Shreya et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. No. 9, Issue No. 2, June 2022, pp. 24-32

A Novel Neural Network Technique for handling challenges of Cyber security

Shreya[1], Vandana Dabass[2]

[1]M.Tech Scholar, Department of Computer Science Engineering, Ganga Technical Campus, Rohtak, Haryana, India Email - shreya3343@gmail.com

[2]H.O.D, Department of Computer Science Engineering, Ganga Technical Campus, Rohtak, Haryana, India Email- hod.cse@gangatechnicalcampus.com

Abstract: **Prevent, detect and respond to security alerts and events are the goals of security operations centres (SOCs). Security operations centers are concerned about the rapid growth of digital information and the resulting challenges. These concerns are related to whether or not SOCs are capable of handling a wide range of information from various systems, devices, and networks to prevent or identify security alerts or events. To address this issue, this article examines the use of artificial intelligence in a security operations center. Artificial intelligence is taken into consideration when doing the analysis. Governmental agencies in the Netherlands are contrasted to theoretical potential and problems. There is a gap analysis that helps the businesses figure out the next measures to deal with this issue.**

Keywords: Cyber security, Intrusion detection system, Feature selection, Data reduction, Decision tree, Local Outlier Factor, Network security, Network infrastructure

I. INTRODUCTION

The value of security operations centres in an organization's data security cannot be overstated. Preventing, detecting, and responding to security alerts and events are the primary goals of a security operations centre. In order to carry out their duties, security operations centres rely on both internal and external information sources. The security operations centre uses the data it collects to make informed judgments. The complexity of the information source makes it difficult to analyse the data, but the connection across multiple data sources is much more difficult. A human being's ability to analyse the combined information sources is insufficient. Basic capability for examining data sources is supported by applications. However, emerging technologies such as machine learning and artificial intelligence provide up new possibilities because of the volume and complexity of data sources.

With the growth of artificial intelligence, organisations and especially the security operations centre need to comprehend the effect of artificial intelligence from a variety of perspectives. When employing new technology, such as artificial intelligence, it is necessary to be aware of the benefits and drawbacks.

In order to prevent, identify, and respond to security alerts, the security operations centre relies on information. Due to digitization, the internet of things, and the proliferation of BYOD (bring your own device), digital information, including metadata, is growing quickly. In particular, equipment that are not under the organization's management and maintenance impose an extra security risk on the company.

Figure 1 Cyber security elements

It is necessary to take additional steps such as onboarding in order to protect the devices themselves from malware. Data for a security operations centre to analyse is becoming more and more plentiful. It's nearly hard for people to keep track of and make sense of everything that's going on these days. Large volumes of data may be analysed by computers depending on predefined use cases. Humans set up and machines process these specified use cases. Three unsuccessful login attempts, a huge number of document downloads in a short period of time, or harmful traffic outside

of business hours are examples of use cases. Computers are better at these jobs than people because they can do them more quickly, more efficiently, and with more precision. It's nearly hard for the average person to make sense of all the information when it's combined from many sources.

Governments and businesses alike have made cybersecurity and information assurance a primary concern in the last decade. Some of the worst-case situations for many firms include cybersecurity breaches like Sony Pictures Entertainment's data exposure in late 2014. Globally, 83 percent of firms said that cyberattacks were among their top three concerns in 2015. (ISACA, 2015). It is worth noting that in 2014, congress in the United States passed the Cybersecurity Workforce Assessment Act (Pub.L. 113–246), which calls for a strategy for boosting the number of cybersecurity specialists in the workforce. As long as demand for cybersecurity specialists continues to be low (ISACA, 2015), it is imperative that existing ways of increasing the entry of people into this field are evaluated and improved.

Sponsoring cybersecurity competitions is a popular way for the government and private sector to get people interested in cybersecurity jobs. It is critical to address the shortage of cybersecurity professionals through improving cybersecurity contests. An important first step in understanding the sorts of people attracted to contests and whether or not they are inspired to pursue careers in cybersecurity afterward is the work we have done. The participants in one of the most well-known cybersecurity contests serve as a proxy for the general attitude of competition competitors.

II. PROBLEM FORMULATION

In the past, researchers have found that students participate in cybersecurity competitions for a variety of reasons, including the opportunity to apply the skills they already have to new challenges, the development of socialisation skills, and the opportunity to network with fellow students and potential employers (Gavas et al., 2012). We need to understand more about these cybersecurity rivals and what their interests are, so that we can better lead those who are interested in pursuing a career in cybersecurity.

It has recently been discovered that IT workers share some personality qualities in common with each other (Ash et al., 2006a, 2006b; Cruz et al., 2015; Lounsbury et al., 2007, 2009; Rosenbloom et al., 2008; Warren et al., 2012). In a study by Ash et al., IT workers were compared to other types of working professionals in terms of their personality characteristics and career interests. It was shown that IT workers had a lower level of conscientiousness and a greater level of openness to new experiences on the NEO-FFI (a well-established "big five" personality test) (Ash et al., 2006a). IT workers are more likely to favour occupations with realistic and investigative themes, according to a second study conducted by the same team using the Strong Interest Inventory (a psychometric measure widely used by career counsellors and occupational researchers).

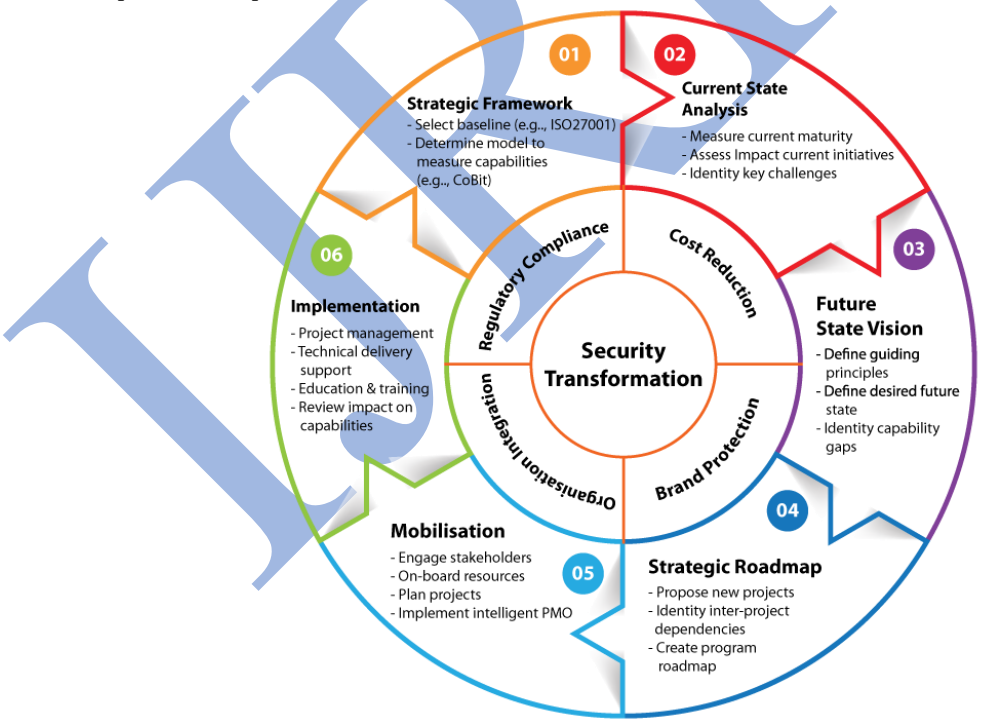

Figure 2 security-strategy-and-transformation

For their part, non-IT workers performed better when it came to the social and entrepreneurial aspects of their jobs (Ash et al., 2006b). A analysis of 90 research in software engineering by Cruz et al. (2015) found that the Myers-Briggs Type Indicator was the most commonly utilised and that their samples had greater degrees of introversion, sensing, thinking, judgement and logical temperaments. In general, these studies reveal that IT workers differ from those in other industries in terms of their personality traits and vocational choices. Despite the fact that cybersecurity is a part of Information Technology, it is a distinct area of study.

In contrast to Ash et aldefinition .'s of IT professionals, the tasks performed by cybersecurity experts are separate (application developers, programmers, web administrators,

and software engineers). In contrast to IT workers, security professionals must analyse how such systems may fail and implement contingency plans to prevent intrusion.

III. RELATED WORK

Numerous scientists have proposed a variety of security approaches for VANETs that meet both privacy and security concerns. Several current VANET approaches are discussed in this section, all of which focus on the same VANET challenges. According to Ying and colleagues (9) an anonymous and lightweight authentication system smart card (ASC) is proposed to handle privacy preservation concerns such as the authenticity of a user or a communication conveyed over the network. The user and message verification processes leverage low-cost cryptographic operations. This protocol ensures the privacy of the concerned user but does not authenticate or verify the sent communications. Decentralized, light-weight authentication and key agreement protocol (LAKAP) for VANET was developed by Wazid et al. [10]. This uses the bitwise exclusive OR (XOR) operation and the one-way hash function. Using the properties of the pseudonym and the group signature-based approaches with conditional anonymity, Rajput et al. [11] developed a hybrid method for privacy preserving authentication (HEPPA). The pseudonyms used in this method are lightweight and basic, allowing for conditional secrecy. An efficient, scalable, and privacy-preserving authentication (ESPA) system based on a hybrid cryptographic approach was proposed by Tangade and Manvi [12]. Cui et al. [13] proposed a VANET with cuckoo filter (SPACF) safe privacy-preserving authentication technique to improve client privacy and security while lowering data transmission costs. In addition, the researchers proposed a new authentication technique without bilinear pairings, which might result in high computing costs. Data structures such as the cuckoo filter use hash functions to speed up searches and improve accuracy. Methods like the ones discussed here have been adopted as the work's standard protocol because of their focus on enhancing the security and privacy of individual network users. Methodologies now in use focus mostly on authentication and privacy protection solutions. However, additional VANET security requirements, such as non-repudiation, availability, and integrity, have received little attention. There is now a void that can be filled by a new security-based approach that is now available in order to further enhance VANET security. As a result, the resolution provided here aims to improve VANET security by utilising cutting-edge technology that can address security concerns and improve road safety by utilising vehicle resources and data transmission systems.

Intrusion detection using artificial neural networks is discussed in this section.

Cybersecurity is a huge issue, with a wide range of solutions to protect against a variety of threats [10]. Intrusion detection systems and virus detection using Artificial Neural Networks (ANNs) are not new ideas. Anomaly detection and virus detection have been tested using ANNs as long back as 2009 [11]. Overfitting, memory consumption, and overhead of traditional IDS/malware detection are addressed by a feed-forward ANN in [12]. It was suggested that a two-layered feed-forward ANN be used. The aforementioned issues were dealt with using a training function and validation dataset that were combined together. For a fraction of the computing effort, the authors claim that their approach delivers the same outcomes as traditional methods. An evaluation of the process was carried out using the KDD'99 dataset as a reference. The paper's conclusion indicates that less data is preferable because the computer needs to crunch it for a shorter period of time. Pruning of the ANN is examined in [13] as part of the network's optimisation. Nodes in the input or hidden layers of the brain are deleted in this process. Having a smaller number of computations to do makes the ANN more efficient. Using an Artificial Neural Network (ANN) as an IDS was also shown to be promising. As it turned out, the results were rather positive.

In [15], instead of supplying inputs directly from the dataset, Principal Component Analysis (PCA) is used as a feature extractor before feeding the data to the ANN. With this strategy, training time and memory needs are much reduced, as the paper demonstrates. There was no significant difference in accuracy between the two tested procedures. This means that PCA is the better choice. The training time of an ANN can be improved by using Kernel PCA, however it consumes a lot of memory. Because the accuracy metrics of both techniques are similar, the authors of [16] come to the conclusion that combining various algorithms is desirable. Graphical Processing Units (GPUs) have been studied with the purpose of speeding up computation.

Based on an ANN, as GPUs are well-suited for ANN calculations. There has been a documented boost in performance [17]. A one-layer neural network (ANN) is compared to a Support Vector Machine, a Naive Bayes, and a C4.5 algorithm by the authors of [18]. The ANN performs as well as, or better than, existing malware detection techniques, but because of the 3-layer ANN framework's simplicity, it requires less calculations. As a replacement for KDD'99, the NSL-KDD dataset was used for these tests. NSL-KDD Deep hierarchical network model is the name given to the convolutional neural network used to extract spatial characteristics and the Bidirectional long short-term memory used to extract temporal features in [19]. Security benchmarks such as NSL-KDD and UNSW-NB15 are used to test the solution. Use of one-sided selection and synthetic minority oversampling techniques to first minimise noise in the benign class and then oversample minority classes, resulting in balanced training data. NSL-KDD has an accuracy rate of 83.58 percent, whereas UNSW-NB15 has an accuracy rate of 77.16 percent. To address the issue of high dimensionality and noise in cybersecurity data, the authors of [20] have proposed a novel approach. A deep belief network (DBN) and a feature-weighted support vector machine (SVM) are used to achieve this goal (WSVM). An adjustable learning rate is employed as a feature extractor to train the DBN. Then, the characteristics are sent into a WSVN tailored for particle swarms. On the NSL-KDD, the solution achieves a binary classification accuracy of 85.73 percent. BAT (Bidirectional Long Short-term Memory Network and Attention Mechanism) is proposed by the authors of [21]. The BLSTM features are scanned by the attention mechanism. There are numerous convolutional layers in a CNN to achieve

a model that does not need feature engineering. The method has a success rate of 85.25 percent.

IV. IDS EVALUATION METRICS

An IDS's efficiency and efficacy may be evaluated using a variety of metrics, but most fall into two categories: security-based metrics and performance metric [31, 32].

1) Security-Based Metrics:

According to this group of metrics, IDS may distinguish between intrusive and noninvasive activities. It is possible for an IDS to produce one of these results: When an intrusion is correctly categorised as an intrusion, it's a true positive (TP), and when a valid activity is correctly classified as legitimate, it's a true negative (TN). However, when an intrusion is erroneously labelled as an intrusion, it's also an error.

- *Confusion matrix:* This metric shows the classification outcome. For example, it shows if a categorization is correct or incorrect. Binary classification can have dimensions, but a multi-class classifier with various classes can also have dimensions. A baseline of metrics from which additional measures of efficacy can be measured, the confounding matrix is not an independent metric.
- *Accuracy:* An IDS's ability to correctly classify test and validation sets is measured by this metric.
- *Precision:* Percentage of categorised activities by the IDS that are invasive is represented by this measure.
- *Recall:* this indicator is the percentage of invasive behaviours that the IDS classifies as intrusive.
- *F-score:* A weighted harmonic mean of precision and recall, where accuracy is mirrored by the importance of recall, is the statistic known as the F-score. Multi-class classifications are evaluated using the F-score as well. The F1-score is a result of using the formula (4). Based on the frequency of classes, or the relevance of all classes, the final score is calculated [33]. There are several ways to evaluate binary and multi-class classifiers using the Gmeasure, which is the geometric mean of accuracy and recall. The -score is usually compared to the Gmeasure.
- ROC curve: The receiver operator characteristic (ROC) curve is a robust measure of the sensitivity and specificity associated with a continuous variable it is a graph with two axes: a vertical axis for true positive rate (TPR) and a horizontal axis for false positive rate (FPR).

As a crucial assessment metric, the area under the receiver operating characteristic (AUC) curve is widely recognised.

2) Performance-Based Metrics

i) Computational cost: the time it takes to complete a necessary job in order to determine whether or not an action is invasive or legal. Secondarily, the amount of data an IDS can analyse in a second is known as the "communication overhead." This is the IDS's throughput rate in Giga Bits per second, which is used to demonstrate the IDS's performance.

iii) CPU usage: when an IDS is added to the infrastructure, this measure shows how much of an impact it has on the CPU.

iv) Memory usage: the memory consumption of an IDS in order to perform its categorization is measured here.

v) Energy consumption: this parameter measures how much more power a device uses when it is paired with an IDS. For hardware-limited appliances like smartphones and IoT devices, this is a must.

V. PROPOSED METHOD BASED ON ARTIFICIAL NEURAL NETWORK

An all-purpose modelling tool is Artificial Neural Networks (ANN). Convolutional Neural Networks (CNN), Radial Basis Function Networks (RBFN), Radial Basis Probabilistic Function Neural Networks (RBPN), Recurrent Neural Networks (RNN) and many more have been developed from the original concept [22]. They are a well-known and widely used data mining technique, capable of classification, regression, clustering, and time series analysis, and have a wide range of applications, including Natural Language Processing [28], Biometrics [29], discovering polynomial roots [30–32], and intrusion detection [33]. Assumption #1: An ANN mimics, to a degree, the learning capabilities of a biological neural network, highlighting the principles of neural networks found in human brains, however simplified.

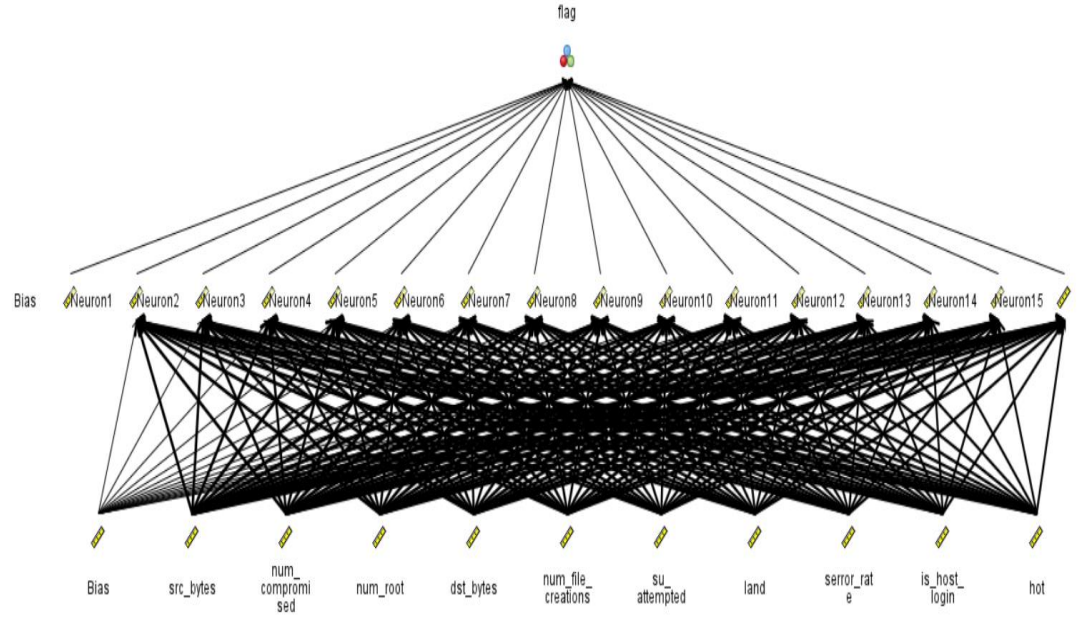

Figure 3.6 Neural Network for current problem

When it comes to pattern recognition, an ANN's remarkable modelling power comes from its tremendous malleability as it adapts to data. Approximation is critical when dealing with real-world data, when the information is ample but the patterns hidden in it remain undiscovered. There are several factors that contribute to how well a setup performs.

An artificial neural network (ANN) learns by adjusting its weights based on new data sets. Because of its generalizability and ability to recognise correlations between variables, the algorithm can perform well on new, unexpected datasets [36]. It's like trying to pass a line, plane, or hyper-plane through a set [37].

Perceptrons are artificial neural networks with only one computational layer. It has an input and an output layer of computation. The computational layer receives the data points from the input layer. The output layer calculation produces a binary value for the perceptron's forecast, which is demarcated by the sign of the value. Bias can be used to even out the distribution of wealth.

The activation function Uv is represented by the sign in the equation. Artificial neural networks with several hidden layers can use a variety of activation functions. Rectified Linear Unit (ReLU) or Hard Tanh are often used in multi-layered networks for simpler training. It is possible to express the regression error in terms of a difference between the expected and actual test values. The weights should be changed if the error is not zero. For all data points in a dataset, the perceptron is designed to minimise the least squares difference between the two variables:

D. The loss function is the term given to this aim.

All of the data in the dataset X is taken into account while defining a loss function, and the weights W are updated with a learning rate when the algorithm repeats over the complete dataset. Stochastic gradient-descent is the term given to this algorithm.

The hidden levels of a multi-layer neural network are referred to as computational layers. The title itself alludes to the layers' black-box nature, which hides calculations from the user's view. All the way to the output layer, the data has been processed all the way from the input layer.

The feedforward neural network [38] is the name given to the method described above. In most cases, the number of nodes in the topmost computational layer does not match the number of nodes in the input layer exactly.. According to the level of complexity of the model, the number of neurons and the number of hidden layers must be determined. The usage of hidden layers with a lower number of neurons than the number of neurons in the inputs provides a loss in representation, which in many situations improves the network's performance. There's a good chance that removing the noise from the data is to blame.

Overfitting, also known as overtraining, can occur when a network has too many neurons. As a result of this phenomena, an artificial neural network is unable to function well when confronted with new data since the approximation is not adequately generalised. In this study, the effect on ANN performance of the number of hidden layers and the number of neurons in those hidden layers was examined (in addition to other hyperparameters). Topology and network structure are two terms that might be used interchangeably to refer to hyperparameters.

Backpropagation is used. A single-layer perceptron's loss function is a simple function of its weights, therefore training it is trivial. The method becomes more difficult when there are numerous layers of weights interfering with each other. Local gradients along numerous pathways to the output node are summed together to calculate the Error Gradient [38]. There are two stages to the algorithm: forward and reverse. To begin, input nodes receive the data points and use them to calculate outcomes at successive layers using the current weights. The predicted outcome is compared to the training case. The gradient of the loss function for all weights is shown in the backward phase. Gradients recalculate the weights, starting at the output layer and working their way backwards

all the way to the top. A single iteration of this weight-updating process is termed an epoch, and for ANNs, it can take thousands of epochs to reach convergence.

Hyperparameter optimization is used to enhance the selected methods. The activation function is one of the most critical aspects of the Artificial Neural Network design, since the influence it has on the feasible outcomes is clear. As a result, the network is able to handle various activation functions. In multi-layer networks, the choice of activation function is critical since each layer might have its own non-linear activation function. In addition to affecting the ANN's output and convergence, each individual function can also have an impact on the network's overall size and scope. There are many activation functions Uv, however we focused on the four that appear most frequently in the present literature:

- Sigmoid
- Sigmoid horn
- Linear Unit Rectified (ReLU)
- Asymptotically Tangential (tanh)

A grid search strategy is used to find the best network configuration since it covers the whole space of hyperparameters.

Experimental setup

The KDD'99 virus and intrusion data concerns have been regularly mentioned in the literature, hence NSL-KDD was designed to solve these issues. A benchmark dataset has been developed despite the fact that some of the undesirable traits persist. Even still, the paucity of available IDS datasets and the difficulties of acquiring the data make NSL-KDD a reliable solution for intrusion detection/malware detection research.

There are approximately 5,000,000 entries in the dataset, which makes it both acceptable for machine learning and not so huge that researchers are forced to arbitrarily select areas of the data set. This makes it easier to compare the findings. An enhancement over the original KDD'99 dataset is that the NSL-KDD has been cleaned of redundant data.

This dataset was developed in response to the scarcity of contemporary and credible cybersecurity datasets, and it is the first of its kind. The IDS datasets that are made accessible to researchers frequently have a slew of flaws, such as a lack of diversity in traffic, a lack of variation in attacks, a lack of features, and more. By abstracting the behaviour of 25 users across several protocols, the authors of CICIDS2017 provide a dataset with realistic background traffic. Over the course of five days, the setup was subjected to a variety of assaults, including malware, DoS, web and other types of attacks. Over eighty network flow characteristics are included in CICIDS2017, making it one of the most recent datasets available to researchers. In order to minimise the total number of features to 50, PCA is employed. An arbitrary number of characteristics was chosen based on the results of the early tests of the setup. The input layer of the Artificial Neural Network receives this reduced feature set.

VI. RESULTS

The results of the reinforcement learning algorithm clearly answer the research questions presented earlier. We have shown how to map the features of a Petri net to the reinforcement framework from (Sutton and Barto, 2018). The agent is the player and the action that the player can take is to change the transition rates. The reward is calculated by whether or not the player reached a success or failure place at the end of the episode. The state is the marking of the places. The environment is the Petri net itself. The reward is based on the final end state. All intermediate states are updated based on the final reward. The second question was answered by implementing the Petri net simulator and the machine learning algorithm. The results from the experiments show that the attacker and defender can both learn by varying their policies, or transition rates. The -Greedy solution allows for exploitation and exploration to determine the best set of transitions rates. Players can compete against one another to maximize their potential success while at the same time minimizing the impact of the other player.

Both classic firewalls, on the other hand, were able to detect every bogus deauthentication packet.

Observed \ Predicted	OTH	REJ	RSTO	RSTOS0	RSTR	S0	S1	S2	S3	SF	SH
OTH	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	100.0%	0.0%
REJ	0.0%	95.6%	3.6%	0.0%	0.3%	0.3%	0.0%	0.0%	0.0%	0.1%	0.0%
RSTO	0.0%	20.7%	77.1%	0.0%	0.5%	0.0%	0.0%	0.0%	0.0%	1.7%	0.0%
RSTOS0	0.0%	50.0%	50.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
RSTR	0.0%	3.4%	1.6%	0.0%	91.9%	0.0%	0.0%	0.0%	0.0%	3.0%	0.0%
S0	0.0%	0.5%	0.0%	0.0%	0.3%	99.0%	0.0%	0.0%	0.1%	0.0%	0.0%
S1	0.0%	19.0%	0.0%	0.0%	0.0%	4.8%	0.0%	0.0%	23.8%	47.6%	4.8%
S2	0.0%	0.0%	6.7%	0.0%	0.0%	20.0%	0.0%	6.7%	33.3%	33.3%	0.0%
S3	0.0%	0.0%	0.0%	0.0%	2.0%	1.2%	0.0%	0.0%	96.4%	0.4%	0.0%
SF	0.0%	0.0%	0.1%	0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	99.7%	0.0%
SH	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	100.0%

Row Percent: 100.00, 80.00, 60.00, 40.00, 20.00, 0.00

Figure 3 Predicated values in Neural Network

The DNN technique outperformed the decision tree classifier in terms of false positives and accuracies. It is also possible to determine the sensitivity of a classifier with a high threshold, making it a potential foundation for the prevention of deauthentication attacks

.

Observed	Predicted										
	OTH	REJ	RSTO	RSTOS0	RSTR	S0	S1	S2	S3	SF	SH
OTH	0	0	0	0	0	0	0	0	0	4	0
REJ	0	3682	139	0	12	12	0	0	0	5	0
RSTO	0	160	596	0	4	0	0	0	0	13	0
RSTOS0	0	1	1	0	0	0	0	0	0	0	0
RSTR	0	23	11	0	615	0	0	0	0	20	0
S0	0	10	1	0	7	1993	0	0	2	0	0
S1	0	4	0	0	0	1	0	0	5	10	1
S2	0	0	1	0	0	3	0	1	5	5	0
S3	0	0	0	0	5	3	0	0	240	1	0
SF	1	5	15	0	10	2	0	2	5	14835	0
SH	0	0	0	0	0	0	0	0	0	0	73

Row Percent
100.00
80.00
60.00
40.00
20.00
0.00

Figure 5 Predicated values (Figure) in Neural Network

The techniques presented here can enable informed decision making by computer system managers and operators. Persons responsible for defending a computer system can benefit from knowledge of vulnerabilities in their systems and the relative likelihood of them being exploited found by the machine learning process. Persons responsible for attacking a computer system can use machine learning to plan their attacks. The methods can be customized to specific computer systems by adjusting the success and cost reward values and the allowable transition rates. Models of additional CAPEC attack patterns can be developed using the PNPSC formalism, and those models can be composed into more complete models of a specific system (Mayfield et al., 2018a). Finally, the PNPSC formalism can be used to model non-CAPEC attacks as well.

VII. CONCLUSION AND FUTURE WORKS

For this research, the goal was to demonstrate that the machine learning method could work in principle. A primary area that needs further research is how to apply the models and the ma- chine learning algorithm to a realistic computing environment. The values for success, cost, and rate variables are all notional and currently have no relation to a real computing system. Obtaining realistic values relies on reports from system administrators and man- agers who are hesitant to reveal detailed information about their systems especially when considering the impact of an attack. Another future work is to build a complete example of the computing environment including the details on the decision process to choose the values previously mentioned. This example needs to include how the model is composed from various attack patterns to represent a complete system.

REFERENCES

[1]. B. C. Stahl et al., "Artificial intelligence for human flourishing – Beyond principles for machine learning," J. Bus. Res., vol. 124, no. December 2020, pp. 374–388, 2021, doi: 10.1016/j.jbusres.2020.11.030.

[2]. J. Vávra, M. Hromada, L. Lukáš, and J. Dworzecki, "Adaptive anomaly detection system based on machine learning algorithms in an industrial control environment," Int. J. Crit. Infrastruct. Prot., vol. 34, no. April, 2021, doi: 10.1016/j.ijcip.2021.100446.

[3]. E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, "Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems," J. Inf. Secur. Appl., vol. 58, no. February, 2021, doi: 10.1016/j.jisa.2020.102717.

[4]. A. Shahraki, M. Abbasi, A. Taherkordi, and A. D. Jurcut, "A comparative study on online machine learning techniques for network traffic streams analysis," Comput. Networks, vol. 207, no. July 2021, p. 108836, 2022, doi: 10.1016/j.comnet.2022.108836.

[5]. N. R. Sabar, X. Yi, and A. Song, "A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security," IEEE Access, vol. 6, pp. 10421–10431, 2018, doi: 10.1109/ACCESS.2018.2801792.

[6]. H. Karimipour, A. Dehghantanha, R. M. Parizi, K. K. R. Choo, and H. Leung, "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids," IEEE Access, vol. 7, pp. 80778–80788, 2019, doi: 10.1109/ACCESS.2019.2920326.

[7]. Z. Ma, H. Ge, Y. Liu, M. Zhao, and J. Ma, "A Combination Method for Android Malware Detection Based on Control Flow Graphs and Machine Learning Algorithms," IEEE Access, vol. 7, pp. 21235–21245, 2019, doi: 10.1109/ACCESS.2019.2896003.

[8]. T. Wisanwanichthan and M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM," IEEE Access, vol. 9, pp. 138432–138450, 2021, doi: 10.1109/ACCESS.2021.3118573.

[9]. S. K. Tayyaba et al., "5G vehicular network resource management for improving radio access through

machine learning," IEEE Access, vol. 8, pp. 6792–6800, 2020, doi: 10.1109/ACCESS.2020.2964697.

[10]. W. Wang, F. Harrou, B. Bouyeddou, S. M. Senouci, and Y. Sun, "A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems," Cluster Comput., vol. 25, no. 1, pp. 561–578, 2022, doi: 10.1007/s10586-021-03426-w.

[11]. K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," Ad Hoc Networks, vol. 133, no. December 2021, p. 102894, 2022, doi: 10.1016/j.adhoc.2022.102894.

[12]. M. Pawlicki, "Neurocomputing A survey on neural networks for (cyber-) security and (cyber-) security," vol. 500, pp. 1075–1087, 2022, doi: 10.1016/j.neucom.2022.06.002.

[13]. A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," Comput. Networks, vol. 183, no. September, p. 107593, 2020, doi: 10.1016/j.comnet.2020.107593.

[14]. K. S. K. Maathavan and S. Venkatraman, "A secure encrypted classified electronic healthcare data for public cloud environment," Intell. Autom. Soft Comput., vol. 32, no. 2, pp. 765–779, 2022, doi: 10.32604/iasc.2022.022276.

[15]. M. Vedaraj and P. Ezhumalai, "A secure IoT-Cloud based healthcare system for disease classification using neural network," Comput. Syst. Sci. Eng., vol. 41, no. 1, pp. 95–108, 2022, doi: 10.32604/csse.2022.019976.

[16]. Dalal, S., Seth, B., Jaglan, V. et al. An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks. Soft Comput 26, 5377–5388 (2022). https://doi.org/10.1007/s00500-022-07099-4

[17]. R. Shahin and K. E. Sabri, "A Secure IoT Framework Based on Blockchain and Machine Learning," Int. J. Comput. Digit. Syst., vol. 11, no. 1, pp. 671–683, 2022, doi: 10.12785/ijcds/110154.

[18]. Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4), e4108..

[19]. E. Tufan, C. Tezcan, and C. Acartürk, "Anomaly-based intrusion detection by machine learning: A case study on probing attacks to an institutional network," IEEE Access, vol. 9, pp. 50078–50092, 2021, doi: 10.1109/ACCESS.2021.3068961.

[20]. S. C. Buraga, D. Amariei, and O. Dospinescu, "An OWL-based specification of database management systems," Comput. Mater. Contin., vol. 70, no. 3, pp. 5537–5550, 2022, doi: 10.32604/cmc.2022.021714.

[21]. E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review," IEEE Access, vol. 7, pp. 13960–13988, 2019, doi: 10.1109/ACCESS.2019.2894819.

[22]. T. S. Riera, J.-R. B. Higuera, J. B. Higuera, J.-J. M. Herraiz, and J.-A. S. Montalvo, "A new multi-label dataset for Web attacks CAPEC classification using machine learning techniques," Comput. Secur., vol. 120, p. 102788, 2022, doi: 10.1016/j.cose.2022.102788.

[23]. Seth, B., Dalal, S., Le, D. N., Jaglan, V., Dahiya, N., Agrawal, A., ... & Verma, K. D. (2021). Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm. Computers, Materials & Continua, 67(1), 779-798..

[24]. R. Malik, Y. Singh, Z. A. Sheikh, P. Anand, P. K. Singh, and T. C. Workneh, "An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems," J. Adv. Transp., vol. 2022, 2022, doi: 10.1155/2022/7892130.

[25]. S. H. Javed, M. Bin Ahmad, M. Asif, S. H. Almotiri, K. Masood, and M. A. Al Ghamdi, "An Intelligent System to Detect Advanced Persistent Threats in Industrial Internet of Things (I-IoT)," Electron., vol. 11, no. 5, pp. 1–25, 2022, doi: 10.3390/electronics11050742.

[26]. X. Qiu, Z. Du, and X. Sun, "Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks," IEEE Access, vol. 7, pp. 172004–172011, 2019, doi: 10.1109/ACCESS.2019.2956480.

[27]. Rani, U., Dalal, S., & Kumar, J. (2018). Optimizing performance of fuzzy decision support system with multiple parameter dependency for cloud provider evaluation. Int. J. Eng. Technol, 7(1.2), 61-65.

[28]. S. Kristombu et al., "Automation in Construction Artificial intelligence and smart vision for building and construction 4 . 0 : Machine and deep learning methods and applications," Autom. Constr., vol. 141, no. June, p. 104440, 2022, doi: 10.1016/j.autcon.2022.104440.

[29]. P. Negro and C. Pons, "Artificial Intelligence techniques based on the integration of symbolic logic and deep neural networks: A systematic literature review," Intel. Artif., vol. 25, no. 69, pp. 13–41, 2022, doi: 10.4114/intartif.vol25iss69pp13-41.

[30]. J. Hegde and B. Rokseth, "Applications of machine learning methods for engineering risk assessment – A review," Saf. Sci., vol. 122, no. October 2019, p. 104492, 2020, doi: 10.1016/j.ssci.2019.09.015.

[31]. P. S. Pisa, B. Costa, J. A. Gonçalves, D. S. Varela de Medeiros, and D. M. F. Mattos, "A private strategy for workload forecasting on large-scale wireless networks," Inf., vol. 12, no. 12, pp. 1–15, 2021, doi: 10.3390/info12120488.

[32]. G. Rosenthal, O. E. Kdosha, K. Cohen, A. Freund, A. Bartik, and A. Ron, "ARBA: Anomaly and Reputation Based Approach for Detecting Infected IoT Devices," IEEE Access, vol. 8, pp. 145751–145767, 2020, doi: 10.1109/ACCESS.2020.3014619.

[33]. Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," Comput.

Secur., vol. 56, pp. 1–27, 2016, doi: 10.1016/j.cose.2015.09.009.

[34]. I. Idrissi, M. Azizi, and O. Moussaoui, "A Lightweight Optimized Deep Learning-based Host-Intrusion Detection System Deployed on the Edge for IoT," Int. J. Comput. Digit. Syst., vol. 11, no. 1, pp. 209–216, 2022, doi: 10.12785/ijcds/110117.

[35]. N. Nissim, A. Cohen, and Y. Elovici, "ALDOCX: Detection of Unknown Malicious Microsoft Office Documents Using Designated Active Learning Methods Based on New Structural Feature Extraction Methodology," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 3, pp. 631–646, 2017, doi: 10.1109/TIFS.2016.2631905.

