International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6641
***Article Received**: 22 February 2023 **Revised**: 04 April 2023 **Accepted**: 22 April 2023*

Securing IoT Networks for Detection of Cyber Attacks using Automated Machine Learning

Urvashi Sangwan[1], Dr. Rajender Singh Chhillar[2]
[1]Ph.D Scholar, Department of Computer Science and Applications
Maharshi Dayanand University, Rohtak-124001
Haryana, India
usangwan@gmail.com
[2]Professor, Department of Computer Science and Applications
Maharshi Dayanand University, Rohtak-124001
Haryana, India
chhillar02@gmail.com

Abstract— Cybercriminals are always developing innovative strategies to confound and frustrate their victims. Therefore, maintaining constant vigilance is essential if one wishes to protect the availability, confidentiality, and integrity of digital systems. Machine learning (ML) is becoming an increasingly powerful technique for doing intelligent cyber analysis, which enables proactive defenses. Machine learning (ML) has the potential to thwart future assaults by studying the recurring patterns that have already been successful. Nevertheless, there are two significant drawbacks associated with the utilization of ML in security analysis. To begin, the most advanced machine learning systems have significant problems with their computing overheads. Because of this constraint, firms are unable to completely embrace ML-based cyber strategies. Second, in order for security analysts to make advantage of ML for a wide variety of applications, they will need to develop specialized frameworks. In this study, we aim to put a numerical value on the degree to which a hub can improve the safety of an ecosystem. Typical cyberattacks were carried out on an Internet of Things (IoT) network located within a smart house in order to validate the hub. Further investigation of the intrusion detection system's (IDS) resistance to adversarial machine learning (AML) assaults was carried out. In this method, models can be attacked by supplying adversarial samples that attempt to take advantage of the defects in the detector that are present in the pre-trained model.

Keywords- Intrusion Detection Systems, Adversarial Machine, Internet of Things. Cyber Physical System

I. INTRODUCTION

A number of other terms, such as "Internet of Things," "Cyber Physical System," "Ubiquitous computing," and "Pervasive Computing," are frequently used to allude to the ongoing automation movement. There is one thing that all of these nouns have in common, and that is the fact that they describe a part of the automation of the system. In the field of automation, the implementation of Cyber Physical Systems (CPS) is quickly becoming the standard practice [1]. A CPS takes an existing physical system and transforms it into a computerized one by employing various pieces of hardware and software as well as a predetermined set of operating procedures. With the help of CPS, even the most basic instrument can function just like a sophisticated piece of technology. These electronic devices, in general, are not very useful due to the limited amount of data that they are able to process, the large amount of power that they require, and the limited amount of room that they have for storing data. A new generation of electronic systems is currently in the process of being developed. The integration of computational processes with physical systems is what this word alludes to. Computational algorithms are a type of computer programmes that, when executed on a computer, can carry out a variety of functions. Computers that are talking with a network are controlling and monitoring a wide variety of distinct physical processes at the same time. As a consequence of this, it makes the creation of automated technologies that require a smaller number of operators much easier [2]. It lessens the likelihood of system failures being brought on by individual users. Some examples of smart technology include "smart" devices, "smart" buildings, and "smart" automobiles. With regard to CPS, the Internet of Things serves as the engine that drives forward the development of the international economy. It is utilized in the construction of "smart" homes as well as metropolitan settings.

CPSs have attracted attention as a multifunctional method of carrying out tasks in a variety of contexts, including but not limited to the following: power grids, industrial automation, transportation systems, military and healthcare equipment [3-7]. Due to the extent to which they are entwined with the aforementioned systems, disruptions or damages to several of them might potentially have far-reaching effects on a nation's economy, public health, or data security. These effects could

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6641
***Article Received**: 22 February 2023 **Revised**: 04 April 2023 **Accepted**: 22 April 2023*

even extend across international borders. Because it is becoming more likely that CPSs may be the target of cyber attacks, it is essential to develop effective countermeasures against a wide variety of potential security flaws in order to protect these systems. It is necessary to implement security measures at each stage of the organizational structure of the CPS in order to protect critical infrastructure from cyber attacks. These measures must be implemented from the most fundamental components (such as field devices) all the way up to the most advanced components (control centre).

CPS is used in a wide variety of contexts because of its useful features such as remote control and handling, self-organization, sensing the physical environment, sharing position data, and monitoring sensing data, etc.

As many major nations engage on IoT-based projects to better the lives of their citizens and increase their standard of living, the global market is ripe with possibilities for CPS. The need for CPS programmes has grown as civil society has evolved in the modern era. These days, CPS can be found in a wide variety of applications, from renewable energy and electric vehicles to healthcare, government and infrastructure, smart home systems, and beyond [8]. The year 2015 saw the beginning of the smart cities project in India. The concept of "smart cities" is gaining momentum in many parts of the world. Several nations have already launched smart city initiatives. Twenty-plus cities throughout India have been selected for the "smart city" initiative. The increasing popularity of IoT-enabled services like "Smart Governance," "Smart Healthcare," "Smart Homes," "Smart Mobility," and "Smart Environment" is predicted to boost the market value of the IoT to several trillion dollars. Security issues (including privacy, authenticity, and access control) and a lack of interoperability between the many technologies currently utilized in cities and urban development are the greatest technical challenges to the adoption of CPS initiatives in future smart cities.

Not every problem has a straightforward method, and if one cannot be discovered, a direct programming approach to solving the problem is useless. Machine learning (ML) improves computer-human interaction by providing a means of problem-solving in areas where custom-built algorithms are not feasible [9]. It is possible to specify a non-constructive algorithm by providing examples of proper operation. This definition establishes ML algorithms as a meta-algorithm for generating algorithms given a description of their target output. These algorithms provide a vastly improved method of interacting with computers, as they need the user to supply merely data for computation rather than the necessary procedures.

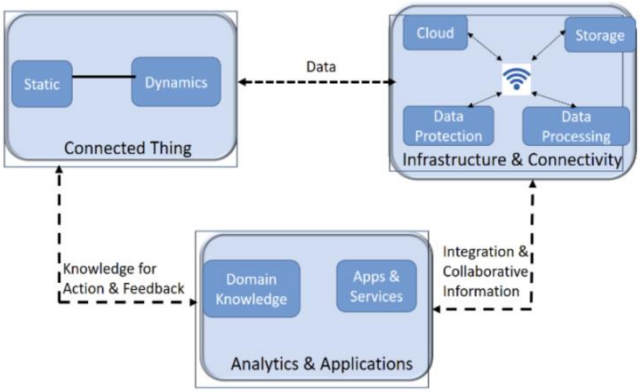

Figure1 Architecture of Cyber physical System

The ability to use computers to solve more problems is an excellent incentive to study ML, but it's not the only one. Studying computing can teach one about learning, and vice versa. The field of ML investigates the computational underpinnings of learning as a scientific subject. Problem solving using ML models built in a computational environment both informs our understanding of the brain and provides inspiration for new ML model designs.

Researching ML has scientific merit because it provides a window into the intersection of computation and learning. At the same time, science is only worthwhile if it has a meaningful impact on society. Opportunities to expand ML research lie in maintaining a steady connection to important practical challenges and making a good global impact. Many problems of practical and commercial significance can be addressed with ML methods [10]. Since our only goal as scientists is to advance knowledge, we can either start with a novel approach or then look for a problem that it can address, or we can start with a problem and then figure out what needs to be done to fix it. Extensive study will be conducted in these areas, shedding light on the positives and negatives of current frameworks and the key features of the problem at hand.

II. Literature Survey

Both the digital and physical realms play crucial roles in the overall cyber physical system (also known as the cyber network). Communication, computation, and control are the means through which a cyber and a physical system interact with one another. See Figure 2 demonstrates that it is vulnerable to both cyber and physical attacks.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6641
***Article Received**: 22 February 2023 **Revised**: 04 April 2023 **Accepted**: 22 April 2023*

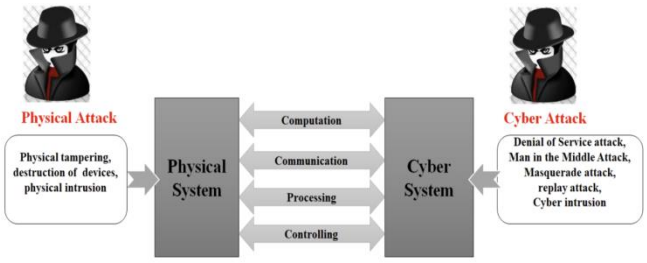

Figure2. Process of Cyber Physical Attack System

A CPS would be physically attacked to destroy the physical infrastructure and the control system. Physical attacks include things like sabotaging equipment or sneaking around inside a structure. In this type of assault, the adversary penetrates the device's defenses and modifies its underlying architecture. The attacker provides an uncontrolled or unrestricted flow of voltage to illustrate this type of attack. It messes with hardware in a very real way. By physically damaging the devices with physical instruments, an attacker renders them useless for their intended use in a physical device destruction attack [11]. Environment based sensor devices that have been modified. Some areas have temperature sensors installed in them for special purposes. In this scenario, the CPS is vulnerable to assault since a change in temperature can cause the sensors' processing unit to malfunction. All too often, hackers get access to a system through an unprotected Wi-Fi connection, a stolen smart phone, or the cloud and use malicious software to steal sensitive information. Denial of service (DoS) assaults, man in the middle attacks, masquerade attacks, replay attacks, and cyber intrusions are just a few examples of the many different types of attacks that can be launched in a cyber environment [12]. A cyber attack occurs when a hacker creates an unauthorized node in a network, which then makes a connection with a trusted node and effectively assumes its identity. Physical acts and events that could severely damage or destroy a CPS system, including its hardware, software, networks, and data, are prevented. As a distributed computing system whose nodes are linked together via physical infrastructure. A very high level of physical security is needed for CPS to safeguard its data, devices, and networks. The increasing interconnectedness of CPS has widened the scope of physical security. The three cornerstones of physical security are access control, monitoring, and testing. Access control is the process of limiting access to certain resources to authorized individuals. The physical protections of a CPS have an effect on its cyber defenses [13]. Any time an attacker gains access to a CPS-based system without permission, the CPS infrastructure is at risk. Such attacks can be thwarted and physical security bolstered by giving authorized access through cyber security procedures. Surveillance is one of the most important aspects of physical security, since it aids in both incident avoidance and clean-up. Monitoring and surveillance operations within a network will reveal malicious activity by an intruder. If these actions are watched, they will be outlawed. Moreover, damage control is simplified in the event the system is attacked. Physical security functions as both a preventative measure and an emergency response system. The security of the network will be examined in order to forestall any potential intrusions. Finding the weaknesses in the system will be helpful.

III. METHODOLOGY

The IoT attack detection method of the future, based on Random Forest-Synthetic Minority Over Sampling, is presented. Every tree in RF is constructed using a bootstrap test of the initial training data, as described by the developers of the algorithm. If you place an order with an info vector, it will chop down every tree in the forest to fulfill it. That is, both the connection and its strength weaken when m is reduced. The RF algorithm outperforms a simple decision tree calculation on large datasets in terms of both efficiency and accuracy. Because it doesn't over-fit, RF is able to handle seemingly irrelevant data . A majority, based on a vote based on presumptions about the participants' wardrobe, has made the final decision about the characterization of test data. When the order of classifications is not given consistently across a dataset, it is considered to be unbalanced. RF, like other classifiers, might suffer from the problem of learning from an extremely unbalanced dataset. In order to reduce the overall error rate in characterization, the RF calculation was developed. When discussing data discrepancies, the majority of instances tend to come from the dominant group. As a result, the RF classifier will prioritize increasing the accuracy of predictions for the majority class, leaving the minority class with no choice but to accept the accuracy of its predictions. The amount of random selections from among the k nearest neighbours affects the oversampling measure [14]. It generates synthetic tests by first determining the difference between the case viable include vector and the vector of its nearest neighbour, and then multiplying this difference by a random number between 0 and 1. At last, include this information into the existing element vector. The suggested model consists of four phases: gathering the necessary data, analysing that data, segmenting it, and finally recognising a threat or attack using the RF-SMOTE model. The proposed RF-SMOTE model is summarized graphically in Figure 3.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6641
***Article Received**: 22 February 2023 **Revised**: 04 April 2023 **Accepted**: 22 April 2023*

Figure 3. flow chart for the proposed model

In general, the N-BaIoT and NSL-KDD datasets, both of which are widely used in the context of the Internet of Things, represent the backbone of all the data. The multivariate, sequential N-BaIoT dataset consists of 7062606 data points. And it has 115 real-number properties, including assaults like Mirai, where the difficulties are around classifying and grouping. Once the data has been partitioned, RF-SMOTE is implemented to classify the various forms of traffic present in the two sets of data. To classify enormous datasets effectively, RF is widely regarded as a viable option. The reason for this is that it uses high-quality data standards to classify different types of attacks, generates a large number of decision trees (DTs), and then organises these DTs into a federation in order to move forward towards an effective classifier. The decision tree t method prioritises branches based on information gain and entropy values. To evaluate if our Internet of Things (IoT) infrastructure is under attack ("attack detection") and, if so, to identify the contributing structure or device ("attack identification"), we create a machine learning technique. In order to identify potential attacks, we plan to train our machine with a benign traffic profile (a one-class classifier) for each IoT controller and then flag any variation (from the expected pattern) in the controller's network flows as suspicious (obtained from the system ontology). See Figure 4 for a high-level overview of our anomaly detection system's architecture. We train models at the building level (Stage1: Mbi) and the device level (Stage2) for each IoT controller (Stage2: Mdk).

IV. Results and Analysis

In this paper, we present a novel attack detection using new model architecture for NIDS and HIDS, consisting of an input layer, 5 hidden layers, and an output layer. Attack detection using RF-SMOTE model in hierarchical layers make it possible to improve pattern detection in IDS data and extract very complicated characteristics. As the data passes from one layer to the next in a RF-SMOTE, classification is handled by the final layer. For KDDCup 99, there are 41 neurons in the input layer; for NSL-KDD, there are 41; for UNSW-NB15, there are

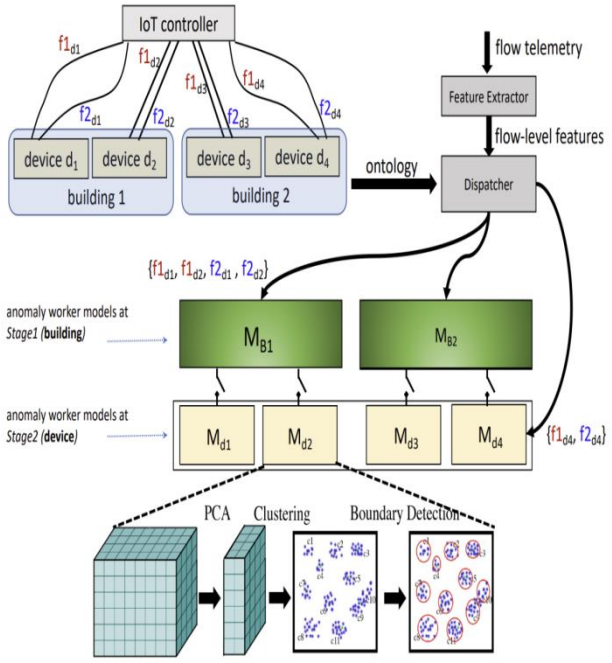

Figure 4. Structure of IoT based cyber attack detection

43; for WSN-DS, there are 17; and for CICIDS 2017, there are 77. For all datasets, an output layer has one neuron for binary classification and five for multiclass classification in KDDCup 99, five for NSL-KDD, ten for UNSW-NB15, five for WSN-DS, and eight for CICIDS 2017. Backpropagation is used to teach the RF-SMOTE new tricks. The units in the input layer to the hidden layer and the hidden layer to the output layer are typically fully connected.

The fact that feature-set-2 completely misses attack instances despite the fact that the three feature sets all yield nearly the same overall accuracy (about 92%) demonstrates that coarse-grained flow telemetry would not be able to tightly model the behaviours of the network, leading to poor visibility. We also find that feature-set-3 produces a TPR that is lower than feature-set-1 (88.0%) and feature-set-2 (59.5%). In our testing, we found that feature-set-1 yields the greatest results for both attack detection and FPR. This is due to the fact that features-set-1 catches more information of the timeseries waveform, making it better equipped to identify tiny variations in traffic volumes, while features-set-2 fails to capture fine-grained behaviours, resulting in subpar performance. When we looked at specific attacks, we discovered that feature-set-1 could detect all attack streams, albeit with a lag (especially in the case of early attack instances).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6641
***Article Received**: 22 February 2023 **Revised**: 04 April 2023 **Accepted**: 22 April 2023*

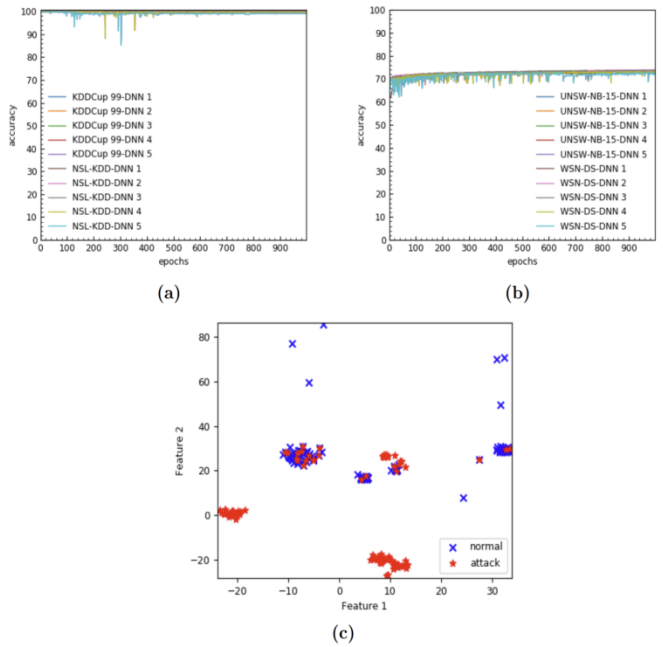

Figure5. Training Accuracy of the proposed method

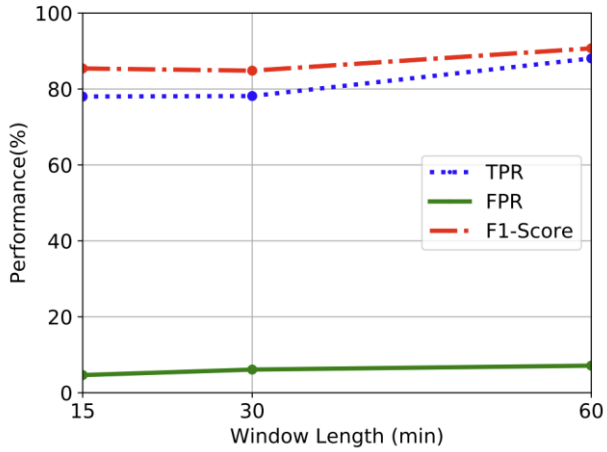

Figure6. Performance of the proposed method

V. CONCLUSION

The motivation for this research is the fact that, despite their widespread use in homes and CNIs, IoT devices create serious security vulnerabilities and are thus vulnerable to many forms of cyber assault. It has been said that the Internet of Things (IoT) is the "weakest link" in a secure infrastructure due to the pervasiveness of such devices within networks. As a result, there is a pressing need for the creation of cutting-edge methods to enhance not only the protection of the Internet of Things (IoT) from a variety of cyber attacks but also the identification of these attacks and the subsequent elimination of their negative effects on IoT networks. As CPSs are often operated continuously, efficiency in energy use has not been a primary consideration in their design in the past. Several modern battery-operated gadgets have found uses for CPSs due to their low power requirements. Therefore, there is a pressing need for long-term, low-energy consumption CPSs. With CPSs, balancing the priorities of security and energy efficiency can be difficult. Making systems that are both secure and energy efficient is difficult since increasing security reduces energy efficiency and increases operational costs. In this paper, we propose a new approach to achieving a happy medium between energy savings and system safety in CPS.

REFERENCES

[1] S. Kumar, M. K. Chaube and S. Kumar, "Secure and Sustainable Framework for Cattle Recognition Using Wireless Multimedia Networks and Machine Learning Techniques," in IEEE Transactions on Sustainable Computing, vol. 7, no. 3, pp. 696-708, 1 July-Sept. 2022, doi: 10.1109/TSUSC.2021.3123496.

[2] P. Kumar et al., "PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2326-2341, 1 July-Sept. 2021, doi: 10.1109/TNSE.2021.3089435.

[3] S. Yılmaz, E. Aydogan and S. Sen, "A Transfer Learning Approach for Securing Resource-Constrained IoT Devices," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4405-4418, 2021, doi: 10.1109/TIFS.2021.3096029.

[4] N. Chawla, A. Singh, H. Kumar, M. Kar and S. Mukhopadhyay, "Securing IoT Devices Using Dynamic Power Management: Machine Learning Approach," in IEEE Internet of Things Journal, vol. 8, no. 22, pp. 16379-16394, 15 Nov.15, 2021, doi: 10.1109/JIOT.2020.3021594.

[5] D. H. Hagos, A. Yazidi, Ø. Kure and P. E. Engelstad, "A Machine-Learning-Based Tool for Passive OS Fingerprinting With TCP Variant as a Novel Feature," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3534-3553, 1 March1, 2021, doi: 10.1109/JIOT.2020.3024293.

[6] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, doi: 10.1109/COMST.2020.2988293.

[7] S. Zafar et al., "A Systematic Review of Bio-Cyber Interface Technologies and Security Issues for Internet of Bio-Nano Things," in IEEE Access, vol. 9, pp. 93529-93566, 2021, doi: 10.1109/ACCESS.2021.3093442.

[8] W. Y. B. Lim et al., "Hierarchical Incentive Mechanism Design for Federated Machine Learning in Mobile Networks," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9575-9588, Oct. 2020, doi: 10.1109/JIOT.2020.2985694.

[9] M. U. Aftab et al., "A Hybrid Access Control Model With Dynamic COI for Secure Localization of Satellite and IoT-Based Vehicles," in IEEE Access, vol. 8, pp. 24196-24208, 2020, doi: 10.1109/ACCESS.2020.2969715.

[10] O. Mendsaikhan, H. Hasegawa, Y. Yamaguchi and H. Shimada, "Quantifying the Significance and Relevance of Cyber-Security Text Through Textual Similarity and Cyber-Security Knowledge

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6641
***Article Received**: 22 February 2023 **Revised**: 04 April 2023 **Accepted**: 22 April 2023*

Graph," in IEEE Access, vol. 8, pp. 177041-177052, 2020, doi: 10.1109/ACCESS.2020.3027321.

[11] N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[12] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. -K. R. Choo and R. M. Parizi, "An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8852-8859, Sept. 2020, doi: 10.1109/JIOT.2020.2996425.

[13] A. Kovačević, N. Putnik and O. Tošković, "Factors Related to Cyber Security Behavior," in IEEE Access, vol. 8, pp. 125140-125148, 2020, doi: 10.1109/ACCESS.2020.3007867.

[14] B. Chatterjee, D. Das, S. Maity and S. Sen, "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 388-398, Feb. 2019, doi: 10.1109/JIOT.2018.2849324.

[15] M. H. Cintuglu, O. A. Mohammed, K. Akkaya and A. S. Uluagac, "A Survey on Smart Grid Cyber-Physical System Testbeds," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 446-464, Firstquarter 2017, doi: 10.1109/COMST.2016.2627399.

[16] R. Kozik, M. Choraś and W. Hołubowicz, "Packets tokenization methods for web layer cyber security," in Logic Journal of the IGPL, vol. 25, no. 1, pp. 103-113, Feb. 2017, doi: 10.1093/jigpal/jzw044.