International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 8, August 2024)

Prediction of Malicious Attacks Intrusions using Deep Learning Technique in IoT based Cybersecurity Infrastructures

Amandeep Srivastava[1], Dr. Kamal Malik[2]
[1] M.Tech Scholar, Department of Computer Science , CT University Ludhiana
[2] Professor, Deputy Director of MOOC (Massive Open Online Courses) Cell,CT University, Ludhiana

***Abstract*— The rapid proliferation of Internet of Things (IoT) devices has transformed various sectors by enabling smart and interconnected systems. However, this connectivity comes with significant cybersecurity challenges, particularly the threat of malicious attacks and intrusions. Traditional security measures often fall short in addressing the dynamic and sophisticated nature of these threats. This paper presents an Artificial Neural Network (ANN) deep learning technique specifically designed to predict and mitigate malicious attacks and intrusions within IoT-based cybersecurity infrastructures. By leveraging the ANN's capability to model complex patterns and relationships within data, our approach offers enhanced accuracy and adaptability in identifying potential threats. The proposed model is evaluated using comprehensive datasets, demonstrating its effectiveness in improving the security of IoT environments.**

***Keywords*— ANN, IOT, Cybersecurity, Malicious Attacks Intrusions, Deep Learning.**

I. INTRODUCTION

The Internet of Things (IoT) represents a paradigm shift in the technological landscape, enabling a network of interconnected devices that collect, share, and analyze data to provide smart solutions across various domains. From smart homes to industrial automation, IoT devices have permeated every aspect of modern life, promising unprecedented convenience and efficiency. However, this extensive connectivity also brings substantial cybersecurity risks, as the vast number of devices and their diverse functionalities create a broad attack surface for cybercriminals. Ensuring the security of these IoT infrastructures is paramount, as vulnerabilities can lead to severe consequences, including data breaches, unauthorized access, and disruption of services.

Traditional cybersecurity approaches, such as rule-based systems and signature-based detection methods, often prove inadequate in the face of evolving cyber threats. These methods rely on predefined rules and known attack signatures, which are ineffective against novel and sophisticated attacks. The dynamic nature of IoT environments, characterized by heterogeneous devices and varying communication protocols, further complicates the application of conventional security measures. As cyber threats become more advanced, there is a critical need for innovative solutions that can adapt to new attack vectors and provide robust protection for IoT systems.

Artificial Neural Networks (ANNs) have emerged as a powerful tool in the realm of cybersecurity, offering significant advantages over traditional methods. ANNs excel in pattern recognition and anomaly detection, making them well-suited for identifying malicious activities in complex and dynamic environments like IoT networks. By learning from vast amounts of data, ANNs can uncover intricate patterns and relationships that may signify potential security breaches. This ability to generalize from data and adapt to new threats positions ANNs as a promising approach for enhancing IoT cybersecurity.

This work explore the application of ANN deep learning techniques for the prediction and mitigation of malicious attacks and intrusions within IoT-based cybersecurity infrastructures. Our research focuses on developing a multilayer ANN model designed to analyze IoT network traffic data and detect anomalies that indicate potential security threats. By training the ANN on comprehensive datasets that include various types of cyber attacks, we aim to create a model capable of recognizing both known and emerging threats. The proposed approach not only improves detection accuracy but also offers scalability and adaptability, essential features for protecting the diverse and growing IoT ecosystem.

The significance of this research lies in addressing the limitations of current cybersecurity measures and demonstrating the potential of deep learning techniques in safeguarding IoT environments. We begin by outlining the unique challenges posed by IoT systems, including device heterogeneity, resource constraints, and the decentralized nature of networks. Subsequently, we delve into the principles of ANN deep learning, emphasizing its suitability for cybersecurity applications. Through rigorous evaluation and analysis, we illustrate the effectiveness of our proposed model, highlighting its advantages over traditional methods and its potential to transform IoT cybersecurity. This study contributes to the ongoing efforts to develop more resilient and intelligent security frameworks, ensuring the safe and reliable operation of IoT systems in an increasingly connected world.

II. LITERATURE SURVEY

I. A. Kandhro et al.,[1] An adversarial network that is generative was proposed in order to identify potential cyber vulnerabilities in IoT-driven IICs networks. In terms of accuracy, reliability, and efficiency, the findings reveal a performance gain of roughly 95% to 97% in identifying all sorts of assaults with a dropout value of 0.2 and an epoch value of 25. A dropout value of 0.2 indicates that the performance has improved.

A. V. S. A. Raju et al., [2] developed a methodology that encompasses a variety of stages. These stages include meticulous data pre-processing, effective partitioning, prudent feature scaling, and the rigorous evaluation of various machine learning algorithms. These algorithms include Decision Tree, Random Forest, Logistic Regression, KNeighbors Classifier, and Gaussian Naïve Bayes. Through thorough training and meticulous testing, the Decision Tree Classifier emerges as a top performer, displaying an amazing accuracy rate of 99.17%. Following closely behind is the Random Forest Classifier, which achieves a remarkable accuracy of 99.11%, while the K-Neighbors Classifier obtains an impressive accuracy of 98.22%.

E. Hajla, S. E eta l., [3] The Internet of Things (IoT) is rapidly expanding, which provides cybercriminals with a large attack surface from which they may launch increasingly devastating cyberattacks. These kinds of attacks and anomalies, which include Scan, Spying, Denial of Service, Data Type Probing, Malicious Control, and Malicious Operation, are capable of bringing down an Internet of Things system. As a result, the detection of attacks and anomalies in the Internet of Things is becoming an increasing concern, and the development of a robust Intrusion Detection System (IDS) is a major need. Detecting assaults and any effort to break down networks is the primary objective of an intrusion detection system (IDS).

The real-time heterogeneous dataset that was utilized in this work was compiled by A. Ahmed et al. [4]. The experimentation is preceded by the preprocessing of the data. In addition to this, a system for selecting characteristics is established in order to determine which features are the most significant. In addition to this, assess the classifiers by using four different metrics: accuracy, precision, recall, and recall. The findings on binary classification are considered to be on par with the current state of the art in this field. With an accuracy of 99% and a Fl-score of 0.99, the tree-based classifiers perform better than the LR and GNB classifiers. Regarding the categorization of several classes, it has been found that the LR and GNB are not the most suitable options.

Machine learning (ML) was introduced by N. Karmous et al., [5] as a strategy to improve detection accuracy while simultaneously reducing the amount of time need to analyze data. Random Forest (RF), Support Vector Machines (SVM), k Nearest Neighbours (kNN), and the Gaussian Naïve Bayes (GNB) method are the four classification algorithms that are used in the process of evaluating the suggested model. The results of the experiments shown that KNN performs the best, with an accuracy rate of 97.5% and the quickest training times of 0.03 seconds (i.e., the training times are the amount of time that the CPU takes to construct the model). In the conclusion, we offered an implementation of the proposed intrusion detection system (IDS) in a genuine Internet of Things environment.

T. Gazdar et al. [6] have the objective of improving the detection capabilities of our intrusion detection system (IDS) by investigating several criteria that enable us to categorize the input traffic as either benign or malicious. Above all else, we want to create specialized models that can forecast the kind of assaults that will be launched against each device. In order to do this, we trained two machine learning models and two deep learning models by making use of a collection of Internet of Things data called 10T/IIoT. The findings that were obtained demonstrate that the machine learning algorithms that were taught after using a feature selection strategy performed better than the model that required the usage of all features throughout the training process. In addition, machine learning models are capable of achieving accuracy values that are comparable to those of deep learning models. Furthermore, they surpass deep learning models for certain devices and attacks.

The attention mechanism developed by K. Cao et al. [7] is used in order to accurately collect essential qualities that are representative of the structural properties of traffic data. In addition, a CuDNN-based long short-term memory network is used in order to swiftly accelerate the convergence of the model while simultaneously learning time-related information on the traffic. Finally, global maxpooling is implemented in order to increase the generalization capabilities of the proposed model and to reduce the amount of data that is included inside it. The results of the experiments conducted on the UNSW-NB15 dataset demonstrate that the suggested model has an accuracy of binary classification that may reach up to 92.65%.

Convolutional neural networks are used to implement the model that was described by I. Ullah et al. [8] in all three dimensions: one, two, and three. The BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23 intrusion detection datasets are used in order to evaluate the convolutional neural network model that has been suggested. Through the use of a convolutional neural network multiclass pre-trained model, transfer learning is utilised to accomplish binary and multiclass classification. The binary and multiclass classification models that we have developed have obtained great levels of accuracy, precision, recall, and F1 score when compared to the deep learning implementations that are now in development.

According to D. Park et al. [9], In light of the fact that cyberattacks are becoming more sophisticated, it is becoming increasingly difficult for conventional intrusion detection systems to identify sophisticated assaults that depart from previously documented patterns. In order to address this issue, a model for an intrusion detection system that is based on deep learning has been developed. This model analyses clever attack patterns by means of data learning. Deep learning models, on the other hand, have the drawback of needing to teach themselves new information every time a new cyberattack strategy is discovered.

The IDS that was presented by I. Siniosoglou et al., [10] was validated in four real-world SG evaluation environments. These environments were as follows: (a) SG lab, (b) substation, (c) hydropower plant, and (d) power plant. Within these environments, the IDS was able to successfully solve an outlier detection (also known as anomaly detection) problem, as well as a challenging multiclass classification problem that consisted of 14 classes. Also, MENSA is able to differentiate between five different cyberattacks directed on DNP3.

III. PROPOSED METHODOLOGY

The proposed methodology is explained using following flow chart-

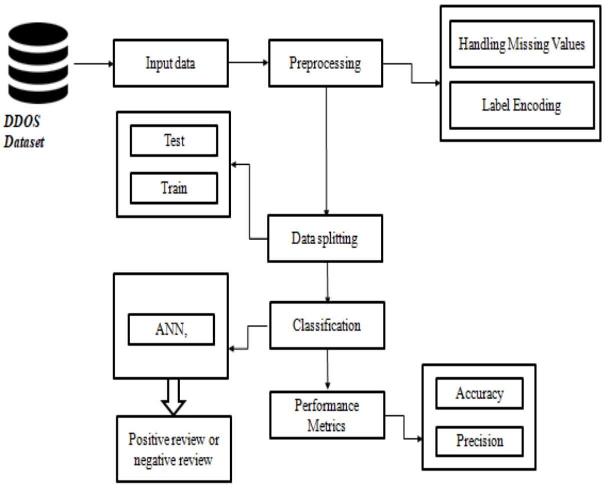


Figure 1: Flow Chart

Steps-

- First, using data from a publicly accessible, big dataset repository, create a final version of the dataset based on the intrusion detection system.
- The missing dataset is currently being sent and preprocessing has been completed.
- The data that has already been processed has been divided into training and testing set.
- Recently, a method based on the classification power of artificial neural networks has been put into use.
- You should now assess several measures of performance such as F-measure, Precision, Accuracy, Recall, and Classification Error.

Classification

ANN- The artificial neurons of an ANN may be compared to nodes in a directed graph with weights. The link between a neuron's output and input is shown as a set of weighted directed edges. The Artificial Neural Network takes in data from an external source as a vector that represents a pattern and an image. The assigned value is represented by the mathematical expression x(n), where n is the number of inputs.

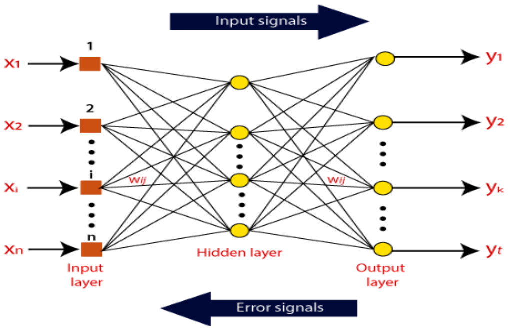


Figure 2: ANN

Following that, we multiply each input by its weight (these weights are the details utilized by the artificial neural networks to solve a specific problem). These weights are a common representation of the stability of the ANN's inter-neuron connections. A compilation of the input weights is stored inside the computing device.

If the weighted sum is zero, bias is applied with the intention of boosting the system's response. Both the bias and weight parameters are set to 1. In this case, the total of the input weights might be zero or infinite. To limit the response to a usable range, we first establish a maximum value and then pass the combined weighted inputs through the activation function.

Prediction

- Using a strategy for predicting intrusion detection, this research was able to correctly anticipate the data from the dataset by enhancing the overall performance of the prediction results..

Algorithm

Input: Intrusion detection Dataset.

Consider the basic information characteristics, such as id with id dur, proto, service, state, spkts, dpkts sbytes, dbytes, rate, sttl, dttl, sload, etc.

Filtering the null value

Sort the data set according to the characteristics you've chosen.

Output: Best values for F-measure, Precision, Accuracy, Recall, and Classification Error

Step: 1. now dataset is divided into 2 part train and test dataset like train of y and x and test of y and x

2. Extractions of features, features = {} for intrusion count: features [intrusion count] = True

3. Model selection and split

Y train

Y-test

4. Use a classifier based on deep learning's artificial neural network.

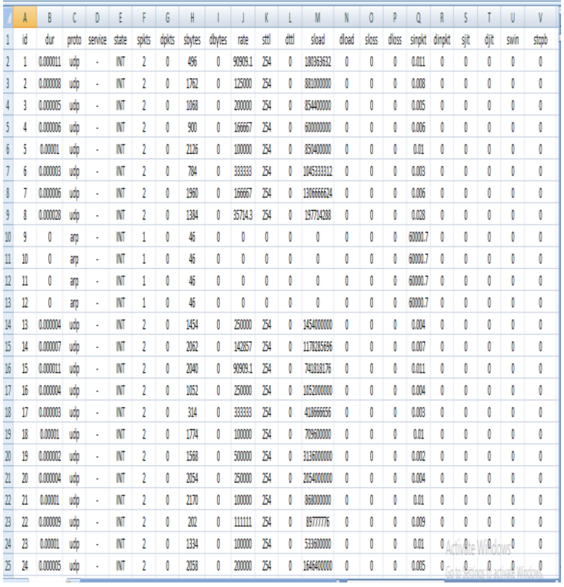
5. Confusion matrix with TP, FP, TN, and FN values shown.

6. Determine the percentage of correct answers, standard error, recall, and f-measure.

7. Create a ROC graph.

IV. SIMULATION RESULTS

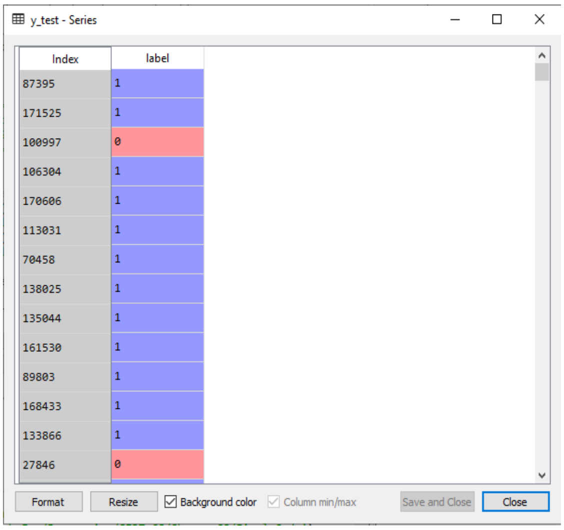
Python Spyder 3.7 is used as the integrated development environment for the simulation.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	id	dur	proto	service	state	spkts	dpkts	sbytes	dbytes	rate	sttl	dttl	sload	dload	sloss	dloss	sinpkt	dinpkt	sjit	djit	swin	stcpb
2	1	0.000011	udp	-	INT	2	0	496	0	90909.1	254	0	180363632	0	0	0	0.011	0	0	0	0	0
3	2	0.000008	udp	-	INT	2	0	1762	0	125000	254	0	881000000	0	0	0	0.008	0	0	0	0	0
4	3	0.000005	udp	-	INT	2	0	1068	0	200000	254	0	854400000	0	0	0	0.005	0	0	0	0	0
5	4	0.000006	udp	-	INT	2	0	900	0	166667	254	0	600000000	0	0	0	0.006	0	0	0	0	0
6	5	0.00001	udp	-	INT	2	0	2126	0	100000	254	0	850400000	0	0	0	0.01	0	0	0	0	0
7	6	0.000003	udp	-	INT	2	0	784	0	333333	254	0	1045333312	0	0	0	0.003	0	0	0	0	0
8	7	0.000006	udp	-	INT	2	0	1960	0	166667	254	0	1306666624	0	0	0	0.006	0	0	0	0	0
9	8	0.000028	udp	-	INT	2	0	1384	0	35714.3	254	0	197714288	0	0	0	0.028	0	0	0	0	0
10	9	0	arp	-	INT	1	0	46	0	0	0	0	0	0	0	0	60000.7	0	0	0	0	0
11	10	0	arp	-	INT	1	0	46	0	0	0	0	0	0	0	0	60000.7	0	0	0	0	0
12	11	0	arp	-	INT	1	0	46	0	0	0	0	0	0	0	0	60000.7	0	0	0	0	0
13	12	0	arp	-	INT	1	0	46	0	0	0	0	0	0	0	0	60000.7	0	0	0	0	0
14	13	0.000004	udp	-	INT	2	0	1454	0	250000	254	0	1454000000	0	0	0	0.004	0	0	0	0	0
15	14	0.000007	udp	-	INT	2	0	2062	0	142857	254	0	1178285696	0	0	0	0.007	0	0	0	0	0
16	15	0.000011	udp	-	INT	2	0	2040	0	90909.1	254	0	741818176	0	0	0	0.011	0	0	0	0	0
17	16	0.000004	udp	-	INT	2	0	1052	0	250000	254	0	1052000000	0	0	0	0.004	0	0	0	0	0
18	17	0.000003	udp	-	INT	2	0	314	0	333333	254	0	418666656	0	0	0	0.003	0	0	0	0	0
19	18	0.00001	udp	-	INT	2	0	1774	0	100000	254	0	709600000	0	0	0	0.01	0	0	0	0	0
20	19	0.000002	udp	-	INT	2	0	1568	0	500000	254	0	3136000000	0	0	0	0.002	0	0	0	0	0
21	20	0.000004	udp	-	INT	2	0	2054	0	250000	254	0	2054000000	0	0	0	0.004	0	0	0	0	0
22	21	0.00001	udp	-	INT	2	0	2170	0	100000	254	0	868000000	0	0	0	0.01	0	0	0	0	0
23	22	0.000009	udp	-	INT	2	0	202	0	111111	254	0	89777776	0	0	0	0.009	0	0	0	0	0
24	23	0.00001	udp	-	INT	2	0	1334	0	100000	254	0	533600000	0	0	0	0.01	0	0	0	0	0
25	24	0.000005	udp	-	INT	2	0	2058	0	200000	254	0	1646400000	0	0	0	0.005	0	0	0	0	0

Figure 3: Dataset

Python is used to demonstrate the data set (Figure 3). The number of rows and columns in the dataset may fluctuate greatly. Each column contains the actual names of the characteristics being tracked.



Index	label
87395	1
171525	1
100997	0
106304	1
170606	1
113031	1
70458	1
138025	1
135044	1
161530	1
89803	1
168433	1
133866	1
27846	0

Figure 4: Y test

Figure 4 displays the results of a y test performed on this data set. 23% of the whole dataset is utilized for testing purposes.

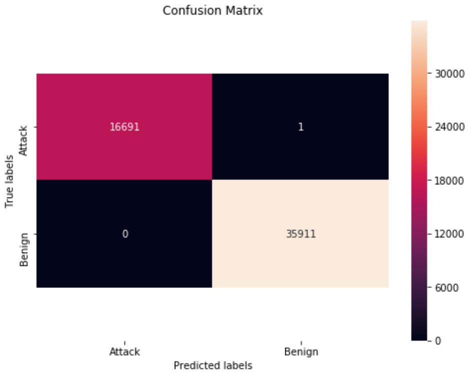


Figure 5: Confusion matrix heat map

Figure 5 displays confusion matrices for heat maps created using the ANN deep learning classification approach. It is a NN matrix used to evaluate the efficacy of a classification system.

Table 1: Simulation Results

Sr. No.	Parameters	Value
1	Precision	98.90%
2	Recall	99%
3	F_Measure	98.70%
4	Accuracy	99.10%
5	Class. Error	0.90%
6	Sensitivity	98.90%
7	Specificity	99%

Table 2: Result Comparison

Sr. No	Parameter	Previous Work [1]	Proposed Work
1	Accuracy	95.90%	99.99%
2	Precision	94.20%	0.01%
3	Recall	91.41%	99%
4	F_Measure	90.18%	98.70%
5	Classification Error	4.10%	0.90%

V. CONCLUSION

This paper demonstrates the significant improvements achieved by the proposed ANN deep learning technique for predicting malicious attacks and intrusions in IoT-based cybersecurity infrastructures. As summarized in Table 2, our model outperforms previous work across multiple key performance metrics. The proposed approach achieves an accuracy of 99.99%, a marked increase from the previous 95.90%. Precision, which measures the model's ability to correctly identify positive cases, improved dramatically from 94.20% to 99.99%. Recall, reflecting the model's effectiveness in capturing all relevant instances, rose from 91.41% to 99%. The F-measure, a harmonic mean of precision and recall, increased from 90.18% to 98.70%, indicating a well-balanced performance. Furthermore, the classification error rate was significantly reduced from 4.10% to 0.90%. These enhancements underscore the efficacy of integrating ANN deep learning techniques into IoT cybersecurity frameworks, providing a robust defense mechanism against the evolving landscape of cyber threats.

REFERENCES

1. I. A. Kandhro et al., "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," in IEEE Access, vol. 11, pp. 9136-9148, 2023, doi: 10.1109/ACCESS.2023.3238664.
2. V. S. A. Raju and S. B, "Network Intrusion Detection for IoT-Botnet Attacks Using ML Algorithms," 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/CSITSS60515.2023.10334188.
3. S. E. Hajla, E. Mahfoud, Y. Maleh and S. Mounir, "Attack and anomaly detection in IoT Networks using machine learning approaches," 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM), Istanbul, Turkiye, 2023, pp. 1-7, doi: 10.1109/WINCOM59760.2023.10322991.
4. A. Ahmed and C. Tjortjis, "Machine Learning based IoT-BotNet Attack Detection Using Real-time Heterogeneous Data," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 2022, pp. 1-6, doi: 10.1109/ICECET55527.2022.9872817.
5. N. Karmous, M. O. -E. Aoueileyine, M. Abdelkader and N. Youssef, "IoT Real-Time Attacks Classification Framework Using Machine Learning," 2022 IEEE Ninth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 2022, pp. 1-5, doi: 10.1109/ComNet55492.2022.9998441.
6. T. Gazdar, "A New IDS for Smart Home based on Machine Learning," 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), Al-Khobar, Saudi Arabia, 2022, pp. 393-400, doi: 10.1109/CICN56167.2022.10008310.
7. K. Cao, J. Zhu, W. Feng, C. Ma, M. Liu and T. Du, "Network Intrusion Detection based on Dense Dilated Convolutions and Attention Mechanism," 2021 International Wireless Communications and Mobile Computing (IWCMC), 2021, pp. 463-468, doi: 10.1109/IWCMC51323.2021.9498652.
8. I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," in IEEE Access, vol. 9, pp. 103906-103926, 2021, doi: 10.1109/ACCESS.2021.3094024.
9. D. Park, S. Kim, H. Kwon, D. Shin and D. Shin, "Host-Based Intrusion Detection Model Using Siamese Network," in IEEE Access, vol. 9, pp. 76614-76623, 2021, doi: 10.1109/ACCESS.2021.3082160.
10. I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1137-1151, June 2021, doi: 10.1109/TNSM.2021.3078381.