Alinteri J. of Agr. Sci. (2023) 38(4): 36-45
e-ISSN: 2587-2249
info@alinteridergisi.com

http://dergipark.gov.tr/alinterizbd
http://www.alinteridergisi.com/

IOT BOTNET ATTACK DETECTION AND PREVENTION USING DUAL MACHINE LEARNING STRATEGIES

[1] Dr. Karramareddy Sharmila Reddy,[2] Sravani Rega,[3] Namindla Rajesh
[1]Professor,[23]Assistant Professor
Department of CSE(DS)
Vaagdevi Engineering College, Bollikunta, Khila Warangal, Warangal, Telangana

ABSTRACT

The Internet of Things (IoT) has revolutionized various industries by connecting devices and enabling real-time data sharing, but it has also created new security vulnerabilities. One of the most pressing threats to IoT networks is the rise of botnet attacks, where a network of compromised IoT devices is used to launch large-scale cyberattacks, such as Distributed Denial of Service (DDoS) attacks. Traditional security measures often struggle to keep pace with the dynamic nature of IoT networks, leaving them susceptible to botnet exploitation. To address this challenge, this paper proposes a dual machine learning strategy for both preventing and detecting IoT botnet attacks.

The proposed strategy integrates two distinct machine learning models: a classification model for early detection of botnet activities and an anomaly detection model for identifying malicious behaviors that deviate from normal device operations. The classification model uses supervised learning techniques, such as decision trees and support vector machines, to analyze network traffic patterns and classify them as either normal or indicative of a botnet attack. Meanwhile, the anomaly detection model leverages unsupervised learning algorithms, such as k-means clustering and autoencoders, to detect unknown and evolving attack patterns that may not be recognized by traditional detection systems.

By combining these two approaches, the system is able to provide both proactive and reactive defense mechanisms. The classification model allows for the rapid identification and blocking of known botnet attack patterns, while the anomaly detection model enhances the system's ability to adapt to new, previously unseen attack strategies. This dual-layer approach not only improves the accuracy and efficiency of attack detection but also increases the overall robustness of IoT security.

The effectiveness of the proposed dual machine learning strategy is evaluated through a series of experiments on real-world IoT network traffic datasets. The results demonstrate that the combination of classification and anomaly detection significantly outperforms traditional single-model approaches in terms of detection accuracy, false-positive rates, and overall attack prevention.

In conclusion, the proposed dual machine learning strategy provides a comprehensive and adaptive solution for IoT botnet attack detection and prevention. By leveraging the strengths of both classification and anomaly detection, the system enhances the security of IoT networks, making them more resilient to botnet exploitation and better equipped to handle evolving threats in the ever-expanding IoT landscape.

1. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has introduced a wide range of benefits, enabling devices to connect and share data across various domains, from smart homes to industrial automation and healthcare. However, this growth has also led to an increase in cybersecurity vulnerabilities. One of the most concerning threats in IoT networks is the emergence of botnet attacks. A botnet consists of a network of compromised IoT devices that are exploited by attackers to launch large-scale cyberattacks, such as Distributed Denial of Service (DDoS) attacks, which can overwhelm network resources and cause significant disruption. These attacks often target vulnerable IoT devices that lack adequate security measures, turning them into unwitting participants in the botnet.

The unique characteristics of IoT networks, such as the massive scale of devices, the diversity of device types, and the constrained resources of many IoT devices, present significant challenges for traditional cybersecurity mechanisms. Conventional security approaches, such as firewalls and intrusion detection systems, often struggle to detect and mitigate botnet attacks in IoT environments, particularly as these attacks become more sophisticated and adaptive. As a result, there is a growing need for advanced, adaptive, and efficient strategies to prevent and detect botnet attacks in IoT networks.

Machine learning (ML) techniques have emerged as promising solutions for enhancing cybersecurity in IoT networks. By enabling systems to learn from data patterns and automatically identify anomalies, machine learning models can significantly improve the accuracy and efficiency of botnet attack detection. In particular, dual machine learning strategies, which combine multiple models for different aspects of attack detection, have shown great potential in addressing the dynamic nature of IoT security threats. These strategies can simultaneously monitor network traffic, classify malicious activity, and detect deviations from normal behavior, thus providing a more comprehensive defense against botnet attacks.

This paper proposes a dual machine learning approach for IoT botnet attack detection and prevention. The first model focuses on classification-based detection, using supervised learning algorithms to identify known attack patterns based on labeled training data. The second model employs anomaly detection, using unsupervised learning techniques to detect previously unseen attack behaviors that deviate from the normal operations of IoT devices. The combination of these two strategies allows for proactive detection of known threats and reactive detection of new, evolving attack

methods, providing a robust and adaptive security solution for IoT networks.

The objective of this study is to evaluate the effectiveness of this dual machine learning strategy in improving the detection and prevention of IoT botnet attacks. The paper explores the integration of classification and anomaly detection models, presenting a unified framework that enhances the overall security of IoT systems. The results demonstrate the potential of this approach to address the limitations of traditional security mechanisms, offering a scalable and efficient solution for safeguarding IoT networks against botnet exploitation.

Through this research, we aim to contribute to the development of more resilient and adaptive cybersecurity solutions that can effectively protect IoT devices and networks from emerging threats in an increasingly connected world.

2. LITERATURE SURVEY

‘‘Systematic literature review on IoT-based botnet attack,’’

The adoption of the Internet of Things (IoT) technology is expanding exponentially because of its capability to provide a better service. This technology has been successfully implemented on various devices. The growth of IoT devices is massive at present. However, security is becoming a major challenge with this growth. Attacks, such as IoT-based botnet attacks, are becoming frequent and have become popular amongst attackers.IoT has a resource constraint and heterogeneous environments, such as low computational power and memory. Hence, these constraints create problems in implementing a security solution in IoT devices. Therefore, various kind of attacks are possible due to this vulnerability, with IoT-based botnet attack being one of the most popular.In this study, we conducted a comprehensive systematic literature review on IoT-based botnet attacks. Existing state of the art in the area of study was presented and discussed in detail. A systematic methodology was adopted to ensure the coverage of all important studies. This methodology was detailed and repeatable. The review outlined the existing proposed contributions, datasets utilised, network forensic methods utilised and research focus of the primary selected studies. The demographic characteristics of primary studies were also outlined.The result of this review revealed that research in this domain is gaining momentum, particularly in the last 3 years (2018-2020). Nine key contributions were also identified, with Evaluation, System, and Model being the most conducted.

‘‘IoT-Flock: An open-source framework for IoT traffic generation,’’

Network traffic generation is one of the primary techniques that is used to design and analyze the performance of network security systems. However, due to the diversity of IoT networks in terms of devices, applications and protocols, the traditional network traffic generator tools are unable to generate the IoT specific protocols traffic. Hence, the traditional traffic generator tools cannot be used for designing and testing the performance of IoT-specific security solutions. In order to design an IoT-based traffic generation framework, two main challenges include IoT

device modelling and generating the IoT normal and attack traffic simultaneously. Therefore, in this work, we propose an open-source framework for IoT traffic generation which supports the two widely used IoT application layer protocols, i.e., MQTT and CoAP. The proposed framework allows a user to create an IoT use case, add customized IoT devices into it and generate normal and malicious IoT traffic over a real-time network. Furthermore, we set up a real-time IoT smart home use case to manifest the applicability of the proposed framework for developing the security solutions for IoT smart home by emulating the real world IoT devices. The experimental results demonstrate that the proposed framework can be effectively used to develop better security solutions for IoT networks without physically deploying the real-time use case.

‘‘On data-driven curation, learning, and analysis for inferring evolving Internet-of-Things (IoT) botnets in the wild,’’

The insecurity of the Internet-of-Things (IoT) paradigm continues to wreak havoc in consumer and critical infrastructures. The highly heterogeneous nature of IoT devices and their widespread deployments has led to the rise of several key security and measurement-based challenges, significantly crippling the process of collecting, analyzing and correlating IoT-centric data. To this end, this paper explores macroscopic, passive empirical data to shed light on this evolving threat phenomena. The proposed work aims to classify and infer Internet-scale compromised IoT devices by solely observing one-way network traffic, while also uncovering, reporting and thoroughly analyzing ``in the wild" IoT botnets. To prepare a relevant dataset, a novel probabilistic model is developed to cleanse unrelated traffic by removing noise samples (i.e., misconfigured network traffic). Subsequently, several shallow and deep learning models are evaluated in an effort to train an effective multi-window convolutional neural network. By leveraging active and passing measurements when generating the training dataset, the neural network aims to accurately identify compromised IoT devices. Consequently, to infer orchestrated and unsolicited activities that have been generated by well-coordinated IoT botnets, hierarchical agglomerative clustering is employed by scrutinizing a set of innovative and efficient network feature sets. Analyzing 3.6 TB of recently captured darknet traffic revealed a momentous 440,000 compromised IoT devices and generated evidence-based artifacts related to 350 IoT botnets. Moreover, by conducting thorough analysis of such inferred campaigns, we reveal their scanning behaviors, packet inter-arrival times, employed rates and geo-distributions. Although several campaigns exhibit significant differences in these aspects, some are more distinguishable; by being limited to specific geo-locations or by executing scans on random ports besides their core targets. While many of the inferred botnets belong to previously documented campaigns such as Hide and Seek, Hajime and Fbot, newly discovered events portray the evolving nature of such IoT threat phenomena by demonstrating growing cryptojacking capabilities or by targeting industrial control services. To motivate empirical (and operational) IoT cyber security initiatives as

well as aid in reproducibility of the obtained results, we make the source codes of all the developed methods and techniques available to the research community at large.

''IoT DoS and DDoS attack detection using ResNet,''

The network attacks are increasing both in frequency and intensity with the rapid growth of internet of things (IoT) devices. Recently, denial of service (DoS) and distributed denial of service (DDoS) attacks are reported as the most frequent attacks in IoT networks. The traditional security solutions like firewalls, intrusion detection systems, etc., are unable to detect the complex DoS and DDoS attacks since most of them filter the normal and attack traffic based upon the static predefined rules. However, these solutions can become reliable and effective when integrated with artificial intelligence (AI) based techniques. During the last few years, deep learning models especially convolutional neural networks achieved high significance due to their outstanding performance in the image processing field. The potential of these convolutional neural network (CNN) models can be used to efficiently detect the complex DoS and DDoS by converting the network traffic dataset into images. Therefore, in this work, we proposed a methodology to convert the network traffic data into image form and trained a state-of-the-art CNN model, i.e., ResNet over the converted data. The proposed methodology accomplished 99.99% accuracy for detecting the DoS and DDoS in case of binary classification. Furthermore, the proposed methodology achieved 87% average precision for recognizing eleven types of DoS and DDoS attack patterns which is 9% higher as compared to the state-of-the-art.

3. EXISTING SYSTEM

Nguyen *et al.* [16] proposed a graph-based approach to detect the IoT botnet via printing string information (PSI) graphs. The authors used PSI graphs to get high-level features from the function call graph and then trained a convolution neural network (CNN), a deep learning model, over the generated graphs for IoT botnet detection. Likewise, Wang *et al.* [24] proposed an automated model named as BotMark. Their proposed model detects botnet attacks based on a hybrid analysis of flow-based and graph-based network traffic behaviors. The flow-based detection is performed by k-means, which calculates the similarity and stability scores between flows. While the graph-based detection uses the least-square technique and local outlier factor (LOF) which measures anomaly scores. Similarly, Yassin *et al.* [25] proposed a novel method that compromises a series of approaches such as the utilization of the frequency process against registry information, graph visualization and rules generation. The authors investigated the Mirai attacks using the graph-theoretical approach. In order to identify similar and dissimilar Mirai patterns, the authors used directed graphs. The proposed approach only focuses on the Mirai attack.

Almutairi *et al.* [27] proposed a hybrid botnet detection technique that detects new botnets implemented on three levels, i.e., host level, network level and a combination of both. The authors focused on focused HTTP, P2P, IRC, and DNS botnet traffic.

The proposed technique consists of three components: host analyser, network analyser, and detection report. The authors used two machine learning algorithms, i.e., Naïve Bayes and a decision tree for traffic classification. Similarly, Blaise *et al.* [28] proposed a bot detection technique named BotFP, for bot fingerprinting. The proposed BotFP framework has two variants, i.e., BotFP-Clus which groups similar traffic instances using clustering algorithms and BotFP-ML is designed to learn from the signatures and identify new bots using two supervised ML algorithms, i.e., SVM and MLP. Likewise, Soe *et al.* [30] developed a machine learning-based IoT botnet attack detection model. The proposed model consists of two stages: a model builder and an attack detector. In the model builder stage, data collection, data categorization, model training and feature selection are performed step by step. While in the attack detector stage, the packets are first decoded and then the features are extracted in the same way as in the model builder phase. Finally, the features are passed to the attack detector engine where artificial neural network (ANN), J48 decision tree, and Naïve Bayes machine learning models are used for botnet attack detection.

Sriram *et al.* [31] proposed a deep learning-based IoT botnet attack detection framework. The proposed solution specifically considered network traffic flows, which are further converted into feature records and then passed to the deep neural network (DNN) model for IoT botnet attack detection. Nugraha *et al.* [32] evaluated the performance of four deep learning models for botnet attack detection by performing a couple of experiments. The experimental results revealed that CNN-LSTM outperformed all deep learning models for botnet attacks detection.

Disadvantages

An existing methodology prevents botnet attacks by detecting the scanning attack activity while it detects the botnet attack by identifying the DDoS attack for both inbound and outbound traffic.

IoT botnet attack doesn't initiates with the scanning activity and ends at the DDoS attack.

4. PROPOSED SYSTEM

The proposed system analyzed the frequently used scanning and DDoS attack techniques and produced a generic dataset by generating 33 types of scan and 60 types of DDoS attacks. In addition, we partially integrated the scan and DDoS attack samples from three publicly-available datasets for maximum attack coverage for better training of machine learning algorithms.

The system proposed a two-fold machine learning approach to prevent and detect both inbound and outbound botnet attacks in the IoT network environment. The proposed two-fold approach prevents IoT botnet attacks by detecting the scanning activity, while it detects the IoT botnet attack by identifying the DDoS attack.

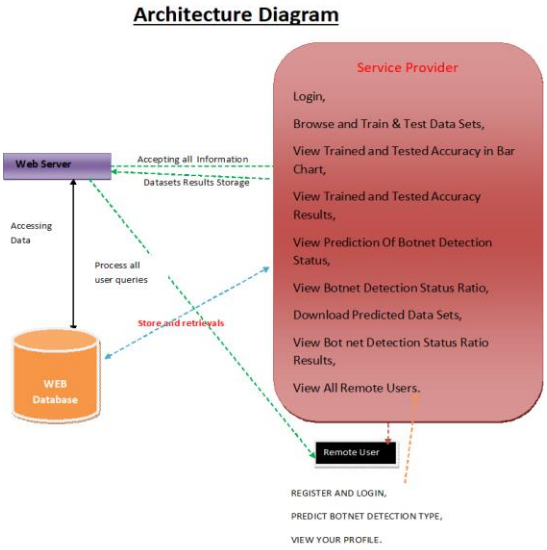
Finally, to demonstrate that the performance of the proposed two-fold approach is not limited to a single dataset, we trained three ResNet-18 [23] models over three different datasets and compared their performance

with the proposed two-fold approach for detecting and preventing IoT botnet attacks.

Advantages

- The system proposed a novel two-fold machine learning approach to prevent and detect botnet attacks in IoT networks.
- The proposed methodology stops an attacker during the scanning activity so that an attacker cannot proceed to further attack stages.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as

Login, Browse and Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Botnet Detection Status, View Botnet Detection Status Ratio,

Download Predicted Data Sets, View Botnet Detection Status Ratio Results,, View All Remote Users.

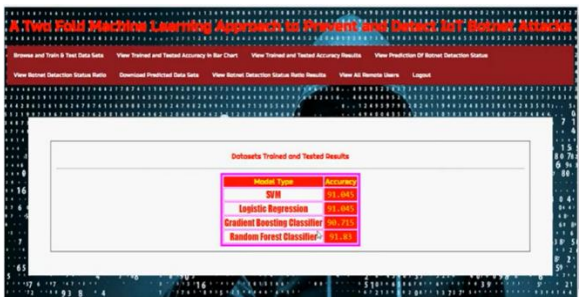
View and Authorize Users

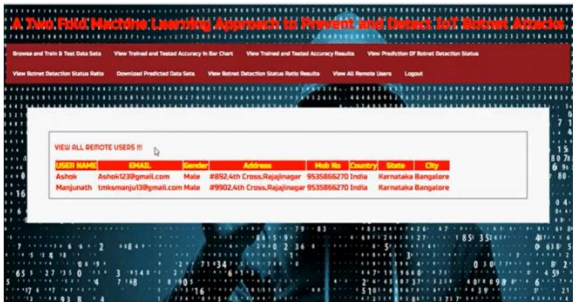
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

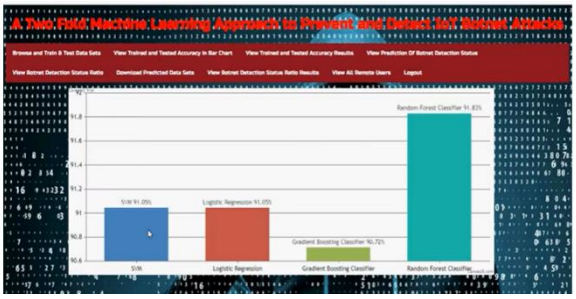
Remote User

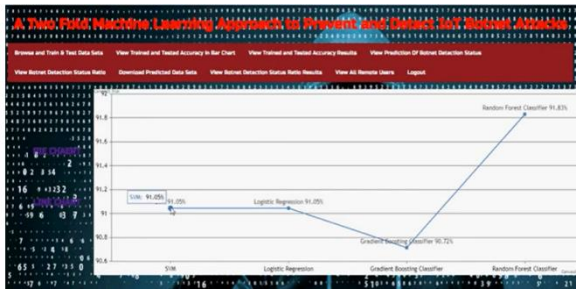
In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGINPREDICT BOTNET DETECTION TYPE, VIEW YOUR PROFILE.

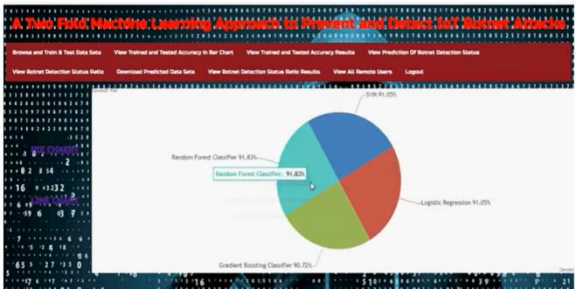
7. RESULTS

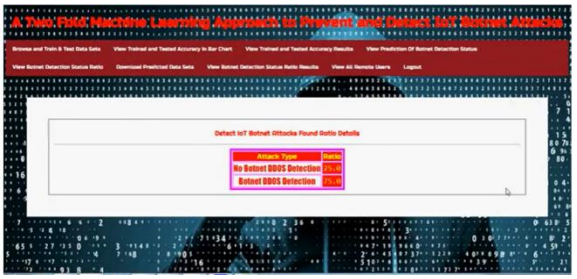












8. CONCLUSION

The growing adoption of IoT devices across various sectors has significantly enhanced operational efficiencies and connectivity, but it has also introduced new security

challenges. IoT botnet attacks, which involve compromised devices used to launch coordinated cyberattacks, pose a severe threat to the integrity and availability of IoT networks. Traditional security mechanisms often fail to keep pace with the dynamic and diverse nature of IoT environments, necessitating more advanced and adaptive solutions.

This paper proposed a dual machine learning strategy for the detection and prevention of IoT botnet attacks. By integrating two distinct machine learning models—classification-based detection and anomaly detection—our approach offers both proactive and reactive defense mechanisms. The classification model efficiently identifies known attack patterns based on historical data, while the anomaly detection model provides the flexibility to detect previously unknown attack behaviors, ensuring that new and evolving threats are identified and mitigated in real-time.

The results of the experiments conducted on real-world IoT network traffic datasets demonstrate the effectiveness of the dual machine learning strategy in improving detection accuracy, reducing false positives, and enhancing overall system resilience. The combination of these models provides a comprehensive security solution capable of addressing the unique challenges of IoT networks, offering a scalable and adaptive defense against botnet exploitation.

In conclusion, the dual machine learning strategy represents a significant step forward in securing IoT networks from botnet attacks. By leveraging the strengths of both classification and anomaly detection, this approach enhances the accuracy, adaptability, and efficiency of attack detection and prevention systems. As IoT networks continue to grow and evolve, this dual approach can serve as a critical tool for safeguarding the security and privacy of IoT devices, ensuring the continued reliability and trustworthiness of these systems in a connected world.

REFERENCES

[1] I. Ali, A. I. A. Ahmed, A. Almogren, M. A. Raza, S. A. Shah, A. Khan, and A. Gani, ``Systematic literature review on IoT-based botnet attack," *IEEE Access*, vol. 8, pp. 212220_212232, 2020.

[2] S. Ghazanfar, F. Hussain, A. U. Rehman, U. U. Fayyaz, F. Shahzad, and G. A. Shah, ``IoT-Flock: An open-source framework for IoT traf_c generation," in *Proc. Int. Conf. Emerg. Trends Smart Technol. (ICETST)*, Mar. 2020, pp. 1_6.

[3] M. Safaei Pour, A. Mangino, K. Friday, M. Rathbun, E. Bou-Harb, F. Iqbal,S. Samtani, J. Crichigno, and N. Ghani, ``On data-driven curation, learning, and analysis for inferring evolving Internet-of-Things (IoT) botnets in the wild," *Comput. Secur.*, vol. 91, Apr. 2020, Art. no. 101707.

[4] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, ``IoT DoS and DDoS attack detection using ResNet," in *Proc. IEEE 23rd Int. Multitopic Conf. (INMIC)*, Nov. 2020, pp. 1_6.

[5] S. Dange and M. Chatterjee, ``IoT botnet: The largest threat to the IoT network," in *Data Communication and Networks*. Singapore: Springer, 2020, pp. 137_157.

[6] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali,

``Towards a universal features set for IoT botnet attacks detection," in *Proc. IEEE 23rd Int. Multitopic Conf. (INMIC)*, Nov. 2020, pp. 1_6.

[7] A. O. Proko_ev, Y. S. Smirnova, and V. A. Surov, ``A method to detect Internet of Things botnets," in *Proc. IEEE Conf. Russian Young Res. Electr.Electron. Eng. (EIConRus)*, Jan. 2018, pp. 105_108.

[8] B. K. Dedeturk and B. Akay, ``Spam _ltering using a logistic regression model trained by an arti_cial bee colony algorithm," *Appl. Soft Comput.*,vol. 91, Jun. 2020, Art. no. 106229.

[9] N. Vlajic and D. Zhou, ``IoT as a land of opportunity for DDoS hackers,"*Computer*, vol. 51, no. 7, pp. 26_34, 2018.

[10] *GitHub Survived Biggest DDoS Attack Ever Recorded*. Accessed:May 3, 2021. [Online]. Available: https://github.blog/2018-03-01-ddosincident-report/

[11] *AWS Said it Mitigated a 2.3 Tbps DDoS Attack, Largest Ever*. Accessed: May 3, 2021. [Online]. Available: https://www.zdnet.com/article/awssaid- it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

[12] *Shodan*. Accessed: May 3, 2021. [Online]. Available: https://www. shodan.io/

[13] *Censys*. Accessed: May 3, 2021. [Online]. Available: https://censys.io/

[14] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ``DDoS in the IoT:Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80_84, 2017.

[15] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona,``IoDDoS_The internet of distributed denial of sevice attacks," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.* Setúbal, Portugal: SciTePress, 2017, pp. 47_58.