A hybrid cloud-based Intrusion Detection and Response System (IDRS) based on Grey Wolf Optimizer (GWO) and Neural Network (NN)

Ismail.M. NUR[1] and E. ÜLKER[2]

[1] Selcuk University, Konya/Turkey, ismailmohamednur@gmail.com
[2]Konya Technical University, Konya/Turkey, eulker@konyateknik.edu.tr

***Abstract* - The technology is growing rapidly and cloud computing usage is increasing. Most of the big and small companies use the cloud nowadays. Cloud computing has the economic benefit which is paid as you use (i.e. pay on the demand). With the increase of cloud usage, security problems on the cloud also increasing. Some mechanisms like firewall, vulnerability scanners and Intrusion Detection System (IDS) and other methods are used to mitigate the intrusions, but they are not enough to detect attacks against the cloud due to new intrusion releases. There are a variety of security methods for improving cloud security from threats and vulnerabilities. In this paper, a new hybrid cloud-based IDRS based on Grey wolf optimizer (GWO) and Neural Network (NN) is proposed to secure and detect intrusions over the cloud. GWO is one of the effective metaheuristic algorithms in many fields such as security. In this paper, GWO is employed to train an NN and the results are compared with other classification algorithms. For experimental results, most up-to-date intrusion detection datasets such as NSL-KDD and UNSW-NB15 are used.**

***Keywords* - Cloud computing, Grey wolf optimizer, Security, Intrusion Detection System.**

I. Introduction

Cloud computing (CC) is a service-based technology that depends on internet connection and central remote servers to use, store and process data and applications, providing users to access the data at a decreased cost and faster speed. It is often referred to by the relevant sources and recognized by the most adopted United States National Institute of Standards and Technology (NIST). NIST defined cloud computing as a model that allows access to a common collection of configurable resources of computing such as (computer networks, data storage, servers, services and applications etc.) at all times, on a suitable basis, and in any case, at anytime, anywhere [1].

Cloud computing is getting well-known in the last 10 years due to their offering good services such as advanced IT support, decreased price, maintenance, controlling, remote access and helping the companies to achieve their business aims easier and speedier. A report stated by Forrester says that the cloud computing market including services, cloud applications, and business administrations will arise to $236 billion in the year of 2020. Bain & Company researchers expect the market income of global cloud IT will reach $ 390 billion in 2020. SiliconANGLE also believes that cloud storage costs will arise to %16 CAGR between 2016 to 2026. In additions, IDC foretells that no less than half of IT using will be cloud-based in 2018, reaching 60% of all IT resources. Also, the cloud is relied on to become the most powerful/effective delivery component and the most preferred for IT sector.

The services provided over the cloud computing are defined as Anything as Service (XaaS). there are three fundamental components of cloud computing services: Software as a Service (SaaS) which developed for end-users and used on the web (e.g. Salesforce.com, Google's mail service, and Gmail). Platform as a Service (PaaS) which is a group of tools and services implemented to make programming/coding applications and distributing those applications efficiently and quickly (e.g. Salesforce1 and Google App Engine). Infrastructure as a Service (IaaS) which is main service that powers all the cloud (i.e. it contains hardware and software that powers all the cloud such as operating systems, storage, servers and networks) (e.g. Amazon EC2 and Windows Azure and Rackspace) [1].

Malware, phishing, DDoS, ransomware and others attacks happen on daily based. A business gets affected to a ransomware attack in every 40 seconds or maybe less. Cyber-attacks include misappropriation, loss of productivity, stolen money, theft of financial and personal data, intellectual property theft, destruction and damage of data, deletion of data and hacked systems. According to the 2017 White Hat's Report on Application Security, 30% of the violations reported in 2016 related to attacks on cloud/web applications [2].

In the year 2017 was marked by a large number of cyber-attacks. CIA Vault 7 hacking, WannaCry ransomware, and Equifax data breach have clearly shown the current vulnerabilities. The benchmark security capability of Cisco 2017 study observed that around a quarter of companies that have experienced an attack lost business opportunities [2]. One in five companies lost customers as a result of an attack and they lost approximately 30% revenue. For example, the breach of Equifax's credit data has resulted in the publication of a large number of personal names, driver's license numbers, Social Security and Mastercard resulting in losses and crucial misfortunes for the company and its customers [2].

Despite the many benefits of cloud computing, many companies still undecided about transferring their information to the cloud because of security risks and challenges. Firewalls, vulnerability scanners, and intrusion detection systems are employed for security over information systems. The use of any of these security mechanisms alone is not considered adequate in terms of security; because each one is focused on security aspects from different angles. Ensuring safety in the system requires that these mechanisms be used together to support each other. Moreover, cloud computing systems are focused on various management models to ensure the security [3]. Organizations and researchers are discovering new ways in which technologies such as machine learning can improve the ability to detect and respond to intrusion and analyze threat data more effectively/ efficiently.

An Intrusion Detection System (IDS) is the process that continuously monitors and analyzes the traffic and events that occur in a network or system, and then detects the harmful ones by checking packets getting in the system or network as an outcome. The system that IDS observes can be a network, a computer, or any information system source [4]. Such tools could help human-security analysts, who are already processing a large data sets and a deluge of security alerts every day, to better prioritize their security task.

In this paper, we investigate Grey Wolf optimizer to train neural networks to test the effectiveness of most up-to-date intrusion detection data set. The rest of the paper is structured as follows: the short review about intrusion detection in cloud security using machine learning approaches studied in section II, Methodology of neural networks, grey wolf optimizer, and GWO-NN is discussed in section III. Datasets and Experimental results are presented in section IV. Conclusion and planned work are in section V.

II. Related work

Due to its distributed nature, cloud environments are the target for attackers/intruders who are looking for possible security vulnerabilities. Most studies have shown that it is difficult to rely on cloud computing providers to ensure clients' data, confidentiality and privacy [5]. The security risks encountered in cloud computing are stated as data privacy and privacy protection, management inadequacy, possible security vulnerability in the management interface, cloud employees' malicious behavior, usability guarantee, isolation failure, compliance and legal risks [6]. Doelitzscher *at el.* an anomaly detection system for infrastructure as service clouds has been proposed. It is based on the analysis of the usage behavior of cloud clients. Neural networks have been used to analyze and learn the normal behavior of cloud clients, in order to detect anomalies that may arise from a cloud security incident introduced by an out-of-date virtual machine. This increases the transparency for Cloud clients regarding the security of their cloud instances and helps the Cloud Provider to detect infrastructure abuse. An anomaly detection model and simulation environment are implemented. Experiments approve that the effectiveness of the proposed system [7]. Bhamare et al investigated the UNSW dataset to train supervised machine learning models (Naïve Bayes, DTree J48, SVM-RBF, SVM-Polynomial, SVM-Linear and logistic regression (LR)). They then test these models with the ISOT dataset. They present their findings and argue that other applications in the field of machine learning are still needed for its applicability to cloud security [8]. Marwan *et al*. [9] proposed a new approach based on machine learning techniques to secure data processing in the cloud environment. In the experiment, support vector machines (SVM) and Fuzzy C-means Clustering (FCM) implemented to classify the image pixels more efficiently. Avdagic, I., & Hajdarevic, K. [10] used Microsoft's new technologies to provide a host and network framework for the cloud intrusion detection and prevention system. The purpose of the study was to suggest the use of the architecture to detect network anomalies and protect large amounts of data and traffic generated by cloud systems. He, Z., *et al*. [11] proposed a source-side DOS attack detection system in the cloud, based on machine learning techniques. This system uses statistical information from the cloud server hypervisor and virtual machines to prevent sending network packages to the external network. They evaluated nine machine learning algorithms and carefully compared their performance. The experimental results showed that more than 99.7% of the four types of DOS attacks were successfully detected. Their approach does not degrade performance and can be easily extended to larger DOS attacks. Zekri *et al*. [12] presented a DDoS mitigation system using the C.4.5 algorithm to prevent the threat of DDoS. The algorithm, coupled with signature detection techniques, generates a decision tree for automatically and effectively detecting signature attacks for DDoS flood attacks. To validate the system, other machine learning techniques selected and compared the results obtained. Arora, D., & Li, K. F. [13] showed how users can be classified into malicious and non-malicious categories based on the activities performed when accessing data residing on the cloud employing K-means algorithm as anomaly mitigation approach. In addition, it is demonstrated that by using a supervised learning algorithm such as SVM, it is possible to further classify malicious users into internal and external opponents. The results showed that machine learning algorithms are a promising solution in terms of identifying malicious and non-malicious users in a cloud infrastructure fast and efficiently.

III. Methodology

In this section, Neural Network (NN), Grey Wolf Optimizer (GWO) algorithm and the hybrid of both algorithms are explained.

A. NEURAL NETWORK(NN)

Neural Networks (NN) is one of the main classification algorithms in machine learning. The concept of NN was discovered by Warren McCulloch and Walter Pits in 1943 [14]. This algorithm is the inspiration of how human brain neurons work (i.e. how human brain cells interconnected and learn). We as human learn by examples then classify similar problems, and it is true for NN too. NN endeavors to explore an interconnection between the input and output of the given data set. Back-propagation algorithm is one of the first method used to adjust the weights and biases when training the NN to discover interconnection between input and output of the data. Different researchers proposed distinct versions of NN. Most popular types are Kohonen self-organizing network [15], Radial basis function (RBF) network [16], Spiking neural networks [17], Feed-forward network [18], Recurrent neural network [19].

In this study, we will implement multi-layer perceptron which is a feed forward neural network with one or more hidden layers. Figure 1 shows NN with 2 hidden layers. The neural networks equations used as follows [20]:

1. Firstly, inputs weighted totals are computed by Eq.1

$$S_j = \sum_{i=1}^{n} W_{ij} \cdot X_i - \theta_j, \quad j = 1,2,3,\ldots,h \quad \text{(Eq. 1)}$$

where n is the number of the inputs, W_{ij} shows the connection weight from the ith in the input layer to the jth in the hidden layer, X_i denotes as the ith input and θ_j is the bias of the jth hidden node.

2. The output of each hidden neuron is computed as below:

$$S_j = sigmod(S_j) = \frac{1}{\left(1 + exp(-S_j)\right)}, j = 1,2,3,\ldots,h \text{ (Eq. 2)}$$

3. The output(s) is/are computed based on hidden neurons output as below:

$$O_k = \sum_{i=1}^{h} W_{jk} \cdot S_j - \acute{\theta}_k, \quad k = 1,2,3,\ldots,m \quad \text{(Eq. 3)}$$

$$O_k = sigmod(O_k) = \frac{1}{\left(1 + exp(-O_k)\right)}, \quad k = 1,2,3,\ldots,m \text{ (Eq. 4)}$$

Where W_{jk} the connection weight from the j_{th} hidden layer to the k_{th} is output layer, and $\acute{\theta}_k$ is the bias of the kth output layer.

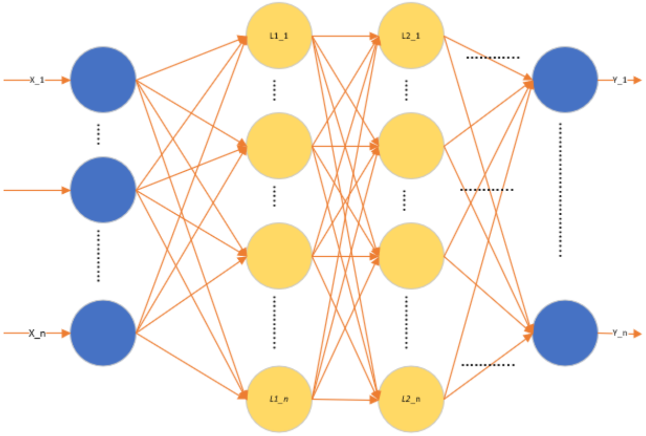

Figure 1: Neural Network for Multi-layer Perceptron design

B. GREY WOLF OPTIMIZER (GWO)

Grey wolf optimizer algorithm (GWO) was proposed by Mirjalili in 2014 [20]. It is bio-inspired of the hunting behavior and social leadership of grey wolves in nature. The GWO swarm split into four groups: alpha(α), beta(β), delta(δ), and omega(ω). The fittest wolves are alpha, beta and delta and they lead other wolves to the search space. The mathematical equations of circling formula defined in Eq.5, and Eq.6 [21].

$$D = |C \cdot X_p(t) - X(t)| \qquad \text{(Eq. 5)}$$

$$X(t+1) = X_p(t) - A \cdot D \quad \text{(Eq. 6)}$$

Where X is the wolf location and t is the number of loops. X_p is prey location and D is computed from Eq.1. A and C are coefficients computed based on [$A = 2a \cdot r_1 - a$] and $C = 2r_2$. The linearly decreased of $a = 2 - t(2/NLoops)$ is from 2 to 0 through the number of loops that used to manage the tradeoff exploration and exploitation of the wolves. r_1 and r_2 are random vectors between 0 and 1 employed to reveal optimal solution (for finding hunting prey).

$$X(t+1) = \frac{X_1 + X_2 + X_3}{3} \qquad \text{(Eq. 7)}$$

The values of X_1, X_2, and X_3 is evaluated as in equations (Eq.8), (Eq.9) and (Eq.10) respectively.

$$X_1 = X_\alpha - A_1 \cdot (D_\alpha) \qquad \text{(Eq. 8)}$$

$$X_2 = X_\beta - A_2 \cdot (D_\beta) \qquad \text{(Eq. 9)}$$

$$X_3 = X_\delta - A_3 \cdot (D_\delta) \qquad \text{(Eq. 10)}$$

The best three solutions in the population are X_1, X_2 and X_3 at iteration t. The equation of A and C are mentioned above. D_1, D_2, and D_3 are computed in Eq.11, Eq.12, and Eq.13 accordingly.

$$D_\alpha = |C_1 \cdot X_\alpha - X| \qquad \text{(Eq. 11)}$$

$$D_\beta = |C_2 \cdot X_\beta - X| \qquad \text{(Eq. 12)}$$

$$D_\delta = |C_3 \cdot X_\delta - X| \qquad \text{(Eq. 13)}$$

The GWO algorithm implementation as in below [20]:

1. Initialize a swarm of wolves randomly based on the upper bound and lower bound
2. Compute the corresponding objective value for each wolf
3. Select the first best 3 wolves and store as α, β, and δ
4. Update the location of the left of the swarm (ω) using equations Eq.7 to Eq.13
5. Update parameters a, A, and C
6. If the end criterion is not achieved then go back to step 2
7. Return the location of α as the best estimated optimum

MLP training is a challenging issue due to unknown search space and may vary datasets and inputs given to the MLP. We investigate how effective is GWO-NN on intrusion detection datasets.

C. GWO-NNN

Weights and biases are the most crucial variables in the training of the MLP. A trainer should obtain a batch of values for weights and biases that present the highest classification accuracy and minimum error. The weights and biases are computed as a vector of variables for this algorithm. GWO is used to get the fittest weight and biases.

The fitness of each vector is computed by using the Mean Square Error (MSE), which obtains the error between the actual input and desired output. Lower MSE points out the good model and better accuracy. Average of MSE is computed as follows:

$$MSE = \sum_{k=1}^{s} \frac{\sum_{i=1}^{m} \left(T_i^k - P_i^k\right)^2}{s} \qquad \text{(Eq. 14)}$$

Where s is the number of training samples, T_i^k is the actual output of ith input once kth training sample in the input and P_i^k is predicted output value of ith input once kth training sample employed. The data sets are preprocessed using normalization of min-max [0,1] then split into training and testing. GWO uses NN as fitness function and NN classifies the training data and returns average MSE to GWO. A GWO algorithm selects the best weights then NN uses those weights as shown in Figure 2.

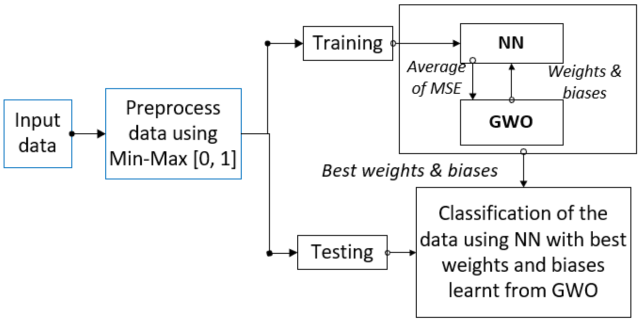
Input data
Preprocess data using Min-Max [0, 1]
Training
Testing
NN
GWO
Average of MSE
Weights & biases
Best weights & biases
Classification of the data using NN with best weights and biases learnt from GWO

Figure 2: GWO-NN architecture

IV. Results & discussion

In this experiment, the algorithms executed on Matlab2018, a system with a 2.50 GHZ Intel(R) Core (TM)i5 processor and 8 GB of RAM. The most recent intrusion detection data sets such as NSL-KDD and UNSW-NB15 data sets were used.

In 2009, a new version of KDD99 called NSL-KDD was published by Tavallaee M. et al [22]. The size of kdd99 was reduced and the duplicates removed. It has 125973 instants for training, 22544 instants for testing and 42 attributes the last attribute is the class which contains five classes one normal and five attacks (Probe, DoS, R2L and U2R). Moustafa Nour and Jill Slay created new data set for intrusion detection called UNSW-NB15 using IXIA PerfectStorm tools in 2015 [23]. It contains 49 attributes the last column is class which contains nine attacks and 1 normal, 175341 instants for training and 82332 for testing.

The result of GWO-NN compared with Naïve Bayes (NB), Multi-layer Perceptron with Back propagation (MLP-BP), Particle Swarm Optimization with NN (PSO-NN) and Gravitational Search Algorithm with NN (GSA-NN). The structure of NN used was *2 x N + 1* [21]. The selected population size of optimization algorithms was 100 and maximum iteration was 200. The implementation of the algorithms tested 15 executions on each and over of all results shown in Table 1 and Table 2.

Results on both data set as follows:

1. NSL-KDD

Table 1 results show that MLP-BP got the best accuracy of 97.38% but fails to avoid local optima. GWO-NN got the second best accuracy of 93% and avoided local optima. NB, PSO-NN and GSA-NN followed with the accuracy of 89.72%, 85.84%, and 68.24% respectively.

2. UNSW-NB15

In the results in Table 2, PSO-NN achieved the best accuracy of 100% and avoided local optima at MSE (0.00000 ± 3.055E-14). MLP-BP also got the good accuracy of 99.67% but still fails to prevent local optima. GWO-NN belonged good accuracy and prevented the local optima with MSE 0.00000 ± 2.687E-09. NB and GSA-NN have the lowest accuracy.

Table 1: Experimental results for NSL-KDD data set

Algorithms/Methods	Accuracy (%)	Mean Square Error (AVG ± STD)
NB	89.722 %	0.03081 ± 0.004045
MLP-BP	**97.380**%	0.02087 ± 0.001908
PSO-NN	85.844%	0.01267 ± 0.002598
GSA-NN	68.244%	0.05804 ± 0.014987
GWO-NN	**93** %	**0.01304** ± 0.004910

Table 2: Experimental results for UNSW-NB15 data set.

Algorithms/Methods	Accuracy (%)	Mean Square Error (AVG ± STD)
NB	86.93%	0.03913 ± 0.032450
MLP-BP	**99.67**%	0.00176 ± 0.002156
PSO-NN	**100**%	**0.00000 ± 3.055E-14**
GSA-NN	83.91%	0.04774 ± 0.003804
GWO-NN	**95.02**%	**0.00000 ± 2.687E-09**

In the experiment, NB was the fastest algorithm among all others during training. It is also observed that UNSW-NB15 data set is capable to use as intrusion detection data for cloud computing security. Moreover, the results showed that the combination of GWO and NN can detect attacks over the cloud.

V. Conclusion

With the widespread use of the Internet, there have been significant increases in security threats to information systems and expansions in the types of attacks. the necessity for the development of new mechanisms has arisen due to the threats and attacks. Cloud computing is facing many attacks on each day. In this article, Grey wolf optimizer and neural network algorithm have been evaluated to enhance cloud security. The results show that GWO-NN is able to detect intrusion over the cloud. UNSW-NB15 data set showed superior results compared with NSL-KDD data set.

Grey wolf feature selection based with neural network is planned to improve grey wolf performance for cloud security.

References

[1] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[2] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html#_Toc503317519 accessed June/2018

[3] Kumar, Akhilesh, Vinay Kumar, Prabhat Singh, and Awadhesh Kumar. "A Novel approach: Security measures and Concerns of Cloud Computing." *Akhilesh Kumar et al, Int. J. Computer Technology & Applications 3*, no. 3 (2012).

[4] Oktay, U., and O. K. Sahingoz. "Attack types and intrusion detection systems in cloud computing." In *Proceedings of the 6th International Information Security & Cryptology Conference*, pp. 71-76. 2013.

[5] Farcasescu, Marcela Roxana. "Trust model engines in cloud computing." In *2012 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2012)*, pp. 465-470. IEEE, 2012.

[6] Ken, R., D. Harris, J. Meegan, B. Pardee, Y. Le Roux, C. Dotson, E. Cohen, M. Edwards, and J. Gershater. "Security for cloud computing: 10 steps to ensure sucess." *Cloud Standards Customer Council (CSCC), Tech. Rep., August* (2012).

[7] Doelitzscher, Frank, Martin Knahl, Christoph Reich, and Nathan Clarke. "Anomaly detection in iaas clouds." In *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, vol. 1, pp. 387-394. IEEE, 2013.

[8] Bhamare, Deval, Tara Salman, Mohammed Samaka, Aiman Erbad, and Raj Jain. "Feasibility of Supervised Machine Learning for Cloud Security." In *Information Science and Security (ICISS), 2016 International Conference on*, pp. 1-5. IEEE, 2016.

[9] Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "Security Enhancement in Healthcare Cloud using Machine Learning." *Procedia Computer Science* 127 (2018): 388-397.

[10] Avdagic, Indira, and Kemal Hajdarevic. "Survey on machine learning algorithms as cloud service for CIDPS." In *Telecommunication Forum (TELFOR), 2017 25th*, pp. 1-4. IEEE, 2017.

[11] He, Zecheng, Tianwei Zhang, and Ruby B. Lee. "Machine learning based ddos attack detection from source side in cloud." In *Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on*, pp. 114-120. IEEE, 2017.

[12] Zekri, Marwane, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi. "DDoS attack detection using machine learning techniques in *cloud computing environments." In Cloud Computing Technologies and Applications (CloudTech), 2017 3rd International Conference of*, pp. 1-7. IEEE, 2017.

[13] Arora, Deepali, and Kin Fun Li. "Detecting anomalies in the data residing over the cloud." In *Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on*, pp. 541-546. IEEE, 2017.

[14] McCulloch, Warren S., and Walter Pitts. "A logical calculus of the ideas immanent in nervous activity." *The bulletin of mathematical biophysics* 5, no. 4 (1943): 115-133.

[15] T. Kohonen, “The self-organizing map,” *Neurocomputing*, vol. 21, no. 1–3, pp. 1–6, 1998.

[16] J. Park and I. W. Sandberg, “Approximation and radial-basis-function networks,” *Neural Computation*, vol. 3, no. 2, pp. 246–257, 1993.

[17] S. Ghosh-Dastidar and H. Adeli, “Spiking neural networks,” *International Journal of Neural Systems*, vol. 19, no. 4, pp. 295–308, 2009.

[18] G. Bebis and M. Georgiopoulos, “Feed-forward neural networks,” *IEEE Potentials*, vol. 13, no. 4, pp. 27–31, 1994.

[19] G. Dorffner, “Neural networks for time series processing,” *Neural Network World*, vol. 6, no. 1, pp. 447–468, 1996.

[20] Mirjalili, Seyedali, Seyed Mohammad Mirjalili, and Andrew Lewis. "Grey wolf optimizer." *Advances in engineering software* 69 (2014): 46-61.

[21] Mirjalili, Seyedali. "How effective is the Grey Wolf optimizer in training multi-layer perceptrons." *Applied Intelligence* 43, no. 1 (2015): 150-161.

[22] Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "A detailed analysis of the KDD CUP 99 data set." In *Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on*, pp. 1-6. IEEE, 2009.

[23] Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." In *Military Communications and Information Systems Conference (MilCIS), 2015*, pp. 1-6. IEEE, 2015.