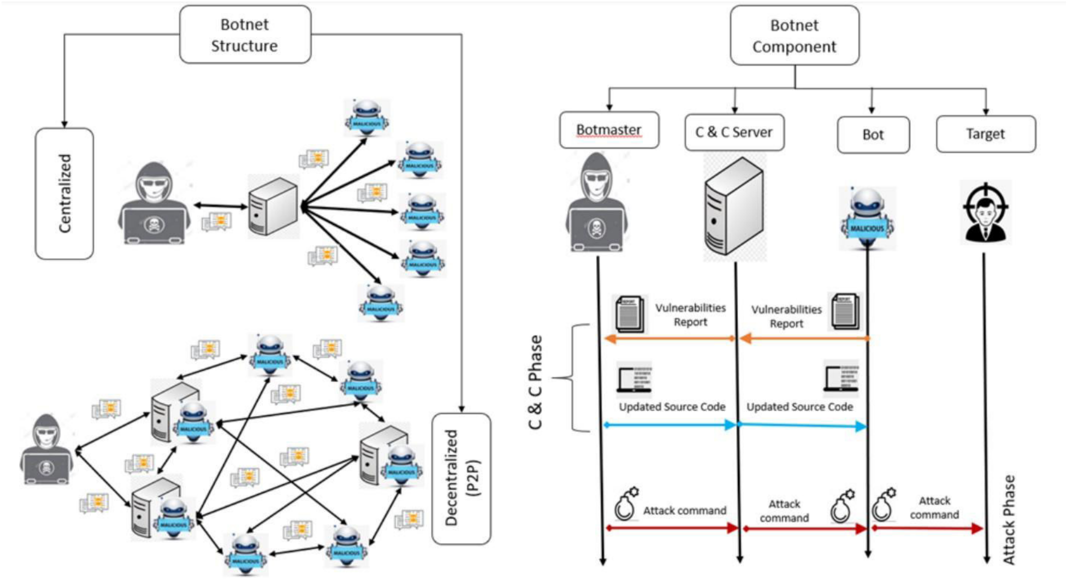
Botnet attacks, an important part of cyber security threats, pose a great risk in today's digital world. Botnets are a distributed network consisting of a large number of devices under the control of attackers and are generally used for purposes such as DDoS attacks, phishing, spamming, and malware propagation. Studies show that botnet attacks have increased rapidly in recent years and have reached much more dangerous dimensions (Ali et al., 2020).

A widely known instance of a botnet attack was the Mirai botnet incident in 2016 (Kambourakis et al., 2017). The Mirai botmaster performed reconnaissance on vulnerable Internet of Things devices connected to the target networks and subsequently deployed the malware against unprotected ports. As a result, the Mirai botnet infected over 600,000 IoT devices, utilizing them to mount a massive DDoS attack that disrupted access to popular websites like Netflix, Twitter, GitHub, and Reddit (Salim et al., 2019). The growing prevalence and sophistication of botnet attacks have necessitated the development of robust and adaptive security measures.

Botnets are large networks of a large number of devices that have been compromised by malware. These devices operate in a coordinated manner through a central command and control (C&C) center under the control of the attackers. The Bootnet structure is given in **Figure 1** (Ibrahim et al., 2022).

Figure 1

The Botnet Structure and Botnet Component



The operating structure and propagation mechanisms of botnets usually consist of the following components:

> *C&C Centre:* The main management center that allows attackers to command the entire bot network.
> *Bots:* Devices connected to the C&C center (computers, IoT devices, etc.) form the main components of the botnet.
> *Command Chain and Propagation:* Botnets attack their targets through commands. They are often spread through social engineering techniques such as malware emails or fake websites.

Botnets can be organized in different ways in terms of propagation and attack diversity. For instance, "Peer-to-Peer" botnets enable bots to communicate directly with one another without requiring a centralized command system, which makes them challenging to detect. These decentralized botnets are frequently employed in a variety of malicious activities, such as DDoS attacks, spamming, phishing, and malware distribution, posing a significant threat to digital security. Unlike traditional botnets with a centralized command and control structure, peer-to-peer botnets are more resilient and adaptive, as they can continue to function even if individual nodes are taken down. This distributed nature makes them particularly difficult to disrupt and monitor, further exacerbating the security challenges they pose.

Data analytics plays a critical role in security strategies to detect and block botnet attacks (Xing et al., 2021). Botnets leave a certain trace by constantly exhibiting abnormal behavior in network traffic, and data analytics can extract these traces from large data sets. The contributions of data analytics in detecting botnet attacks are as follows :

> *Anomaly Detection:* Botnet attacks often generate anomalous traffic patterns. Data analytics algorithms can identify such anomalies and generate alarms for security systems. For example, activities such as excessive connection requests or unusual data transfer can be quickly detected with data analytics tools (Ahmad et al., 2022).
>
> Behavioral Analysis: Data analytics can predict the attack activity of botnets by analyzing user and device behavior. Botnets often exhibit specific communication patterns, which can be identified through deep inspection of network traffic and device logs. Early warning systems can be established by performing communication detection analysis of bot patterns (Analysis of Botnet Attack Communication Pattern Behavior on Computer Networks, 2022).
>
> *Pattern Recognition and Machine Learning:* In defense systems against botnet attacks, attack patterns are determined with machine learning models (Yang et al., 2022). These models can detect new threats faster by learning from past botnet attacks. Especially in DDoS attacks, botnet-based attacks can be monitored more effectively with machine learning algorithms.

These advantages of data analytics strengthen digital security by detecting botnets and reducing the potential for attacks. However, processing large amounts of data and performing real-time analyses can pose both technical and ethical challenges. Nevertheless, data analytics remains an essential component of modern cybersecurity strategies against botnets.

The Effectiveness of Artificial Intelligence Methods in Botnet Detection

Artificial intelligence-based data analytics offers a powerful solution for the detection of botnet attacks, especially through the use of machine learning and deep learning models. In this chapter, the main artificial intelligence methods used in the detection of botnet threats and the effectiveness of these methods will be discussed.

Machine Learning and Botnet Detection

Machine learning provides effective results with classification and clustering techniques commonly used to detect botnet attacks. These techniques allow us to distinguish and categorize botnet activities thanks to algorithms trained on historical data (Yang et al., 2022).

> *Classification Algorithms:* Classification algorithms are used to distinguish botnet traffic from normal network traffic. Classifiers classify the samples in the data set into certain classes in order to predict botnet-based attacks. For example, methods such as Naive Bayes, Support Vector Machines (SVM), and Decision Trees are frequently preferred to detect DDoS attacks. However, classification models have a margin of error such as false positives and false negatives, and the accuracy rate depends on the data quality and the training of the model.

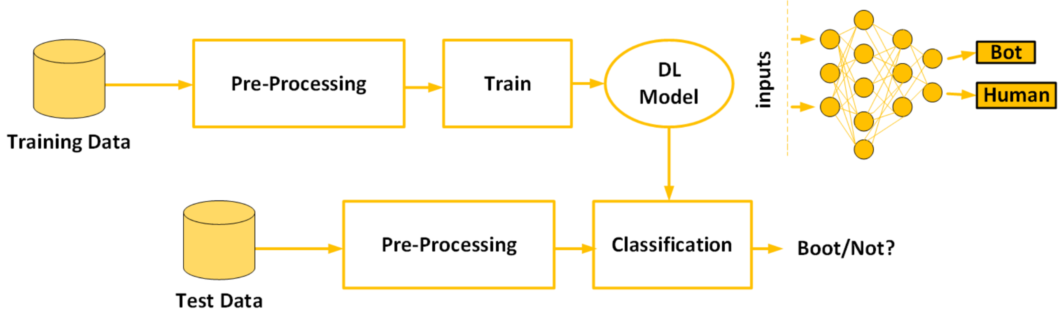
Clustering Techniques: Clustering methods aim to create anomalous clusters in the data set by bringing together similar data points. Clustering, one of the unsupervised learning techniques, is effective in distinguishing botnet activities in previously unlabelled data sets. Methods such as K-Means and Hierarchical Clustering identify the points where botnet activities are concentrated and compare them with normal traffic. However, it can be challenging to correctly identify clusters based on data density and attack type.

Machine learning models enable faster detection of botnet attacks by processing large amounts of data. However, the lack of sufficient data labels, the complexity of attacks, and rapidly changing attack techniques require machine learning-based models to be updated.

Detection with Deep Learning Models

Deep learning is an important method in botnet detection with its capacity to process large amounts of data and its ability to detect complex attack patterns (Yerima et al., 2021). In particular, neural network-based deep learning models perform effectively in large datasets. Figure 2 shows the general steps for using deep learning to detect bots. First, the data is cleaned up by labeling, expanding, and extracting features. This prepared data is then used to train a deep-learning model. Finally, the trained model is used to classify whether users in new data are human or bots.

Figure 2
A Generalized Workflow Diagram DL-Based Bot Detection



Artificial Neural Networks (ANN) and Recurrent Neural Networks (RNN): ANN and RNN are effective in identifying relationships between events by processing temporal data of botnet attacks. RNNs analyze how botnet behavior can be related to past events, especially in time series data.

Convolutional Neural Networks (CNN): CNN is a powerful method for identifying botnet attack traces in network traffic data. CNN, which is often used for image and pattern recognition, can extract data from network traffic to distinguish the specific traffic of botnet attacks.

Although deep learning models have high accuracy rates in botnet detection, they require a large data processing capacity. Preparation, modeling and training of datasets require large amounts of time and computational power. Furthermore, deep learning models, while offering high accuracy, can be of limited use in real-time applications due to excess complexity.

Anomaly Detection Methods

Anomaly detection is based on detecting botnet attacks through unusual network activities. Identifying activity that deviates from normal network behavior is an effective method for botnet detection. This method can be achieved by various algorithms:

Statistical Methods: For the detection of botnet attacks, statistical deviations from normal are analyzed. For example, abnormal behavior, such as a device making more connections than expected, can be determined by statistical anomaly detection (Ashraf et al., 2021).

Machine Learning-Based Anomaly Detection: Anomaly detection methods supported by classification algorithms are used to find anomalous patterns of suspicious activity in data sets. Isolation Forest is one of the common anomaly detection methods used to detect botnet attacks (Borges et al., 2023). This algorithm signals botnet activities by extracting unusual points in the data set.

Time-Series Based Anomaly Analysis: The fact that botnet attacks lead to continuous traffic makes it easy to detect anomalies with time-series analysis. Time series analysis methods can identify attack symptoms by capturing the behavioral patterns of botnets over time(Borges et al., 2023).

Anomaly detection is effective in predicting botnet attacks; however, a high false positive rate may lead security teams to receive unnecessary alarms. Therefore, anomaly detection models should be fine-tuned according to the data set and network traffic characteristics.

Ethical and Social Aspects of Artificial Intelligence Methods in Botnet Detection

Artificial intelligence-based security solutions play an important role in the detection and prevention of botnet attacks. However, it is necessary to consider the ethical and social dimensions of the use of these systems. In this section, the ethical and social issues of AI-based botnet detection systems, such as data privacy, fairness, and regulations, will be discussed.

Data Privacy and Security Concerns

AI-based security solutions detect botnet threats by analyzing large amounts of data, raising concerns about personal data privacy and data security. AI algorithms used for botnet detection monitor users' online activities, network traffic patterns, and other sensitive data. Privacy and security issues come to the forefront in these data analysis processes:

Data Privacy Breaches: Data collected for the training of artificial intelligence models may contain users' personal information. Threats to user privacy arise, particularly when analysing sensitive data such as network traffic. Storing personal data in AI systems increases the risk of misuse through data breaches and cyber-attacks.

Vulnerabilities: The security of AI systems must be resilient against botnet attacks. However, the vulnerabilities of artificial intelligence models themselves can reduce the reliability of these systems. For example, the effectiveness of security solutions can be jeopardized if attackers infiltrate the model training process and manipulate the model (adversarial attacks).

These concerns require AI-based botnet detection systems to adopt a more transparent and privacy-oriented approach to data collection and storage. If data security is not ensured, ethical commitments to protect users' privacy may be violated (Dhirani et al., 2023).

False Alarms and Justice Issues

The false positive rates of AI algorithms in botnet detection pose ethical and social challenges. In particular, false positive alarms can lead to innocent users being unjustly associated with botnet activity and may create injustice.

The Impact of False Positives: Artificial intelligence algorithms used in botnet detection may sometimes mistakenly recognize normal user activity as a botnet attack. This can cause innocent users to be subjected to unnecessary security reviews. For example, network activity of a business that generates heavy network traffic may be incorrectly interpreted as botnet activity. A high number of false positives can cause security teams to spend unnecessary time and users to be unfairly blamed.

Fairness Issues and Model Biases: In order for AI-based security systems to make fair decisions, imbalances in data sets should be considered during the training of models. For example, if user data from certain geographical areas or demographic groups is analyzed more, these groups may be targeted more than others. This may be contrary to principles of social justice and may result in users being unfairly discriminated against by certain groups.

In order to fulfill ethical commitments in terms of fairness and accuracy, it is important to balance the precision and accuracy of AI algorithms, reducing false positives and ensuring the impartiality of algorithms.

Regulations and Policies for Artificial Intelligence Applications

Various regulations and policies are required to fulfill ethical responsibilities during the development and implementation of AI-based botnet detection systems. Such regulations encourage the use of artificial intelligence in the security sector in accordance with ethical principles.

Existing regulations: Today, general data protection regulations, such as GDPR, are in place to protect data privacy. Such regulations oblige artificial intelligence systems to protect user privacy in data collection and analysis processes. However, there is no direct regulation for specific security applications such as botnet detection.

Proposed Regulations: New policies are proposed to increase the transparency and fairness of AI applications. For example, algorithmic transparency allows users to understand how their data is used and what decision processes it influences. It is also recommended to develop standardized testing processes to reduce false positive rates and protocols to ensure algorithm reliability.

Implementation of Ethical Principles and Policies: To ensure ethical commitments in the security applications of AI, policies should cover not only technical standards but also values such as transparency, fairness, and trustworthiness. This aims to ensure that AI-based systems provide effective protection against botnet attacks while protecting user rights.

The effective implementation of these regulations and policies will contribute to the ethical development and reliability of AI-based botnet detection solutions.

Technical Challenges in Artificial Intelligence-Based Botnet Detection

While AI-supported botnet detection systems offer powerful solutions in the field of cyber security, they also face various technical challenges (Zhang et al., 2021). These challenges can affect the accuracy and effectiveness of the systems and make it difficult to develop real-time and adaptive solutions to botnet attacks. In this section, we will discuss the main technical obstacles faced by artificial intelligence applications in botnet detection.

Data Quality and Labelling Problems

In order for artificial intelligence models to accurately detect botnet attacks, high-quality and comprehensive training data is required. However, data quality and data labeling problems are important technical obstacles that directly affect model performance.

Missing or Low-Quality Data: Missing or poor-quality data for botnet attacks makes it difficult for the model to accurately learn attack types. Inadequate data can reduce the reliability of the model, causing it to fail to correctly identify attack patterns. For example, failure to obtain complete network traffic data may lead to missing salient characteristics of botnet activity.

Labelling Problems: Machine learning models need to be trained with correctly labeled data. However, in cybersecurity incidents such as botnet attacks, accurate labeling can be difficult because attacks are complex and constantly evolving. Incorrect or incompletely labeled data can increase the false positive and false negative rates of the model and lead to erroneous results.

Overcoming data quality and labeling problems necessitates the improvement of data collection processes for botnet detection and the use of more advanced labeling methods.

Real-time Detection and Performance Problems

Detecting botnet attacks in real-time is a major technical challenge, especially considering the need to deal with large-scale data sets and high-speed network traffic. This puts pressure on the processing power and performance of AI models.

Large-Scale Data Processing: Most botnet attacks can be hidden in large chunks of data. Especially in large-scale attacks such as DDoS, it is necessary for systems to analyze large amounts of data in real time. However, analyzing large data sets on the fly requires high processing power and memory, which can slow or limit system performance.

Real-time Analysis Requirement: Botnet attacks may require an immediate response; otherwise, the damage can grow rapidly. However, artificial intelligence models may experience delays while performing complex calculations on large amounts of data. In particular, deep learning models may encounter performance problems in real-time analyses due to computational intensity.

In order to overcome such performance problems, the development of lightweight and fast-running models or the use of methods such as parallel processing can facilitate real-time results in AI-based botnet detection.

Adaptation and Update Requirements

Botnet attacks are constantly evolving, developing new techniques and increasing their ability to circumvent security measures. Therefore, AI-based systems need to be regularly updated to adapt to the current state of the attacks.

Adaptation to Evolving Attack Techniques: New variations of botnet attacks can differ from traditional attack techniques. AI models need to be regularly retrained or updated to identify these changes and detect new threats. However, updating the models in this way requires continuous reconfiguration of the data collection and processing processes.

Need for Dynamic Updating: Artificial intelligence models must be dynamically updated to learn about changes in attack types. However, this process is costly in terms of both time and processing power and may affect the uptime of systems. In addition, the constant change in attacks necessitates periodic retraining of artificial intelligence models in order to maintain their accuracy in the long term.

Adaptation and updating needs constitute an important requirement for AI-based botnet detection systems to keep up with attack dynamics. In order to overcome these problems, innovative solutions such as online learning methods and continuously updated model structures are being studied.

Future Perspectives: Artificial Intelligence and the Evolution of Botnet Attacks

Emerging developments in artificial intelligence technologies may offer powerful solutions for detecting and preventing botnet attacks. In particular, advancements in algorithms and hardware can enhance the impact of AI systems in the security domain.

Advanced Deep Learning Models: Researchers are developing deeper and larger-scale neural networks that demonstrate high accuracy in botnet detection. For instance, Transformer-based models and graph-based neural networks have the potential to more precisely recognize botnet behavior patterns. Such advanced algorithms can provide more accurate detections by effectively processing extensive datasets.

Autonomous Learning Systems: AI can adapt to evolving threats through autonomous learning systems. Specifically, AI models supported by techniques like Reinforcement Learning can generate more effective solutions against botnet attacks by self-learning.

Quantum Computing and AI: Developments in quantum computing could revolutionize AI-based botnet detection in the future. Quantum computing can quickly analyze much larger datasets, enabling real-time threat detection. This capability can help more effectively block large-scale botnet attacks.

In the coming years, new artificial intelligence-supported developments are expected in areas such as autonomous systems in the detection of botnet attacks, threat intelligence, and real-time analysis. These developments can provide both more integrated and more effective solutions in the field of security.

Autonomous Defence Systems: In the future, AI-enabled botnet detection systems will be able to operate autonomously without human intervention. These systems can provide faster and more effective defense by recognizing and responding to attacks in real-time. For example, artificial intelligence algorithms integrated with systems such as firewalls or IPS (Intrusion Prevention Systems) can automatically trigger and block the attack at the time of attack.

Integration with Threat Intelligence Systems: AI-powered botnet detection will become part of a broader security network in the future by integrating with threat intelligence systems. Such integrated systems can quickly recognize the first signs of botnet attacks by analyzing threat information on a global scale and transferring threat information to other security elements.

Real-Time and Advanced Algorithms: By making artificial intelligence algorithms faster and more effective, the real-time analysis capacity will increase. Thus, botnet attacks can be detected as soon as they start and can be stopped before the attack spreads. Real-time detection will provide higher accuracy rates, especially in large-scale and complex attacks.

Ethics and Safety Best Practices

Determining ethical and technical best practices in the use of artificial intelligence against botnet attacks is of great importance for ensuring security and protecting ethical rules. These practices ensure the effective and responsible use of AI-based security solutions.

Transparency and Accountability: It is important to inform users about what data AI systems use and what kind of analysis they perform when detecting botnets. Transparency has become an ethical imperative for both the protection of user privacy and the reliability of the system. Accountable AI applications also provide an important safety net to protect users as a result of faulty decisions.

Reducing False Positives: Reducing the false positive rates of AI systems in botnet detection is critical to improving the user experience. Unjustifiably associating users with botnet activity due to false positives can lead to trust issues. Best practices should include verification techniques and multi-layer verification mechanisms to minimize false positive rates.

Data Privacy and Security: User data must be protected in AI-based security solutions. Best practices such as data anonymization, data minimization, and processing only the data that is necessary should be adopted to reduce the risk of privacy breaches. In addition, security measures should be increased to ensure that user data is stored securely and not shared.

The implementation of these best practices will enable AI-based security systems to develop within the framework of ethical rules and increase user security. In the future, these principles will contribute to the evolution of artificial intelligence systems to benefit society by creating a more effective and reliable defense mechanism against botnet attacks.

Conclusion

Artificial intelligence-supported data analytics stands out with its various advantages in detecting and preventing botnet attacks. Its ability to quickly and accurately analyze large-scale data sets allows it to quickly detect a large number of botnet activities. In addition, methods such as machine learning and deep learning offer strong performance in recognizing patterns specific to botnet attacks and supporting automatic threat detection processes based on these patterns.

However, AI-supported botnet detection solutions have some limitations. First of all, high-quality and comprehensive training data is needed for AI models to be successful. Lack of data, low-quality data, or mislabelled data may negatively affect model accuracy. In addition, as botnet attacks constantly evolve and develop new ways against security systems, it is imperative that artificial intelligence systems adapt quickly to these changes. This adaptation need can be costly in terms of time and resources, as it requires constantly updated and evolving structures.

There are important opportunities for the development of artificial intelligence-based systems against botnet attacks. In particular, advances in areas such as advanced learning algorithms, autonomous threat detection systems, and real-time analysis capabilities will increase the effectiveness in this area and make security stronger.

The evolution of botnet attacks and the future of artificial intelligence-supported solutions against these attacks offer new perspectives in the field of security. In the future, it is expected to develop systems that are more autonomous, flexible, and capable of real-time analyses. Furthermore, with the integration of quantum computing and advanced deep learning algorithms into this field, artificial intelligence models with much more powerful data processing capacity may emerge.

With the advancement of the adaptive learning capabilities of artificial intelligence, systems used in botnet detection will become more resilient to dynamic attacks. In addition, ethical and security best practices are expected to gain more importance in this field. Issues such as data privacy, false positives, and fairness will be among the most important components of AI-supported security solutions in the future.

In conclusion, there are both technical and ethical development opportunities in the field of AI-based botnet detection. The development of technological innovations and applications in this field will continue to provide stronger, reliable, and ethical solutions in the field of cyber security.

References

Ahmad, S., Jha, S., Alam, A., Alharbi, M., & Nazeer, J. (2022, May 12). Analysis of Intrusion Detection Approaches for Network Traffic Anomalies with Comparative Analysis on Botnets (2008–2020). Hindawi Publishing Corporation, 2022(undefined), 1-11. https://doi.org/10.1155/2022/9199703

Ali, I., Ahmed, A I A., Almogren, A., Raza, M A., Shah, S A., Khan, A., & Gani, A. (2020, January 1). Systematic Literature Review on IoT-Based Botnet Attack. Institute of Electrical and Electronics Engineers, 8(undefined), 212220-212232. https://doi.org/10.1109/access.2020.3039985

Analysis of Botnet Attack Communication Pattern Behavior on Computer Networks. (2022, June 24). Intelligent Networks and Systems Society, 15(4). https://doi.org/10.22266/ijies2022.0831.48

Ashraf, J., Keshk, M., Moustafa, N., Abdel-Basset, M., Khurshid, H., Bakhshi, A D., & Mostafa, R R. (2021, May 25). IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Elsevier BV, 72, 103041-103041. https://doi.org/10.1016/j.scs.2021.103041

Borges, J B., Medeiros, J P S., Barbosa, L P A., Ramos, H S., & Loureiro, A A F. (2023, December 1). IoT Botnet Detection Based on Anomalies of Multiscale Time Series Dynamics. IEEE Computer Society, 35(12), 12282-12294. https://doi.org/10.1109/tkde.2022.3157636

Dhirani, L L., Mukhtiar, N., Chowdhry, B S., & Newe, T. (2023, January 19). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Multidisciplinary Digital Publishing Institute, 23(3), 1151-1151. https://doi.org/10.3390/s23031151

Ibrahim, W N H., Anuar, M S., Selamat, A., & Krejcar, O. (2022, January 4). BOTNET DETECTION USING INDEPENDENT COMPONENT ANALYSIS. IIUM Press, International Islamic University Malaysia, 23(1), 95-115. https://doi.org/10.31436/iiumej.v23i1.1789

Kambourakis, G., Kolias, C., & Stavrou, A. (2017, October 1). The Mirai botnet and the IoT Zombie Armies. https://doi.org/10.1109/milcom.2017.8170867

Owen, H., Zarrin, J., & Pour, S M. (2022, February 28). A Survey on Botnets, Issues, Threats, Methods, Detection and Prevention. Multidisciplinary Digital Publishing Institute, 2(1), 74-88. https://doi.org/10.3390/jcp2010006

Salim, M M., Rathore, S., & Park, J H. (2019, July 10). Distributed denial of service attacks and its defenses in IoT: a survey. Springer Science+Business Media, 76(7), 5320-5363. https://doi.org/10.1007/s11227-019-02945-z

Stahl, B C. (2021, January 1). Ethical Issues of AI. Springer International Publishing, 35-53. https://doi.org/10.1007/978-3-030-69978-9_4

Xing, Y., Shu, H., Zhao, H., Li, D., & Guo, L. (2021, April 14). Survey on Botnet Detection Techniques: Classification, Methods, and Evaluation. Hindawi Publishing Corporation, 2021, 1-24. https://doi.org/10.1155/2021/6640499

Yang, X., Guo, Z., & Mai, Z. (2022, July 1). Botnet Detection Based on Machine Learning. , 2018(undefined), 213-217. https://doi.org/10.1109/icbctis55569.2022.00056

Yerima, S Y., Alzaylaee, M K., Shajan, A., & Vinod, P. (2021, February 23). Deep Learning Techniques for Android Botnet Detection. Multidisciplinary Digital Publishing Institute, 10(4), 519-519. https://doi.org/10.3390/electronics10040519

Zhang, Z., Ning, H., Shi, F., Farha, F., Yang, X., Xu, J., Fan, Z., & Choo, K R. (2021, March 13). Artificial intelligence in cyber security: research advances, challenges, and opportunities. Springer Science+Business Media, 55(2), 1029-1053. https://doi.org/10.1007/s10462-021-09976-0

About the Author

Dr. Ramazan KOCAOĞLU, completed his PhD in Computer Engineering at Gazi University in 2017. In addition to completing many projects and providing consultancy services in the public and private sectors with the company he founded in 2018, he continues to produce products and solutions that can meet the needs of the IT sector. He is a project manager in TUBITAK 1501 and 1507 Industrial R&D Projects Support Programs. He continues his academic studies as an assistant professor at Ostim Technical University Computer Engineering Department. His research areas mainly include Next-generation Wireless Communication, Computer Network, Software Defined Network, Internet of Things (IoT), Vehicular Ad-hoc Network, Sensor Network, Mesh Network, Nano Network, Cyber Security, Open Source Systems, Intelligent Optimization Techniques.

E-mail: ramazan.kocaoglu@ostimteknik.edu.tr, **ORCID:** 0000-0002-6554-3335

Similarity Index

The similarity index obtained from the plagiarism software for this book chapter is 6%.