Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

Botnet Attack Identification and Mitigation condition Software-Defined Networks Utilizing CNN Algorithm

Mr.G.Karunakar [1], Baddam Shirisha [2], Ankitha Reddy Nagella [3], Boddu Tanisha Shreya [4]

[1] Assistant Professor, Department of CSE, Malla Reddy Engineering College for Women, Autonomous, Hyderabad

[2], [3], [4] Student, Department of CSE, Malla Reddy Engineering College for Women, Autonomous, Hyderabad

ABSTRACT:

One new design that makes managing and communicating across large-scale networks easier and more flexible is software-defined networking, or SDN. It allows for the smooth and dynamic execution of complicated network choices via programmable and centralized interfaces. But SDN opens doors for people and companies to tailor network apps to their needs, allowing them to enhance services. On the other hand, it began to encounter a host of new privacy and security issues and brought the dangers of one point of failure all at once. In most cases, hackers use OpenFlow switches to conduct botnets or distributed Denial of Service (DDoS) assaults against the controller. Popular security apps that use deep learning (DL) to quickly identify and counteract attacks are on the rise. Here, we examine botnet-based DDoS attack detection using DL approaches in an SDN-supported context and demonstrate their performance. For the assessment, we utilize a dataset that we just created ourselves. In order to choose the most useful subset of characteristics, we used weighting of features and tuning techniques. Using both a synthetic dataset and actual testbed conditions, we validate the measurements or simulation results. The primary objective of this research is to identify botnet-based DDoS assaults using easily-obtained characteristics and data using a lightweight DL approach with baseline hyper-parameters. We found that the DL technique's performance is affected by the optimal subset of features, and that the accuracy of predictions of the same approach may be varied with a different collection of features. Lastly, our empirical findings show that the CNN approach works better than both the dataset and the actual

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

testbed environments. With CNN, the detection rate for typical flows is 99% and for malicious flows it drops to 97%.

INTRODUCTION

Traditional networks' limits have been investigated, and the internet is expanding at a fast pace. Patching the network is a common solution to new problems with traditional networks, however it bloats the network and reduces its control capacity. By separating the information and control planes, SDN, or software- has eliminated these issues. Because of its innovative design and ability to meet the needs of rapidly expanding networks, SDN gained notoriety throughout the network world, including the assistant editor who oversaw the manuscript's assessment and final approval, Cheng Chin. Thanks to SDN's centralized control architecture, controllers may manage the whole network using open south API interfaces and access any nearby OpenFlow switches. Applications, oversight, and data layers are additional names for this kind of network architecture. The SDN controller may dynamically adopt the policies and regulations defined by the network administrator, and the application layer executes them all. The network's behavior is susceptible to changes made to the application layer. Volume 11, Issue 49153, 2023 is an outstanding improvement to the application layer made possible by the open-source platform. The administrator is not compelled to depend only on suppliers, according to IEEE Transactions on Machine Learning The volume:11, Issue Date:17. May 2023. One positive aspect of SDN is that it enables administrators to build specialized network apps in the cloud using general-purpose hardware, without worrying about licensing limits. The SDN controllers operate at the control layer, which is sometimes referred to as the architecture's brain. The rules are sent from the application's layer to the underlying information layer via the controllers, who then decode them to produce readable messages. The controllers then gather input from the data level and send it to the layer that runs the application. The control layer also makes a call, and the data layer puts the

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

rules into action. The data layer receives instructions from the control layer and contains various hardware devices like routers and OpenFlow switches; nevertheless, it does not possess intelligence of its own. It also makes building, deploying, and maintaining the network easier and simpler. Updating and adding new programs is a simple way to improve the network's functionality and features. Simple hardware devices are required for SDN-based networks, and there are essentially no compatibility difficulties; moreover, they are cost-effective. Unveiling the information of the many underlying layers allows network access. A single controller can easily administer the network using SDN, which is both an advantage and a disadvantage owing to its centralized management. However, SDN may increase the network's flexibility and controllability. Although SDN does assist to enhance the security of existing networks, it is still far from providing the reliable security necessary to realize the promise of next-generation networking. Its novel design and emphasis on centralization raise the possibility of new security risks and the emergence of just one point of failure. In addition, attackers are able to conduct other forms of assaults, including botnets, also DDoS, saturation, and more, due to the centralized structure of SDN architecture. Malicious botnet assaults pose a significant risk to the future generation of networks. Botnets are hostile networks that use compromised computers to conduct attacks including distributed denial of service (DDoS), identity theft, spamming, phishing, and domain name system spoofing. A "bot master" attempts to get unauthorized entry to a single device in a botnet assault before deploying botnet software to seize control of the gadget while avoiding detection by its legitimate users. Next, link the bots to the attacker's Control and Command (C&C) center; from there, the bots will wait to carry out harmful operations as instructed. The most advanced distributed denial of service (DDoS) attacks across SDN and IoT networks nowadays usually use botnet technologies. The versatility and strength of botnet technology allow it to launch several forms of distributed denial of service assaults.

RELATED WORK

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

How existing datasets impact intrusion detection systems and a taxonomy of network threats

One of the biggest problems this decade has brought is the growing reliance on computers and automation; one of the biggest solutions is the need to develop more secure systems, networks, and applications. As today's networks and services get more intricate, the number of dangers that people and companies confront is growing at an exponential rate. Anomaly detection methods have been suggested by researchers in an effort to mitigate these dangers; nevertheless, existing technologies often can't keep up with the dynamic architectures, related threats, and zero-day assaults. With the proliferation of complex threats and the limitations of existing datasets, this book seeks to identify these issues and how they affect the development of network intrusion detection Systems (NIDS). In order to achieve this goal, this manuscript offers researchers two essential pieces of information: first, a taxonomy for network threats and the tools used to launch them; and second, a survey of notable datasets that analyzes their usage and influence on the evolution of IDS (intrusion detection systems) over the last decade. The paper emphasizes that just 33.3% of our risk taxonomy is covered by existing IDS research. Machine learning detection systems for intrusions are currently limited in their ability to identify real-world attacks because datasets lack attack representation, real-world threats are not available, and there are many outdated threats included. This book presents a novel approach to taxonomy and dataset analysis with the goal of enhancing both the process of creating datasets and the gathering of real-world data. Consequently, this will make next-gen IDS more efficient and better represent network risks in new datasets.

Online Education: Difficulties and Potential for Future Study in the Light of Machine Learning and Data Analytics

As more and more people have access to the internet, e-learning has become a hot topic. For the simple reason that technology has facilitated knowledge sharing and access for people all across

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

the globe. This has contributed to the ever-increasing volume of data being created by various sensors and gadgets used globally. Because of this, it is essential to examine the gathered data and draw conclusions. Proposed methods for extracting information and discovering useful patterns from data include machine learning (ML) and data analytics (DA). This article explores the domain of online education by way of its definitions and defining features. Also covered are the many obstacles that each party involved in this process must overcome. Also included are some of the published publications that attempt to address these issues. Following that, a concise overview of some widely used ML and DA methods is provided. Lastly, we suggest a few study possibilities that make use of these methods in order to shed light on the areas that should be further investigated.

According to Cisco, the amount of IP traffic that occurs in the five years that follow will surpass all previous Internet traffic in history.

Yet the new Visual Networking Index (VNI) by Cisco predicts that is just the beginning. By 2022, more IP traffic will cross global networks than in all prior 'internet years' combined up to the end of 2016. In other words, more traffic will be created in 2022 than in the 32 years since the internet started. Where will that traffic come from? All of us, our machines and the way we use the internet. By 2022, 60 percent of the global population will be internet users. More than 28 billion devices and connections will be online. And video will make up 82 percent of all IP traffic. The size and complexity of the internet continues to grow in ways that many could not have imagined. Since we first started the VNI Forecast in 2005, traffic has increased 56-fold, amassing a 36 percent CAGR with more people, devices and applications accessing IP networks," said Jonathan Davidson, senior vice president and general manager, Service Provider Business, Cisco. "Global service providers are focused on transforming their networks to better manage and route traffic, while delivering premium experiences. Our ongoing research helps us gain and share valuable insights into technology and architectural transitions our customers must make to succeed.

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

Big healthcare data and the proliferation of the internet of things (IoT): a literature review and areas for further study

Every country has health as a sustainable development area. This area has not yet investigated the many potential applications of the Internet of Things. To achieve sustainable development, this study aims to emphasize the utilization of the internet of things (IoT) in healthcare. The research is classified as applied descriptive research based on the data collected. It is a single-sectional survey study according to the FAHP technique. Prioritizing IoT use and establishing agreed-upon paired comparison matrices followed data collecting. Findings indicate that "Economic Prosperity" and "Quality of Life" were the two most important factors for healthcare IoT sustainable development. In addition, "Ultraviolet Radiation," "Dental Health," and "Fall Detection" were determined to be the most important health-related IoT objectives based on use.

A framework for the continuous and diverse availability of cloud services for smart cities' vehicles

No smart city plan is complete without an ICTS, or smart and connected transportation system. A few instances of ICTS services include route navigation, multimedia content exchange, and vehicle power management. An ongoing challenge for smart cities is the efficient and dependable selection of services for smart cars, as they implement various technologies to enhance the variety and performance of vehicular cloud services. On top of that, SPs can only guarantee the quantity, quality, and accessibility of the services they provide to cloud subscribers in vehicles. In order to get the necessary services while in motion, smart cars depend on many SPs. Consequently, it becomes more difficult for customers to vehicle cloud services to get services that match their preferences for quality of experience (QoE). In order to meet the needs of cloud users in the automotive industry, this article presents a novel service provisioning strategy that uses a cluster-based trustworthy third party (TTP) architecture to provide varied cloud services with continuous availability. Third-party intermediaries (TTPs) mediate disputes between users and cloud service

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

providers. Cars are categorized into service-specific clusters if they are thought to have comparable mobility patterns and features for acquiring services. In order to secure services with high quality of experience characteristics, TTPs engage with suppliers and cluster chiefs. The future whereabouts of a vehicle may be predicted using a location prediction approach, enabling the negotiation of services prior to the vehicle's arrival. We demonstrate via simulation results that our method can effectively find and launch cloud services with improved QoE outcomes, decreased end-to-end latency, and little overhead.

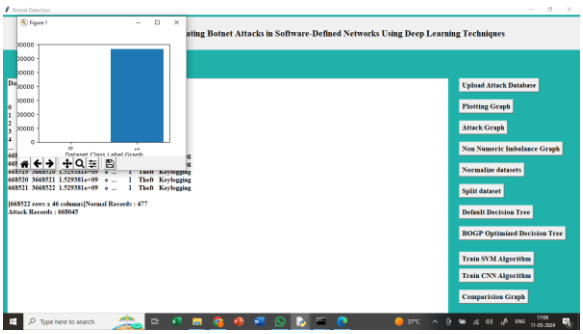
METHODOLOGY

1. We have built the following modules to execute this project and have used the identical dataset that you provided in the requirement file.
2. Dataset upload: Datasets will be uploaded using this module.
3. Dataset preparation: this section will be used to divide and clean the dataset.
4. Execute Default the decision tree Algorithm: Training the default Decision Tree method with this module yields an accuracy of 99.23%.
5. Execute BOGP Optimised Decision Tree Algorithm: we trained a decision tree with the optimal BOGP parameters using this module, and the resulting optimized decision tree outperformed the default decision tree with an accuracy of 99.30%.
6. Sixth, Execute SVM Algorithm: I trained an existing SVM algorithm using this module, and it achieved an accuracy of 96%.
7. Execute the Convolutional Neural Network (CNN) Algorithm: Achieved an Accuracy Rate of 99.996% With the Help of This Module and the CNN Extension
8. Comparison Graph: This module allows you to see how different algorithms stack up against each other. The x-axis shows the names of the algorithms, while the y-axis shows metrics like efficiency and other measures in various color bars. You can see that CNN performed quite well in all of the algorithms' extensions.

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

RESULT AND DISCUSSION

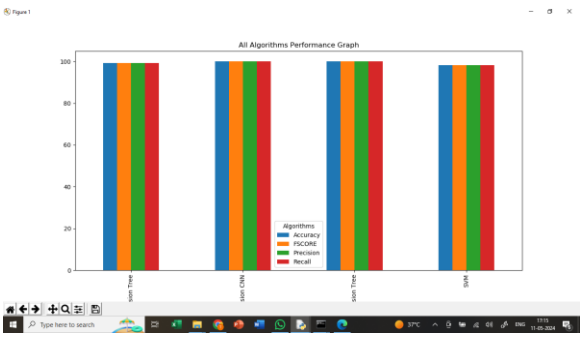


The following screen displays the number of records found in the dataset: 477 for normal and lakhs for attack. The graph also shows that the attack records are more numerous, so the dataset is highly imbalanced; to balance it, we can use the SMOTE technique.

In above results training existing SVM algorithm and it got 96% accuracy

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777



All of the algorithms in the above graph performed quite well, including the CNN extension; the x-axis shows the names of the algorithms, while the y-axis shows metrics like accuracy and others, with various colored bars representing the various metrics.

CONCLUSION

The proliferation of IoT (Internet of Things) gadgets has skyrocketed in recent years, driven by the ever-increasing need for connection and the growing dependence on the Internet. Recent predictions indicate that there will be around 28.5 billion linked gadgets by 2022, lending credence to this claim. Since there are now more possible entry points into networks, the number of attacks targeting these systems has risen. So, to make sure these gadgets are safe, we need detection and mitigation methods that are effective and fast. Therefore, in order to recognize botnet assaults on IoT devices, this study presented an improved ML-based framework that fused the Bayesian Optimization Gaussian Process (BO-GP) with a decision tree (DT) classification model. A framework for dynamic, effective, and economical detection of attacks on the Internet of Things was to be developed. The suggested optimized DT-based framework enhanced the F-score, recall, accuracy, and precision, according to the experimental findings. To be more precise, it hit 99.99%, 0.99, 1.00, and 1.00 for those four criteria in that order. This shown that the suggested system can reliably identify botnet assaults in IoT settings. There is a lot of room for growth in this piece. It would seem sense to utilize the whole dataset in the data oversampling procedure to increase the number of normal instances, which would improve the normal traces situation even more. To find

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

any trends or behaviors connected to time that might be useful in identifying botnet assaults in IoT settings, it's important looking at the time-related aspects.

REFERENCES

[1] Cisco, "Cisco Predicts More IP Traffic in the Next Five Years Than in the History of the Internet," Nov. 2018.

[2] Z. Alansari, S. Soomro, M. R. Belgaum, and S. Shamshir band, "The rise of internet of things (iota) in big healthcare data: review and open research issues," in Progress in Advanced Computing and Intelligent Engineering. Springer, 2018, pp. 675–685.

[3] H. Arasteh, V. Hossein Nezhad, V. Loia, A. Tomasetti, O. Troisi, M. Shafie-khash, and P. Siano, "Iota-based smart cities: A survey," in 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), 2016, pp. 1–6.

[4] I. Al Redhawk, M. Allowably, B. Kant arci, Y. Jarawa, and H. T. Muftah, "A continuous diversified vehicular cloud service availability framework for smart cities," Computer Networks, vol. 145, pp. 207–218, 2018.

[5] Z. Dorfman, "Cyberattacks on iota devices surge 300% in 2019,'measured in billions,' report claims," 2019.

[6] C. Crane, "20 surprising iota statistics you don't already know," 2019.

[7] A. Moubayed, A. Reface, and A. Shami, "Software-defined perimeter (sap): State of the art secure solution for modern networks," IEEE Network, vol. 33, no. 5, pp. 226–233, Sep.- Oct. 2019.

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

[8] P. Kumar, A. Moubayed, A. Reface, A. Shami, and J. Koil Pillai, "Performance analysis of sap for secure internal enterprises," in 2019 IEEE Wireless Communications and Networking Conference (WCNC), Apr. 2019, pp. 1–6.

[9] H. Hindy, D. Brossette, E. Bayne, A. K. Seam, C. Tachiais, R. Atkinson, and X. Billikens, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," IEEE Access, vol. 8, pp. 104 650–104 675, 2020.

[10] A. Moubayed, M. Inayat, A. B. Nassif, H. Lidiya, and A. Shami, "eLearning: Challenges and research opportunities using machine learning data analytics," IEEE Access, vol. 6, pp. 39 117–39 138, 2018.

[11] A. Moubayed, M. Inayat, A. Shami, and H. Lidiya, "Student engagement level in an e-learning environment: Clustering using k-means," American Journal of Distance Education, vol. 34, no. 2, pp. 137–156, 2020.

[12] ——, "Relationship between student engagement and performance in e-learning environment using association rules," in 2018 IEEE World Engineering Education Conference (EDUNINE), 2018, pp. 1–6.

[13] M. Inayat, A. Moubayed, A. B. Nassif, and A. Shami, "Systematic ensemble model selection approach for educational data mining," Knowledge-based Systems, vol. 200, p. 105992, Jul. 2020.

[14] ——, "multi-split optimized bagging ensemble model selection for multiclass educational data mining," Applied Intelligence, pp. 1–23, Jul. 2020.

[15] A. Moubayed, M. Inayat, A. Shami, and H. Lidiya, "DNS Typo Squatting Domain Detection: A Data Analytics & Machine Learning Based Approach," in 2018 IEEE Global Communications Conference (GLOBECOM), Dec. 2018, pp. 1–7.

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

[16] A. Moubayed, E. Areli, and A. Shami, "Ensemble-based feature selection and classification model for dens typo-squatting detection," in 2020 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Aug. 2020.

[17] L. Yang and A. Shami, "On hyperparameter optimization of machine learning algorithms: Theory and practice," Neurocomputing, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/ pie/S0925231220311693

[18] A. Moubayed, "Optimization Modelling and Machine Learning Techniques Towards Smarter Systems and Processes," Ph.D. dissertation, University of Western Ontario, Aug. 2018.

[19] M. Inayat, "Optimized Machine Learning Models Towards Intelligent Systems," Ph.D. dissertation, University of Western Ontario, Aug. 2018.

[20] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-based intelligent intrusion detection system in internet of vehicles," in 2019 IEEE Global Communications Conference (GLOBECOM), Dec 2019, pp. 1–6.

[21] M. Inayat, F. Salo, A. B. Nassif, A. Essex, and A. Shami, "Bayesian optimization with machine learning algorithms towards anomaly detection," in 2018 IEEE Global Communications Conference (GLOBECOM), Dec 2018, pp. 1–6.

[22] M. Inayat, A. Moubayed, A. B. Nassif, and A. Shami, "Multi-stage optimized machine learning framework for network intrusion detection," IEEE Transactions on Network and Service Management, pp. 1–1, Aug. 2020.

[23] F. Salo, M. Inada, A. Moubayed, A. B. Nassif, and A. Essex, "Clustering enabled classification using ensemble feature selection for intrusion detection," in 2019 International Conference on Computing, Networking and Communications (ICNC), 2019, pp. 276–281.

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Vol.15 No.3(2024),45-57
DOI: https://doi.org/10.61841/turcomat.v15i3.14777

[24] M. A. Teixeira, T. Salman, M. Molinari, R. Jain, N. Meskin, and M. Samake, "Scada system testbed for cybersecurity research using machine learning approach," Future Internet, vol. 10, no. 8, p. 76, 2018.

[25] M. Almain, A. Abigale, A. Al-Raheem, S. Ataui, and A. Razzaque, "Deep recurrent neural network for iot intrusion detection system," Simulation Modelling Practice and Theory, vol. 101, p. 102031, 2020.

[26] E. Anthia, L. Williams, M. Soyinka, G. Theodorakopoulos, and P. Bur- ´ nap, "A supervised intrusion detection system for smart home iota devices," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042–9053, 2019.

[27] Z. Chen, Q. Yan, H. Han, S. Wang, L. Peng, L. Wang, and B. Yang, "Machine learning based mobile malware detection using highly imbalanced network traffic," Information Sciences, vol. 433, pp. 346–364, 2018.

[28] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kielmeyer, "Smote: synthetic minority over-sampling technique," Journal of artificial intelligence research, vol. 16, pp. 321–357, 2002.

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (https://us.sagepub.com/en-us/nam/open-access-at-sage).