IoT Security using Machine Learning Techniques

AARUSHI SETHI[1], BRIJ B. GUPTA[2]
[1]National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@boulder.nist.gov)
[2]Department of Computer Science and Information Engineering Asia University, Taichung 413, Taiwan (e-mail: gupta.brij@gmail.com)

ABSTRACT In today's world IoT and interconnection of devices is fast becoming a reality. With more D2D communication and more inflow and outflow of internet traffic, cyber threats have become a glaring issue for IoT devices, especially the edge devices. In this paper we discuss machine learning and deep learning solutions and touch upon the use cases for cyber security for IoT devices.

KEYWORDS IoT security; machine learning; malware.

I. INTRODUCTION

IoT or Internet of Things [1], [2] is a concept that is based on the decentralization of computing using edge devices instead of relying on a centralized framework. These edge devices may be local servers or daily-use devices such as mobiles, tablets, laptops etc. IoT has revolutionized communication between devices as it allows easy device-to-device (D2D) communication because of various reasons but the primary reasons being that it allows heterogeneity in terms of communication protocols and eliminates the role of a centralized server [3]. Edge computing using IoT devices [4] has enabled computation near the data source which has drastically increased the collection and processing of data at the edge itself [5], [6]. However, since the inflow and outflow of data at the edge has become so convenient, it has led to high internet traffic at the edge which makes these sites vulnerable to cyber threats [7]. There have been many proposed solutions to cyber threats to IoT devices like encryption techniques such as homomorphic encryption, secure-multiparty computation and other techniques like adding noise using differential privacy. However, one of the more novel solutions is that of using artificial intelligence to tackle the problem of cyber threats. In this paper, we discuss the various machine learning solutions that have been suggested to various types of cyber security use cases.

II. LITERATURE REVIEW

For any IoT Network system, ensuring cyber security is a must.There are many cyber security attacks present in recent times such as DDoS [8]–[14], XSS [15]–[18], phishing [19]–[23]. With the integration of SD Networking, big data [24], soft computing [25], [26], cloud computing [27]–[31] and other latest technologies [32]–[34], security of IoT networks is even more indispensable. There have been extensive studies on the security of IoT devices and edge layers [35]–[37]. The protocols that are required for machinetomachine communication, its security and privacy concerns have been studied thoroughly [38], [39]. Various systems rely on trust computational models to select a particular device for communication [40]. However, there still might be files in a trusted device that may cause harm. In such scenarios machine learning models come into play as they consider each file as a separate sample point. Numerous models and studies have been done that discuss the role of machine learning solutions in IoT networks in depth [41], [42]. The author in [43] proposed big data baesed DDoS attack detection. Author in [44] proposed RFID tags based IoT security method. Author

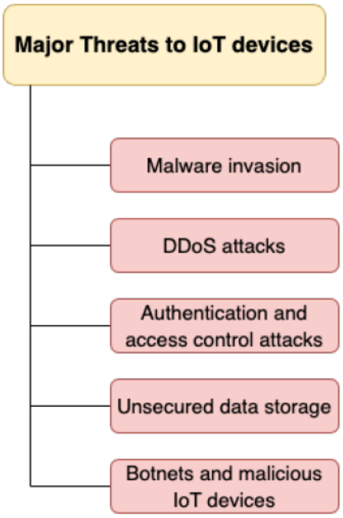
Major Threats to IoT devices
Malware invasion
DDoS attacks
Authentication and access control attacks
Unsecured data storage
Botnets and malicious IoT devices

FIGURE 1: Major threats to IoT devices in a network

in [45] proposed graph theory based attack detection method. Author in [46] proposed approach to secure IIoT devices. Also in another work, author [47] proposed IoT wireless protection technique. Author in [48] proposed Behavior-Aware Privacy for IoT. Author in [49] federated learning based technique for IoT. Author in [50] proposed an approach for medical images. Author in [51] proposed the botnet detection technique using the DNS technique. The author in [52] reviews many Honypot-based attack detection techniques. Authors in [53], [54] proposed different cryptography techniques for attack detection. Attack detection in smart vehicles is discussed by the authors in [55]–[57]. Author in [58], [59] proposed an attack detection technique for small enterprises. Authors in [60], [61] proposed attack detection in medical smart devices and smart cards respectively.

III. AI SOLUTIONS FOR CYBER THREAT TO IOT DEVICES

Artificial Intelligence encompasses the study of machine learning [3] and deep learning algorithms. Machine learning has proven to be an efficient solution to cyber threats as not only can it be used to detect malicious attacks, but also forecast them to prevent them from happening in the first which are novel attacks that are previously unknown. There are mainly three types of subdivisions when it comes to classification on the basis of the structure of the input data i.e. supervised [62], unsupervised and reinforcement learning [63]. In supervised learning, the dataset used to train a model has been previously labeled while in unsupervised learning the data is completely unlabeled. Reinforcement learning is a completely different paradigm of artificial intelligence in which learning is based on an action-response system. Reinforcement learning may incorporate some supervised and unsupervised learning techniques. Another classification that is increasingly gaining traction, especially in the field of cyber-security, is semi-supervised learning. Semi-supervised learning makes use of a small amount of labeled data to classify or generate labels for a large amount of unlabeled data. The following subsections discuss the use of supervised, unsupervised, semi-supervised and reinforcement learning methods to mitigate cyber security issues [64].

A. SUPERVISED LEARNING

As previously mentioned, supervised learning makes use of a labeled dataset to train a model that can be further used to make predictions. There are mainly two types of supervised learning techniques - regression and classification. The use cases that can be used with supervised learning are mentioned next.

1) Anomaly detection

Anomaly detection [65], [66] is used to identify whether a given file or data source is malicious or benign. Generally large previously labeled datasets are already available that can be used to train a model that predicts whether a given file is harmful or not. Some commonly used machine learning algorithms for anomaly detection are SVM, Naive-Bayes, Decision Trees, Random Forest etc. SVM is effective in generating non-linear separation planes which is an advantage for mitigating DDoS attacks and decision trees and random forest can handle more complex data. To handle more complex data, deep learning or neural networks can be used.

2) Cyber attack forecasting

Cyber attack forecasting [67] is a defensive solution to cyber threats. While anomaly and malware analysis can be useful to study the nature and severity of the malicious files, cyber attack forecasting can detect threats to a network system in real time. The most common technique of cyber attack forecasting is by monitoring inflow and outflow of internet traffic. The trends observed during the time series analysis of internet traffic data must depict long range dependency. Generally in deep learning RNN, LSTM and Bi-LSTM are used as they can forecast values based on previous sequential inputs. Further advanced time series models such as ARIMA and FARIMA can also be used to forecast an incoming cyber attack.

3) Authentication and access control

Providing authentication and access controls to particular authorities can be determined by using face recognition [68] or fingerprint recognition systems that are developed on deep CNN models. Further, speech recognition can be developed using a combination of DNN (Deep Neural Network) and RNN or any of its variants. These features can easily be enabled at edge devices like mobiles, laptops etc.

B. UNSUPERVISED LEARNING

Unsupervised learning, contrary to supervised learning, doesn't require a labeled dataset to build its models. As the name suggests unsupervised learning involves detecting underlying patterns and grouping criteria without human intervention. There are several unsupervised machine learning techniques that are encompassed in dimensionality reduction and clustering. As far as deep learning is concerned, autoencoders are one of the most widely used unsupervised learning techniques. The use cases that can be used with unsupervised learning are mentioned next.

1) Malware analysis

Malware analysis is the process of analyzing that a particular threat falls into which type of malware attack e.g. spywares, adwares, rootkits, viruses, trojans etc. Each of these kinds of malware have characteristic footprints. Novel attacks modify certain aspects of the malware that make it unidentifiable to a supervised learning model. However, using clustering [69] like k-means clustering or dimensionality reduction like Principal Component Analysis or Singular value decomposition can prove beneficial in such a scenario. PCA is highly effective against false data ejection malware. Each malware

C. SEMI-SUPERVISED LEARNING

The previously mentioned types have their pros and cons. Semi-supervised learning provides a middle ground to both the extreme types. Semi-supervised learning is used where a very small amount of labeled data is available. Two main techniques used to execute semi-supervised learning are using cluster-based approach or using re-iterative training approach.

1) Novel/Zero-day attacks

Novel or zero day attacks are malware attacks which are previously unknown. These attacks are particularly harmful to a network system as they are completely unknown to the system and so they pass through undetected, eventually causing harm to the system. Semi-supervised clustering is effective against this problem as it uses previously labeled data of similar malware to detect underlying patterns in the novel attack files and then use unsupervised clustering algorithms to classify them into similar clusters and provide mitigation solutions for them. Semi-supervised learning can also be used to provide labels to these attacks without human intervention [70].

D. REINFORCEMENT LEARNING

Reinforcement learning is completely different when it comes to defining the output of the process. The ultimate goal of reinforcement learning is not to generate an output label, unlike previous three types, but for the agent to learn by interacting with a closed loop environment where feedback is readily available. Theoretically, deep reinforcement learning can be used in scenarios where large amounts of high dimensional raw data is available but any sort of structuring and labeling is not readily available. However, this paradigm of artificial intelligence is still under-developed

IV. CHALLENGES AND LIMITATIONS

There are several challenges and limitations that can be encountered while using the aforementioned techniques for ensuring the security of an IoT devices network system. For supervised learning techniques, labeled datasets are a must. However, they are still in scarcity as labeling datasets needs time and it is essential that they must be labeled accurately because in high sensitivity situations, a model trained on faulty data may lead to fatal consequences. Secondly, generally there are huge amounts of files which leads to copious amounts of raw data which needs to be structured first and then labeled. Large amounts of data may also lead to noisy data which may cause problems. Some of these concerns may be resolved using unsupervised learning, as discussed previously, however, the overall accuracy and precision in unsupervised learning is not very high which may be catastrophic in high sensitivity situations. Although these problems may cause slight hindrance, machine learning solutions to cyber threat issues are still considered effective and developments are being made to resolve the encountered issues.

V. CONCLUSION

In this paper we have discussed the machine learning solutions to cyber threats that are encountered in an IoT network system. We have discussed supervised, unsupervised and semi-supervised learning techniques in detail and touched upon why reinforcement learning is required to solve the high level problems. Finally, we have discussed the common challenges that are being faced while executing these techniques.

REFERENCES

[1] A. Tewari and et al., "A mutual authentication protocol for iot devices using elliptic curve cryptography," in 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2018, pp. 716–720.

[2] S. Arisdakessian, O. Wahab, A. Mourad, H. Otrok, and M. Guizani, "A survey on iot intrusion detection: Federated learning, game theory, social psychology and explainable ai as future directions," IEEE Internet of Things Journal, pp. 1–1, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137608785&doi=10.1109%2fJIOT.2022.3203249&partnerID=40&md5=4ad2f5be011033dd34fb63f2f88dd7f1

[3] I. Cvitić and et al., "Ensemble machine learning approach for classification of iot devices in smart home," International Journal of Machine Learning and Cybernetics, vol. 12, no. 11, pp. 3179–3202, 2021.

[4] J. Lu and et al., "Blockchain-based secure data storage protocol for sensors in the industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 18, no. 8, pp. 5422–5431, 2021.

[5] A. Dahiya, B. Gupta, W. Alhalabi, and K. Ulrichd, "A comprehensive analysis of blockchain and its applications in intelligent systems based on iot, cloud and social media," International Journal of Intelligent Systems, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85136579349&doi=10.1002%2fint.23032&partnerID=40&md5=0b4c1567c48849a957579f54fb0a891f

[6] R. Vinoth and et al, "An anonymous pre-authentication and post-authentication scheme assisted by cloud for medical iot environments," IEEE Transactions on Network Science and Engineering, vol. 9, no. 5, pp. 3633–3642, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85130825099&doi=10.1109%2fTNSE.2022.3176407&partnerID=40&md5=dc7643dc59cc6dffad785e6a3e369009

[7] S. R. Sahoo and et al., "Security issues and challenges in online social networks (osns) based on user perspective," Computer and cyber security, pp. 591–606, 2018.

[8] B. B. Gupta, R. C. Joshi, and M. Misra, "Defending against distributed denial of service attacks: issues and challenges," Information Security Journal: A Global Perspective, vol. 18, no. 5, pp. 224–247, 2009.

[9] A. Dahiya and et al., "A reputation score policy and bayesian game theory based incentivized mechanism for ddos attacks mitigation and cyber defense," Future Generation Computer Systems, vol. 117, pp. 193–204, 2021.

[10] A. Gaurav and et al., "Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks," in Security and Privacy Preserving for IoT and 5G Networks. Springer, 2022, pp. 263–278.

[11] M. Chhabra and et al., "A novel solution to handle ddos attack in manet," 2013.

[12] P. Negi and et al., "Enhanced cbf packet filtering method to detect ddos attack in cloud computing environment," arXiv preprint arXiv:1304.7073, 2013.

[13] B. B. Gupta, M. Misra, and R. C. Joshi, "An isp level solution to combat ddos attacks using combined statistical based approach," arXiv preprint arXiv:1203.2400, 2012.

[14] P. Gulihar and et al, "Cooperative mechanisms for defending distributed denial of service (ddos) attacks," in Handbook of Computer Networks and Cyber Security. Springer, 2020, pp. 421–443.

[15] S. Gupta and et al., "Xss-safe: a server-side approach to detect and mitigate cross-site scripting (xss) attacks in javascript code," Arabian Journal for Science and Engineering, vol. 41, no. 3, pp. 897–920, 2016.

[16] S. Gupta and et al, "Php-sensor: a prototype method to discover workflow violation and xss vulnerabilities in php web applications," in Proceedings of the 12th ACM international conference on computing frontiers, 2015, pp. 1–8.

[17] B. Gupta, S. Gupta, S. Gangwar, M. Kumar, and P. Meena, "Cross-site scripting (xss) abuse and defense: exploitation on several testing bed environments and its defense," Journal of Information Privacy and Security, vol. 11, no. 2, pp. 118–136, 2015.

[18] A. Mishra and et al., "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," in 2011 European Intelligence and Security Informatics Conference. IEEE, 2011, pp. 286–289.

[19] A. K. Jain and et al., "Comparative analysis of features based machine learning approaches for phishing detection," in 2016 3rd international conference on computing for sustainable global development (INDIACom). IEEE, 2016, pp. 2125–2130.

[20] A. Almomani and et al., "Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email," arXiv preprint arXiv:1302.0629, 2013.

[21] A. K. Jain and et al., "Phish-safe: Url features-based phishing detection system using machine learning," in Cyber Security. Springer, 2018, pp. 467–474.

[22] B. B. Gupta and A. K. Jain, "Phishing attack detection using a search engine and heuristics-based technique," Journal of Information Technology Research (JITR), vol. 13, no. 2, pp. 94–109, 2020.

[23] A. Mishra and et al., "Intelligent phishing detection system using similarity matching algorithms," International Journal of Information and Communication Technology, vol. 12, no. 1-2, pp. 51–73, 2018.

[24] C. L. Stergiou and et al., "Secure machine learning scenario from big data in cloud computing via internet of things network," in Handbook of computer networks and cyber security. Springer, 2020, pp. 525–554.

[25] M. H. Bhatti and et al., "Soft computing-based eeg classification by optimal feature selection and neural networks," IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5747–5754, 2019.

[26] B. B. Gupta, D. P. Agrawal, S. Yamaguchi, and M. Sheng, "Advances in applying soft computing techniques for big data and cloud computing," pp. 7679–7683, 2018.

[27] K. Bhushan and et al., "Security challenges in cloud computing: state-of-art," International Journal of Big Data Intelligence, vol. 4, no. 2, pp. 81–107, 2017.

[28] E. Ahmed and et al., "Recent advances in fog and mobile edge computing," Transactions on Emerging Telecommunications Technologies, vol. 29, no. 4, p. e3307, 2018.

[29] S. Gupta and et al., "Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges," International Journal of Cloud Applications and Computing (IJCAC), vol. 7, no. 3, pp. 1–43, 2017.

[30] B. B. Gupta, S. Gupta, and P. Chaudhary, "Enhancing the browser-side context-aware sanitization of suspicious html5 code for halting the dom-based xss vulnerabilities in cloud," International Journal of Cloud Applications and Computing (IJCAC), vol. 7, no. 1, pp. 1–31, 2017.

[31] A. M. e. a. Manasrah, "An optimized service broker routing policy based on differential evolution algorithm in fog/cloud environment," Cluster Computing, vol. 22, no. 1, pp. 1639–1653, 2019.

[32] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, vol. 141, pp. 199–221, 2018.

[33] M. Hammad and et al., "Myocardial infarction detection based on deep neural network on imbalanced data," Multimedia Systems, vol. 28, no. 4, pp. 1373–1385, 2022.

[34] A. P. Pljonkin and et al., "Features of detection of a single-photon pulse at synchronisation in quantum key distribution systems," in 2017 6th International Conference on Informatics, Electronics and Vision & 2017 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT). IEEE, 2017, pp. 1–5.

[35] Z. Lv, "Security of internet of things edge devices," Software: Practice and Experience, vol. 51, no. 12, pp. 2446–2456, 2021.

[36] S. Cheruvu, A. Kumar, N. Smith, and D. M. Wheeler, Demystifying internet of things security: successful iot device/edge and platform security deployment. Springer Nature, 2020.

[37] R. Kumar and et al., "Stepping stone detection techniques: Classification and state-of-the-art," in Proceedings of the international conference on recent cognizance in wireless communication & image processing. Springer, 2016, pp. 523–533.

[38] J. Guo, R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," Computer Communications, vol. 97, pp. 1–14, 2017.

[39] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE communications surveys & tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[40] R. Ahmad and I. Alsmadi, "Machine learning approaches to iot security: A systematic literature review," Internet of Things, vol. 14, p. 100365, 2021.

[41] V. Gazis, "A survey of standards for machine-to-machine and the internet of things," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 482–511, 2016.

[42] U. S. Shanthamallu, A. Spanias, C. Tepedelenlioglu, and M. Stanley, "A brief survey of machine learning methods and their sensor and iot applications," in 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA). IEEE, 2017, pp. 1–8.

[43] S. Tripathi and et al., "Hadoop based defense solution to handle distributed denial of service (ddos) attacks," 2013.

[44] A. Tewari and et al., "Secure timestamp-based mutual authentication protocol for iot devices using rfid tags," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 16, no. 3, pp. 20–34, 2020.

[45] Z. Zhou and et al., "Coverless information hiding based on probability graph learning for secure communication in iot environment," IEEE Internet of Things Journal, 2021.

[46] K. Singamaneni, G. Dhiman, S. Juneja, G. Muhammad, S. AlQahtani, and J. Zaki, "A novel qkd approach to enhance iiot privacy and computational knacks," Sensors, vol. 22, no. 18, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138330610&doi=10.3390%2fs22186741&partnerID=40&md5=4734593a7b0192206976e71c469d1fa2

[47] M. Samir, C. Assi, S. Sharafeddine, and A. Ghrayeb, "Online altitude control and scheduling policy for minimizing aoi in uav-assisted iot wireless networks," IEEE Transactions on Mobile Computing, vol. 21, no. 7, pp. 2493–2505, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097924367&doi=10.1109%2fTMC.2020.3042925&partnerID=40&md5=d8e97d5e40b530385257d270f8606bc4

[48] M. Chehab and A. Mourad, "Lp-sba-xacml: Lightweight semantics based scheme enabling intelligent behavior-aware privacy for iot," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 161–175, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85123741412&doi=10.1109%2fTDSC.2020.2999866&partnerID=40&md5=f2864b809ad0c1f00c1d455c39fbcd66

[49] S. Abdulrahman, H. Tout, A. Mourad, and C. Talhi, "Fedmccs: Multicriteria client selection model for optimal iot federated learning," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4723–4735, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85102363246&doi=10.1109%2fJIOT.2020.3028742&partnerID=40&md5=e8e533f1264b695e7c097057bc334263

[50] L. Wang and et al., "Compressive sensing of medical images with confidentially homomorphic aggregations," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1402–1409, 2018.

[51] K. Alieyan and et al., "Dns rule-based schema to botnet detection," Enterprise Information Systems, vol. 15, no. 4, pp. 545–564, 2021.

[52] B. B. Gupta and A. Gupta, "Assessment of honeypots: Issues, challenges and future directions," International Journal of Cloud Applications and Computing (IJCAC), vol. 8, no. 1, pp. 21–54, 2018.

[53] B. B. Gupta and S. T. Ali, "Dynamic policy attribute based encryption and its application in generic construction of multi-keyword search," International Journal of E-Services and Mobile Applications (IJESMA), vol. 11, no. 4, pp. 16–38, 2019.

[54] J. Peng and et al., "A biometric cryptosystem scheme based on random projection and neural network," Soft Computing, vol. 25, no. 11, pp. 7657–7670, 2021.

[55] B. B. Gupta and M. Quamara, "Decentralised control-based interaction framework for secure data transmission in internet of automated vehicles," International Journal of Embedded Systems, vol. 12, no. 4, pp. 414–423, 2020.

[56] F. Mirsadeghi and et al., "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," Peer-to-Peer Networking and Applications, vol. 14, no. 4, pp. 2537–2553, 2021.

[57] B. B. Gupta, A. Gaurav, C.-H. Hsu, and B. Jiao, "Identity-based authentication mechanism for secure information sharing in the maritime transport system," IEEE Transactions on Intelligent Transportation Systems, 2021.

[58] A. Gaurav and et al., "A novel approach for ddos attacks detection in covid-19 scenario for small entrepreneurs," Technological Forecasting and Social Change, vol. 177, p. 121554, 2022.

[59] Z. Zhou and et al., "A statistical approach to secure health care services from ddos attacks during covid-19 pandemic," Neural Computing and Applications, pp. 1–14, 2021.

[60] M. Al-Ayyoub and et al., "Accelerating 3d medical volume segmentation using gpus," Multimedia Tools and Applications, vol. 77, no. 4, pp. 4939–4958, 2018.

[61] B. B. Gupta and M. Quamara, Smart Card Security: Applications, Attacks, and Countermeasures. CRC Press, 2019.

[62] K. T. Chui and et al., "An mri scans-based alzheimer's disease detection via convolutional neural network and transfer learning," Diagnostics, vol. 12, no. 7, p. 1531, 2022.

[63] I. A. Elgendy and et al., "Joint computation offloading and task caching for multi-user and multi-task mec systems: reinforcement learning-based algorithms," Wireless Networks, vol. 27, no. 3, pp. 2023–2038, 2021.

[64] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in iot security: Current solutions and future challenges," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686–1721, 2020.

[65] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource iot devices: A game-theoretic methodology," in 2016 IEEE international conference on communications (ICC). IEEE, 2016, pp. 1–6.

[66] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in iot backbone networks," IEEE Transactions on Emerging Topics in Computing, vol. 7, no. 2, pp. 314–323, 2016.

[67] X. Fang, M. Xu, S. Xu, and P. Zhao, "A deep learning framework for predicting cyber attacks rates," EURASIP Journal on Information security, vol. 2019, no. 1, pp. 1–11, 2019.

[68] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng, and K. Sakurai, "Lightweight classification of iot malware based on image recognition," in 2018 IEEE 42Nd annual computer software and applications conference (COMPSAC), vol. 2. IEEE, 2018, pp. 664–669.

[69] S. K. J. Rizvi, W. Aslam, M. Shahzad, S. Saleem, and M. M. Fraz, "Proudmal: static analysis-based progressive framework for deep unsupervised malware classification of windows portable executable," Complex & Intelligent Systems, vol. 8, no. 1, pp. 673–685, 2022.

[70] I. Mbona and J. H. Eloff, "Detecting zero-day intrusion attacks using semi-supervised machine learning approaches," IEEE Access, vol. 10, pp. 69 822–69 838, 2022.

• • •