Mitigating Cybersecurity Threats in Modern Networks Using Intelligent Approach

Mahmoud A. Zaher[1]*, Yahia B. Hassan[2] , Nabil M. Eldakhly[3]

[1] Faculty of Artificial Intelligence, Data Science department, Egyptian Russian University (ERU), Cairo, Egypt
[2] Electrical Eng. Dept, Higher Institute of Engineering, Minia, Egypt,
[3] Faculty of Computers and Information, Sadat Academy for Management Sciences, Cairo, Egypt &
French University in Cairo, Egypt
Emails: mahmoud.zaher@eru.edu.eg; dryahiabahaahassan@gmail.com; nabil.omr@sadatacademy.edu.eg

Abstract

The proliferation of botnet threats within Internet of Things (IoT) networks has underscored the critical need for robust detection mechanisms. This study addresses this imperative by presenting a comprehensive framework employing Machine Learning (ML) techniques for botnet detection. Leveraging a dataset sourced from authentically compromised IoT devices, the research delves into the intricate behaviors exhibited by botnets, emphasizing the encounters pretended by their polymorphic characteristics. A convolutional neural network architecture, featuring stacked layers with residual connections, serves as the cornerstone of the proposed detection system. The efficiency of the developed model is evaluated using meticulous visualization of data insights, learning behaviors, and detection performance, which demonstrate a great ability to discriminate between different botnet activities. This study presents a prominent improvement to the cybersecurity field by developing an effective solution for invigorating IoT network defenses against developing botnet threats, which highlights the essential role of ML-driven methods in the preservation of the integrity of interconnected devices.

Keywords: Cybersecurity; Network Security; Intrusion Detection; Anomaly Detection; Machine Learning (ML); Threat Detection; Behavioral Analysis.

1. Introduction

Network infrastructures worldwide are at risk from increasingly sophisticated cybersecurity threats. Botnets are one of the most dangerous of these threats, using compromised devices to carry out malicious activities. Botnets operate in a stealthy manner and enable various cybercrimes such as distributed denial-of-service (DDoS) attacks and data breaches, hence the need for strong detection mechanisms [1]. Traditional security approaches often fail to counter changing botnet tactics, necessitating the exploration of new methodologies. In this regard, Machine Learning (ML) techniques can be used to improve botnet detection because they can adapt and identify complex patterns in network traffic [2-3]. Botnets are intricate networks of compromised devices that are controlled by a central command and exhibit dynamic behaviors that cannot be detected by conventional signature-based systems. Their polymorphic nature is constantly changing to avoid being identified which poses a significant challenge to cybersecurity professionals [4]. This problem requires a shift in thinking towards proactive and adaptable detection strategies. ML offers a transformative approach by enabling systems to learn from data, identify anomalies, and classify patterns, thereby fortifying defenses against these elusive botnet incursions [5].

This research aims to develop an advanced security mechanism that uses Machine Learning to detect and mitigate botnet activities in network environments. The study recognizes the importance of strengthening digital infrastructures against increasingly sophisticated threats and therefore seeks to provide a comprehensive framework for effectively detecting and preventing botnet incursions [6-9]. This research combines the power of Machine Learning algorithms with a deep understanding of botnet behaviors, thus enhancing existing security measures and reducing the impact of

DOI: https://doi.org/10.54216/IJWAC.070204
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

these pervasive cyber threats. The importance of this research goes beyond traditional security paradigms into proactive threat mitigation. This study integrates Machine Learning techniques to overcome the limitations of traditional rule-based approaches that often fail to detect polymorphic and zero-day botnet attacks [10-11]. The aim of this research is to use ML's adaptive capabilities to improve the agility and accuracy of botnet detection systems, thus strengthening network defenses and reducing the possible cascading effects of cyber threats on critical infrastructures.

2. The proposed Work

This section explains the comprehensive framework used to design, prepare, and implement the botnet detection mechanism using Machine Learning techniques. The preparation of BoTNet data involved a series of steps that were carefully followed to ensure its relevance and reliability in our study. Initially, raw network traffic data collected from the 9 infected IoT devices compromised by Mirai and BASHLITE was gathered authentically [12-15]. This was followed by a comprehensive preprocessing phase involving data cleaning, feature extraction, and normalization procedures. Irrelevant or redundant attributes were removed while relevant features were extracted to form the basis of the dataset. The dataset then underwent a rigorous normalization process aimed at standardizing values and reducing biases thus ensuring uniformity across features. Missing values were handled with care so as not to compromise data integrity or lose information; this included imputation or exclusion depending on the context. This careful preparation phase was meant to optimize the dataset for subsequent analysis and model development, making it suitable for robust botnet detection through ML methodologies [16].

The proposed architecture comprises multiple convolutional layers with residual connections, fostering deeper network learning while mitigating vanishing gradient issues (see Figure 1). Let's denote the input to the convolutional layer at depth l as $x^{(l)}$, and the output as $H(x^{(l)})$. The residual connection is represented as $F(x^{(l)})$, allowing the network to learn residual mappings. Mathematically, the residual connection for a layer l is formulated as:

$$x^{(l+1)} - H(x^{(l)}) + F(x^{(l)}) \qquad (1)$$

Each convolutional layer l consists of filter weights $W^{(l)}$, biases $b^{(l)}$, and activation functions $\sigma(\cdot)$. The output of a convolutional layer can be computed as:

$$H(x^{(l)}) - \sigma(W^{(l)} * x^{(l)} + b^{(l)}) \qquad (2)$$

In botnet detection, a general choice is the categorical cross-entropy loss function due to its effectiveness in binary classification tasks [17-19].

$$L_{CCE} = \frac{1}{N}\sum_{i=1}^{N} \sum_{c=1}^{C} 1_{y_i \in C_c} \log a_{model}(y_i \in C_c) \qquad (3)$$

In the above expression, N denote the number samples, C represent number of botnet classes, $y_i \in C_c$ term suggests the $i-th$ remark that have its place $c-th$ class.

3. Experimental Design

This section outlines the structured approach adopted to assess the efficacy and robustness of the implemented system. We employ a variety of performance measures to assess our mode's detection capacity.

$$\text{Precision} = \frac{TP}{TP + FP} \qquad (4)$$

$$\text{Recall(Sensitivity)} = \frac{TP}{TP + FN} \qquad (51)$$

$$\text{Specificity} = \frac{TN}{TN + FP} \qquad (6)$$

$$\text{F1} - \text{score} \ \frac{2 \times Precision \times Recall}{Precision + Recall} \qquad (7)$$

DOI: https://doi.org/10.54216/IJWAC.070204
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

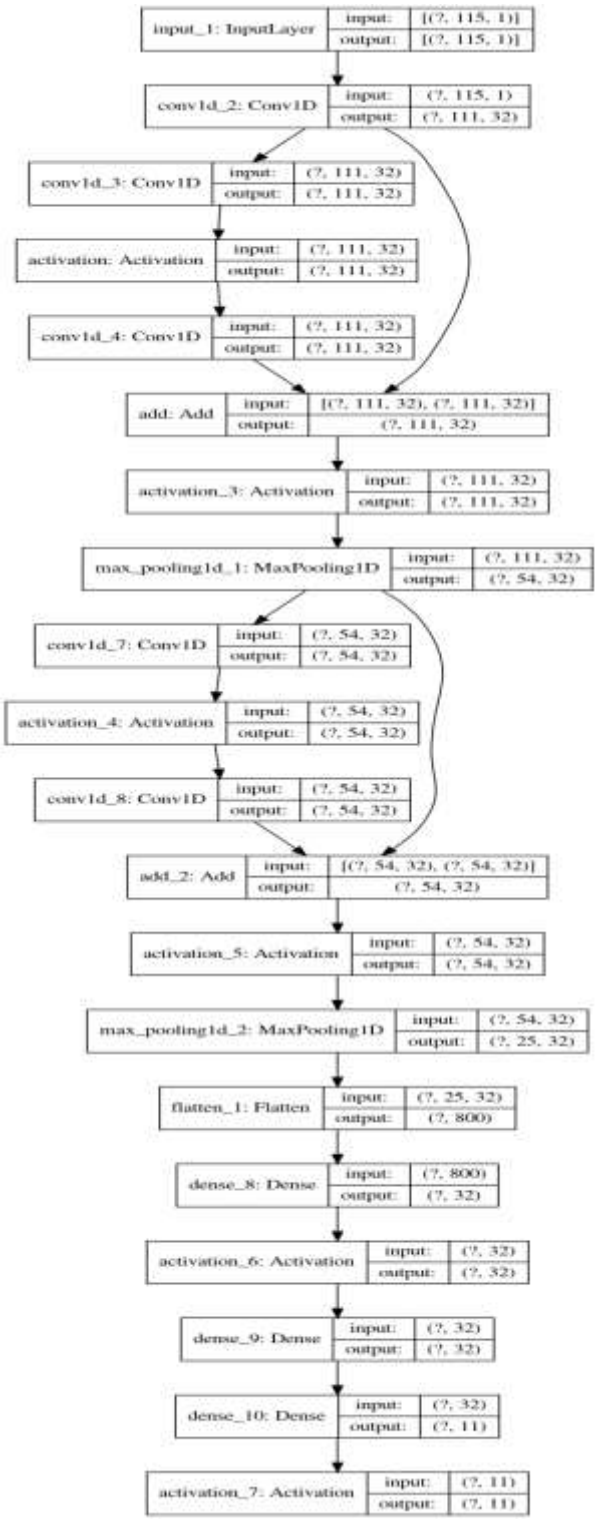

Figure 1: Architecture of the developed CNN

The dataset used in this work is a valuable addition to the public resources that are available, and it specifically addresses the lack of botnet datasets in the Internet of Things (IoT) domain. It consists of real traffic data from nine

DOI: https://doi.org/10.54216/IJWAC.070204
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

different IoT devices that were compromised by Mirai and BASHLITE malware strains. This dataset is very useful for studying and understanding botnet activities within IoT networks as it provides a realistic representation of infected IoT device behavior. The dataset is multivariate, sequential, and large with 7,062,606 instances. It has 115 real-numbered attributes spanning various domains making it an extensive resource for analysis and exploration. The dataset was contributed on March 19, 2018, as a foundational resource for classification and clustering tasks in cybersecurity [20].

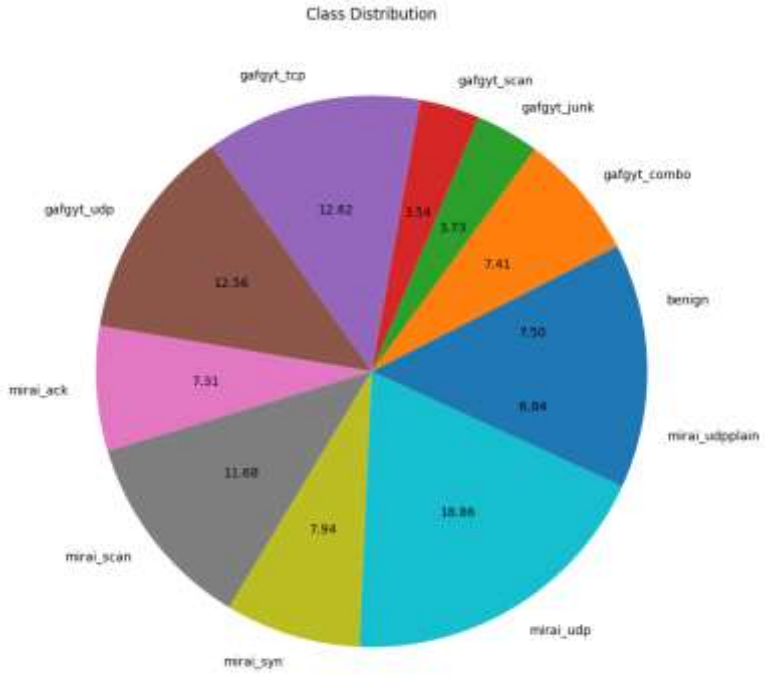

Figure 2: Distribution of Botnet and Non-Botnet Instances in the IoT Traffic Dataset

4. Results and Discussion

This section provides an in-depth analysis of the obtained results, juxtaposing them against predefined benchmarks and industry standards. Additionally, this section serves as a platform for interpreting the findings, elucidating the implications of the outcomes on bolstering network security and addressing the persistent challenges posed by botnet activities.

In Figure 2, we provide a comprehensive visualization depicting the class distribution within the dataset, offering a graphical representation of the frequency and proportion of different classes or categories present. The displayed chart serves as a crucial tool in understanding the imbalance or balance among various classes, shedding light on the distribution of botnet and non-botnet instances within the dataset. By presenting this class distribution graphically, Figure 1 offers a clear and concise portrayal of the relative prevalence of different classes, facilitating a deeper comprehension of the dataset's composition and aiding in informed decision-making regarding modeling strategies and algorithmic approaches for botnet detection and classification tasks.

DOI: https://doi.org/10.54216/IJWAC.070204
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

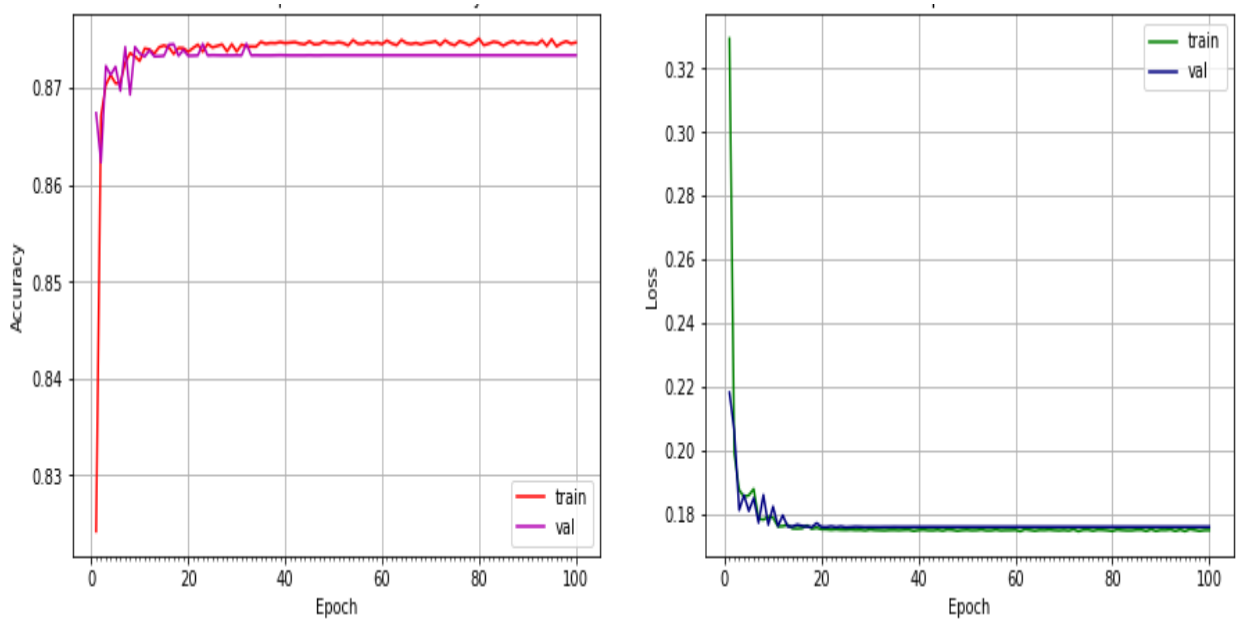

Figure 3: Learning Curves depicting Model Performance with Dataset Size/Iterations in Botnet Detection

Figure 3 presents learning curves that visually show how the model performs in terms of accuracy or loss with respect to dataset size or number of iterations during training. These learning curves provide useful insights into the model's convergence, generalization, and possible problems such as overfitting or underfitting when the dataset size or iterations change. Figure 2 shows these learning curves, which help to analyze the model's learning behavior, evaluate its performance, identify optimal training sizes, and comprehend the trade-offs between bias and variance that are important for improving the efficiency of Machine Learning models in botnet detection.

DOI: https://doi.org/10.54216/IJWAC.070204
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

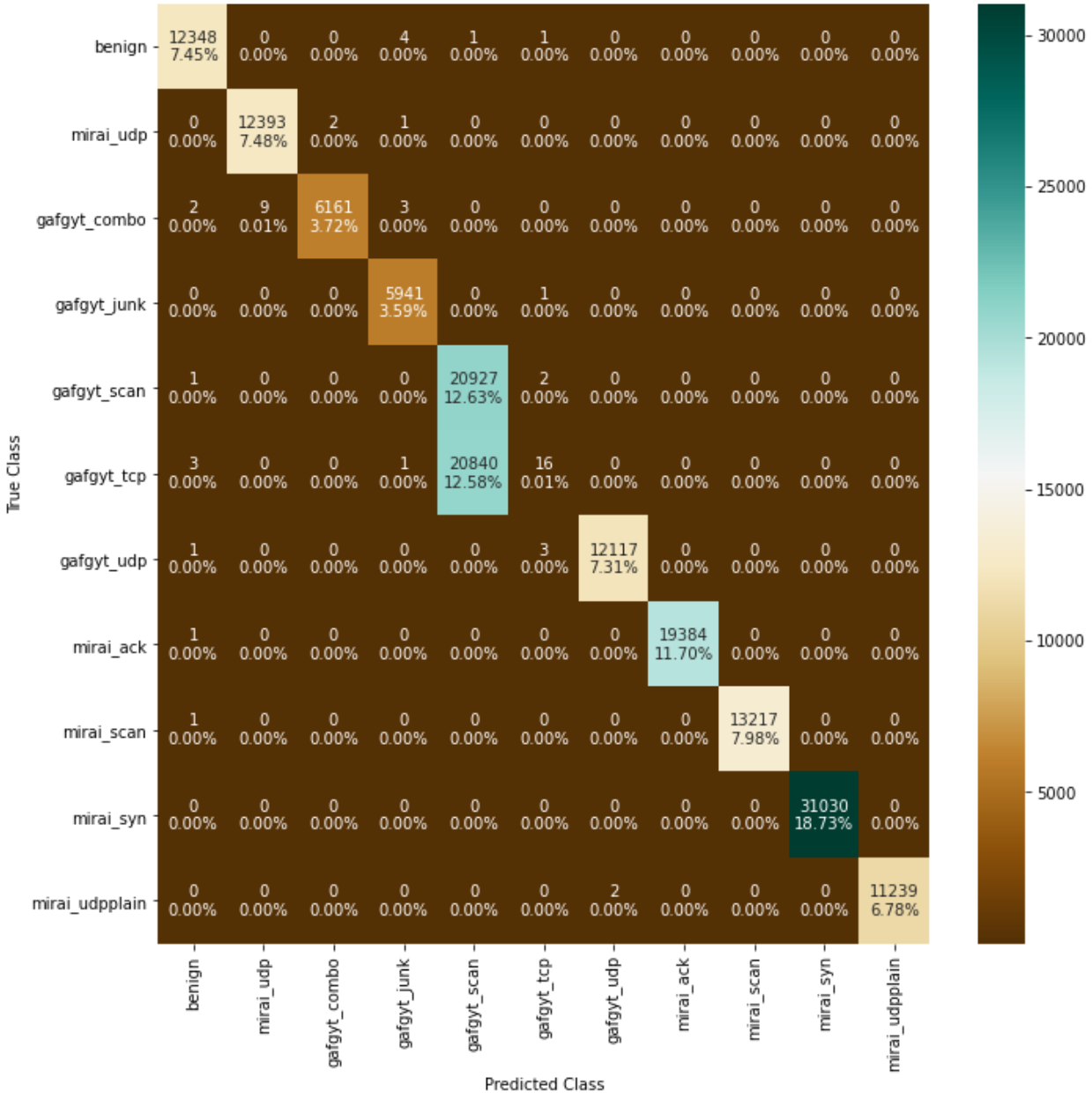

Figure 4: Confusion Matrix depicting Model Performance in Botnet Detection

The confusion matrix generated from the model's predictions and actual class labels is shown in Figure 4, which provides a comprehensive visual representation of the model's performance in botnet detection. This matrix categorizes predictions into true positive, true negative, false positive, and false negative groups, allowing for a more nuanced understanding of the model's accuracy, precision, recall, and F1 score. By visualizing the confusion matrix, Figure 3 gives a brief but detailed summary of how well the model can correctly classify botnet and non-botnet instances by pointing out its strengths and weaknesses thus helping to make informed decisions on refining the detection system for better reliability in real-world cybersecurity scenarios.

DOI: https://doi.org/10.54216/IJWAC.070204
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

5. Conclusion

This research presents a comprehensive and robust approach to botnet detection within IoT networks through the integration of Machine Learning methodologies, specifically leveraging a convolutional neural network architecture with stacked layers and residual connections. The exploration and analysis of the BoTNet dataset, collected from authentically compromised IoT devices, facilitated a meticulous understanding of botnet behaviors and network traffic characteristics crucial for effective detection. The developed model demonstrated promising performance, showcasing its ability to discern between botnet and non-botnet instances with notable accuracy and efficiency. The visualization of class distributions, learning curves, and confusion matrices provided valuable insights into the model's behavior and performance metrics. By amalgamating cutting-edge neural network architectures with carefully prepared datasets, this study contributes to the advancement of cybersecurity practices, offering a promising avenue for fortifying IoT network defenses against the pervasive threat of botnet incursions. Further enhancements and refinements to the model architecture and training strategies stand as promising directions to bolster the efficacy and resilience of botnet detection mechanisms in real-world IoT environments.

References

[1] Chakraborty, Abhilash, Anupam Biswas, and Ajoy Kumar Khan. 2023. "Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation." In Artificial Intelligence for Societal Issues, 3–25. Springer.

[2] Ahsan, Mostofa, Kendall E Nygard, Rahul Gomes, Md Minhaz Chowdhury, Nafiz Rifat, and Jayden F Connolly. 2022. "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review." Journal of Cybersecurity and Privacy 2 (3): 527–55.

[3] Gunduz, Muhammed Zekeriya, and Resul Das. 2020. "Cyber-Security on Smart Grid: Threats and Potential Solutions." Computer Networks 169: 107094.

[4] AJAYI, Wumi, Obi Ibeto, Taiwo Olomola, and Mathias Madewa. 2022. "ANALYSIS OF MODERN CYBERSECURITY THREAT TECHNIQUES ANDAVAILABLE MITIGATING METHODS." International Journal of Advanced Research in Computer Science 13 (2).

[5] Haddaji, Achref, Samiha Ayed, and Lamia Chaari Fourati. 2022. "Artificial Intelligence Techniques to Mitigate Cyber-Attacks within Vehicular Networks: Survey." Computers and Electrical Engineering 104: 108460.

[6] Lykou, Georgia, Argiro Anagnostopoulou, and Dimitris Gritzalis. 2018. "Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls." Sensors 19 (1): 19.

[7] Kitchin, Rob, and Martin Dodge. 2020. "The (in) Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention." In Smart Cities and Innovative Urban Technologies, 47–65. Routledge.

[8] Tufail, Shahid, Imtiaz Parvez, Shanzeh Batool, and Arif Sarwat. 2021. "A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid." Energies 14 (18): 5894.

[9] Zeadally, Sherali, Erwin Adi, Zubair Baig, and Imran A Khan. 2020. "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity." Ieee Access 8: 23817–37.

[10] Radoglou-Grammatikis, Panagiotis, Konstantinos Rompolos, Panagiotis Sarigiannidis, Vasileios Argyriou, Thomas Lagkas, Antonios Sarigiannidis, Sotirios Goudos, and Shaohua Wan. 2021. "Modeling, Detecting, and Mitigating Threats against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach." IEEE Transactions on Industrial Informatics 18 (3): 2041–52.

[11] Alhayani, Bilal, Sara Taher Abbas, Dawood Zahi Khutar, and Husam Jasim Mohammed. 2021. "Best Ways Computation Intelligent of Face Cyber Attacks." Materials Today: Proceedings, 26–31.

[12] Aljuhani, Ahamed. 2021. "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments." IEEE Access 9: 42236–64.

[13] Li, Zhiyi, Dong Jin, Christopher Hannon, Mohammad Shahidehpour, and Jianhui Wang. 2016. "Assessing and Mitigating Cybersecurity Risks of Traffic Light Systems in Smart Cities." IET Cyber-Physical Systems: Theory \& Applications 1 (1): 60–69.

[14] Chehri, Abdellah, Issouf Fofana, and Xiaomin Yang. 2021. "Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence." Sustainability 13 (6): 3196.

[15] Ismail, M. and F.Abd El-Gawad , A. (2023) "Revisiting Zero-Trust Security for Internet of Things", Sustainable Machine Intelligence Journal, 3. doi: 10.61185/SMIJ.2023.33106.

[16] Sai, Chennu Naga Venkata, Rangu Jaswanth, Avula Manasa, Yaramakula Sai Pranathi Reddy, Suryakanth V Gangashetty, and D Govind. 2023. "Assessing the Effectiveness of Artificial Intelligence Techniques

DOI: https://doi.org/10.54216/IJWAC.070204
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

in Mitigating Cyber Security Risks." International Journal of Intelligent Systems and Applications in Engineering 11 (4): 763–71.

[17] Marble, Julie L, William F Lawless, Ranjeev Mittu, Joseph Coyne, Myriam Abramson, and Ciara Sibley. 2015. "The Human Factor in Cybersecurity: Robust \& Intelligent Defense." Cyber Warfare: Building the Scientific Foundation, 173–206.

[18] Harel, Yaniv, Irad Ben Gal, and Yuval Elovici. 2017. "Cyber Security and the Role of Intelligent Systems in Addressing Its Challenges." ACM Transactions on Intelligent Systems and Technology (TIST). ACM New York, NY, USA.

[19] Syrmakesis, Andrew D, Cristina Alcaraz, and Nikos D Hatziargyriou. 2022. "Classifying Resilience Approaches for Protecting Smart Grids against Cyber Threats." International Journal of Information Security 21 (5): 1189–1210.

[20] M. Abdel-Basset, H. Hawash and K. Sallam, "Federated Threat-Hunting Approach for Microservice-Based Industrial Cyber-Physical System," in IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 1905-1917, March 2022, doi: 10.1109/TII.2021.3091150.

DOI: https://doi.org/10.54216/IJWAC.070204
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023