Intrusion Detection Systems Based on Machine Learning Algorithms

Article · August 2021

CITATIONS
0

READS
660

4 authors:

Adnan Mohsin Abdulazeez
Duhok Polytechnic University
187 PUBLICATIONS **2,118** CITATIONS
SEE PROFILE

Yusur Falah
Al-Mustansiriya University
12 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Falah Y H Ahmed
Sohar University
53 PUBLICATIONS **282** CITATIONS
SEE PROFILE

Diyar Zeebaree
Duhok Polytechnic University
95 PUBLICATIONS **1,126** CITATIONS
SEE PROFILE

2021 IEEE International Conference on Automatic Control & Intelligent Systems (I2CACIS) | 978-1-6654-0343-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/I2CACIS52118.2021.9495897

Intrusion Detection Systems Based on Machine Learning Algorithms

Sandy Victor Amanoul
Information Technology Dept.
Duhok polytechnic University
Duhok, Iraq
sandy.victor@dpu.edu.krd

Adnan Mohsin Abdulazeez
Research Center of Duhok
Polytechnic University
Duhok polytechnic University
Duhok,Iriq
adnan.mohsin@dpu.edu.krd

Diyar Qader Zeebare
Research Center
Duhok Polytechnic University
Duhok, *Kurdistan Region, Iraq*
dqszeebaree@dpu.edu.krd

Falah Y. H. Ahmed
Faculty of Information Sciences
& Engineering, Management &
Science University, Shah Alam,
Selangor, Malaysia
falah_ahmed@msu.edu.my

***Abstract*— Networks are important today in the world and data security has become a crucial area of study. An IDS monitors the status of the software and hardware of the network. Curing problems for current IDSs remain they improve detection precision, decrease false alarm rates and track unknown attacks after decades of advancement. Many researchers have focused on the development of IDSs using machine learning approaches to solve the above-described problems. With the high precision of computer teachings, the basic distinctions between usual and irregular data can be recognized automatically. Unknown threats may also be detected because of their generalizability via machine learning system. This paper suggests a taxonomy of IDS, which uses the primary dimension of data objects to classify and sum up IDS literatures based on and dependent on deep learning. We assume this kind of taxonomy is sufficient for researchers in cyber security. We selected three algorithms from machine learning (Bayes Net, Random Forest, Neural Network) and two algorithms of deep learning (RNN, LSTM), and we tested them on KDD cup 99 and evaluated accuracy algorithms, and we used a program WEKA To calculate the accuracy.**

Keywords— intrusion detection system; Kddcup99; machine learning; deep learning.

I. INTRODUCTION

In today's world, there has been great progress and development in communication technologies and the Internet, and one of the most important areas in which it has appeared is network security. It uses instruments like firewalls, antivirus software and intrusion detection systems to ensure a network protection and all its related resources in the Internet (IDS) [1]. These approaches protect networks from both domestic and external threats. An IDS is a detect device that tracks the state of a network's software and hardware and helps protect cyber security [2] [3] [4]. However, several Intrusion detection systems still have a high false alarms, creating numerous warnings for low-threat cases, adding to protection analysts' workload and potentially causing serious attacks to go unnoticed [5]. As a consequence, unknown attacks must be identified by IDSs [6].

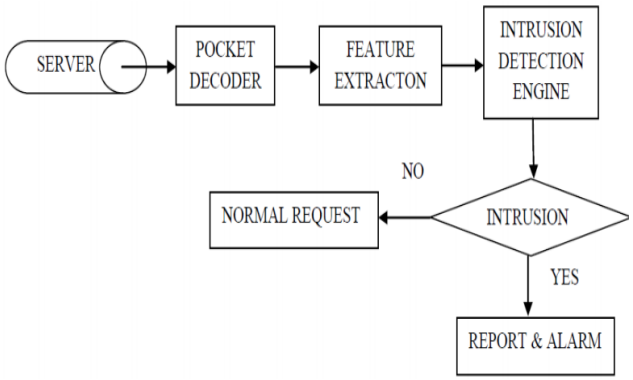

Fig. 1. Intrusion Detection process.

Researchers have started to focus on the construction of machine-learning (ML) techniques because it is an intelligent technology to retrieve precious knowledge automatically from massive datasets [7] [2] [8]. When sufficient training data is available, IDSs can achieve good levels of sensing and machine learning models are sufficiently generalized to detect attacks. In addition, ML does not rely largely on the domain knowledge, making it easy to design and build [9].

Deep learning (DL) can produce excellent results. A distinctive feature of DL is the deep structure that comprises several hidden layers. On the other hand, typical models are either without hidden layers or have only one [10] [11] [12].

This article makes three major contributions.
We have conducted a systematic review of IDS and how they are used with the ML-DL algorithms that have been done during the last two years and discussed each article in terms of strength, weakness and evaluation criteria used, then we applied the algorithms and finally found a difference in accuracy between them.

II. Related Work

Different relative analyses in different classification systems were carried out, but no single methodology was preferred to others. Topics like consistency, time of workout, scalability, and many more help find the correct classification system.

Shone et al.[14] Suggested an auto-encoder (AE) and ML technique RF-based IDS. Only the encoder component of AE used to make the model function in a nonsymmetric manner, making it effective in computation and time. For classification, RF used. The KDD Cup '99 and NSL-KDD datasets were used in experiments for multiclass classification scenarios. The proposed approach outperformed the Deep Belief Network (DBN) in terms of accuracy rate and decreased training time. However, it was ineffective at detecting R2L and U2R attacks.

Khan et al.[15] Suggested two method depended on solid and efficient stacked auto-encoder AE. The proposed model's output evaluated. Down sampling was used for the KDD Cup'99 to eliminate duplicate data. Up sampling of the dataset using SMOTE. The performance of attack classes with fewer training instances increases significantly due to this pre-processing of the dataset.

Xiao et al. [16] Suggested a CNN-based powerful IDS. The key concept is to use Principal Component Analysis and auto-encoder AE to extract features first. The single vector became a two-dimensional matrix that was fed into the CNN. Experiments Prove it is accurate in terms of the amount of time algorithms take to train and evaluate. The biggest disadvantage is that the U2R and R2L attack classes have lower detection rates than other attack classes.

Yao et al.[17] Suggested a multilevel semi-supervised ML (MSML) Model that consists of Four modules in the proposed solution. If an intrusion in one module is not found, it will be redirected to the next. The dataset of the KDD Cup'99 was used to validate the methodology suggested. Except in low data cases, test results revealed that the model is superior for attack detection.

Vinayakumar et al.[18] Proposed hybrid-scalable DNN network for host and network intrusion detections. Net The modular architecture based on the computer platform117 Apache Cluster. The proposed NIDS model was tested on open data sites. Findings from exteriors prove the benefits of the model about other algorithms obtained by lNSL-KDD.

Andresini et al. [19] Used the auto-encoder AE idea to propose an ID-convolution layer multi-stage model of two fully connected layers on top of the other one. first stage phase, 2 of EIs and checked using standard and flows of attack to reproduce Sampling. These newly rebuilt samples are used to generate an additional, supervised 1D-CNN dataset. finally, the data set is categorized by a SoftMax layer. KDD Cup'99 experiments, UNSWNB15 and CICIDS 2017 data set showed the outperformance of other DL models in the proposed solution. They have not really demonstrated how good that performs for minority communities. The second drawback is that it doesn't detail the characteristics of the attack.

TABLE I. COMPARISON BETWEEN METHODOLOGY, AND EVALUATION FROM DIFFERENT STUDIES

CITATION	ALGORITHM	METHODOLOGY	DATASET	EVALUATION
[14]	ML-DL	Random Forest with Non-Symmetric Deep Auto Encoder	KDD Cup'99 NSL-KDD	ACC \ PRE \ REC \ F-M \ FAR
[15]	DL	Two-Stage Model using Stacked Auto Encoder	KDD Cup'99 UNSW-NB15	ACC \ PRE\REC \ F-M \ FAR
[16]	DL	Convolutional Neural Network with Principal component analysis (PCA) and Auto Encoder for dimension reduction	KDD Cup'99	ACC \ REC \FAR
[17]	ML	A Multilevel Model based on K-Means Clustering and Random Forest	KDD Cup'99	ACC \ PRE \ REC \ F-M
[18]	DL	Model based on Fully Connected Networks (FCNs), Variational Autoencoder (VAE), and Sequence-to-Sequence (Seq2Seq) structures	KDD Cup'99 NSL-KDD Kyoto 2006+ UNSW-NB15 CICIDS2017	ACC \ PRE\ REC\ F-M
[19]	DL	Multistage Auto Encoder and CNN	KDD Cup'99 UNSW-NB15 CICIDS2017	ACC\ F-M

III. IDS CONCEPT

Intrusion is an illegal or undesirable attempt to obtain access to computer networks' details or damage the device. An IDS is a cybersecurity software that detects a wide range of security violations, from external attempts to interference with the insider system's intrusion and malpractices [20] [21].

The primary functions of IDSs are hosts and networks monitored, the computer system's behaviour, alerts generated, and unusual activities responded to. IDSs are generally installed near the stable network nodes because the hosts and networks are tracked [22] [23].

Methods of IDS classification split into two categories: Methods focused on identification and techniques based on data source. Detection of misuse and detection of abnormality are two examples of IDS-based detection approaches. In host and network methods, IDSs can be broken into data source-based methods [24] as show in fig.2.

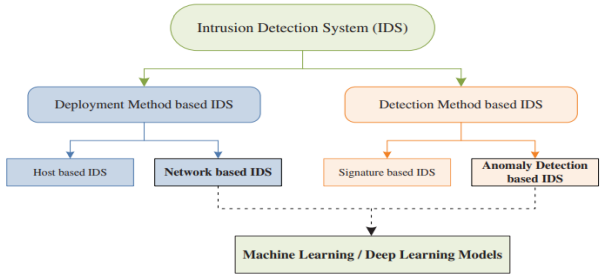

Fig. 2. Taxonomy system of IDS.

A. Detection Methods

Another term for misuse detection is a signature-based recognition. The detection mechanism uses a signature database to adapt to the sample signatures. A low fake warning rate and the ability to view attack types and possible triggers are the advantages of misuse detection [25].

B. Source Of Data

Host-based IDS are capable of monitoring the behaviours, they can detect intrusions and deliver correct answers. Host-based IDS are Could not detect network attacks due to the host's stability and use of Host Resources. The majority of networked IDSs are used in various operating systems. Unique protocol types and attacks can also be identified by network-based IDs. [25] [26].

IV. MATERIALS AND METHODOLOGY

The dataset KDD CUP 99 is chosen as the basis for the planned discovery scheme. Around 4.900,000 single connection vectors are used in the KDD training data collection, each of these 41 features being labelled an attack or normal, showing the approximation to identified attacks. It is necessary to note that the experimental results are not in the same probability division as training data. In datasets there are 24 types of exercise attacks, with 14 more types of test attacks [27] [28] [29]. The simulated attacks can classify into one of four groups:

- DOS**:** Various forms of attacks, such as SYN flood, are involved [30].
- R2L: It does not have allowed remote access [31].
- U2R: unauthorized access to superuser rights on a local system [32].
- Probing**:** Monitoring and examination [33].

In this Study convert the KDD CUP 99 dataset from the CSV group to the ARFF position in the pre-processing stage. the KDD CUP 99 dataset pre-processed into 22 assault subcategories Instead of inflated 5 attack classes .

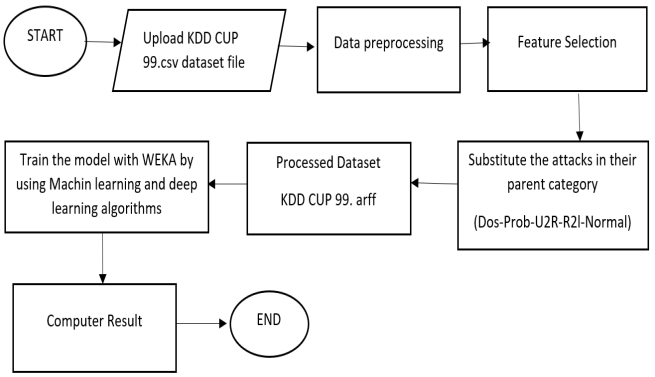

Fig. 3. Research Methodology

Three machine learning algorithms were selected and implemented for IDS.

A. Bayes Net

The model Bayes Net uses a directional graph with unique borders, which displays relationships, and allows anyone to deduce random variables efficiently [34]. That is also called the chain rule of probability.

$$p(\bigcap_{k=1}^{n} A_k) = \prod_{k=1}^{n} p(A_k \mid \bigcap_{j-1}^{k=1} A_j) \quad (1)$$

Further, the conditional freedom of two random variables, A and B is equal to meeting the following property in case of another random variable C [35] [36].

$$P(A, B|C) = (P(A|C) * P(B|C)) \quad (2)$$

B. Random forest

One of supervised learning algorithm is Random forest that can bused to classify and predict data. It is, however, mostly used to solve classification problems. The random forest algorithm generates decision trees from data samples, then gets predictions from each of them before voting on the best solution. It is an ensemble approach superior to a single decision tree because it averages the results to minimize over-fitting. A random sample of dataset is used for the construction of trees. Random function sub-sets are regarded when dividing node C [37] [38] [39] as seen in fig. 4.

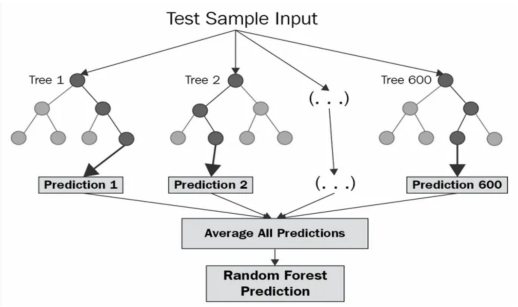

Fig. 4. Random forest Architecture

A random selection of training means that each tree learns from a random sample of data points during the training phase. When these samples drawn with substitution, a process known as bootstrapping, and predictions made by combining each decision tree's predictions at test time, the results are known as bootstrapping. Bagging is the preparation method for each student in different data sub-sets before estimating the predictions. [40] [41].

C. Neural Network

A computer learning system uses a function network to recognize and translate data entries into a desired result in one output the neural network can be used as a part to transform complicated data into a format that computers can understand in different machine learning algorithms. Recognition of the speech and picture, spam email filtering [42] [43].

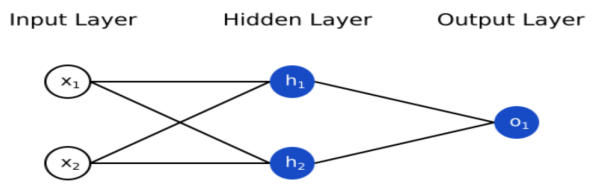

Fig. 5. Neural Network Architecture

We have selected two algorithms for deep learning, and they are RNN and LSTM.

A. *Recurrent Neural Network (RNN)*

Is a form of artificial neural network which works with data from the sequence or time series [47,47]. These profound learning algorithms are widely used in common or temporary issues like language translation and natural language processing (nlp) as show in fig.6. It's in popular apps like Siri, voice, and translates with Google [4].

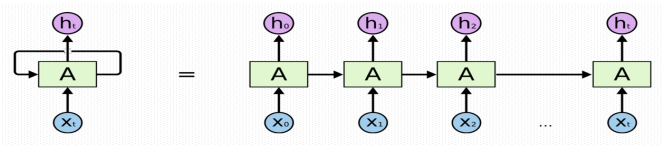

Fig. 6. RNN Architecture

B. *Long Short-Term Memory Networks (LSTMs)*

LSTMs are a form of RNN that can learn and remember them. The default tendency is to recall past knowledge for long periods. LSTMs keep track of data over time. Since they recall previous inputs, they are useful in time-series prediction [44].

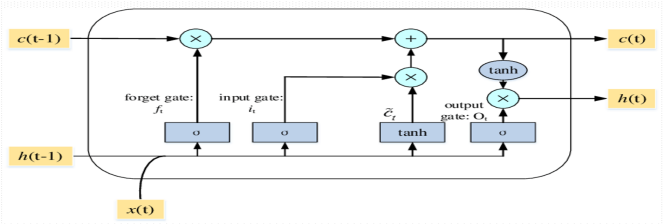

Fig. 7. LSTMs Architecture

V. EVALUATION METRICS

Assessment of performance metrics for IDS based on uncertainty matrix values for ML and DL approaches [3].

False alarm rate**:** It is often called false-positive and is defined as a percentage to all normal samples with wrongly expected attack samples. [16].

$$\text{Accuracy of False Rate} = \frac{\text{False Positive}}{\text{False Positive+True Negavtive}} \quad (3)$$

True negative rate: It is the right number of normal samples divided by the overall number of normal samples [5].

$$\text{Accuracy of True Rate} = \frac{\text{True Negative}}{\text{Trie Negative+False Postive}} \quad (4)$$

Precision: It's the ratio of correctly expected Attacks to all Attacks samples[40] [45].

$$\text{Precision} = \frac{True\ Postive}{True\ Postive + False\ Postive} \quad (5)$$

Recall: It's the proportion of all Attacks samples correctly listed to all Attacks samples that are Attacks. It's also known as a Detection Rate[5,49].

$$\text{Recall} = \frac{\text{True Postive}}{\text{True Postive+False Negative}} \quad (6)$$

F-Measure: Precision and Recall are combined to form the harmonic mean. To put it another way, it's a mathematical method for evaluating a system's accuracy by taking into account both precision and recall [46,50].

$$\text{F} - \text{Measure} = 2\frac{\text{Precision}*\text{Recall}}{\text{Precision+Recall}} \quad (7)$$

VI. EXPERIMENTAL RESULTS AND DISCUSSION

According to the methodology that we previously defined, we have implemented deep learning algorithms (BayesNet-Random Forest-Neural Network) and deep learning algorithms (RNN-LSTM) on a data set (KDD CUP 99) Using program WEKA, we obtained different results as seen in the below tables.

TABLE II. ACCURACY USING ALGORITHMS OF ACCURACY ML DIFFERENT CUP 99 DATASET.

S.N.	ML algorithms	Accuracy	Time in Seconds
1	**BayesNet**	98.7869%	17.57
2	**Random forest**	99.9824%	342.35
3	**Neural Network**	99.3583%	1505.58

The accuracy difference between these algorithms is not significant, as seen in the table above. With little difference from most of the algorithms, the random forest algorithm community scored the maximum precision with 99.98 %. The random forest algorithm can detect IDS attacks, as shown in table II. Similarly, the Neural Network algorithms obtained good results, but they take a long time because we have used four neural network layers that means if we use more layers, the accuracy will be better, but the time takes will be more.

TABLE III. RESULT OF ALL EVALUATION METRICS BY USING RANDOM FOREST

Class	TP Rate	FP Rate	Precision	Recall	F-Measure
Normal	1.000	0.000	0.999	1.000	1.000
U2R	0.615	0.000	0.889	0.615	0.727
Dos	1.000	0.000	1.000	1.000	1.000
R2L	0.981	0.000	0.992	0.981	0.987
Probe	0.993	0.000	0.999	0.993	0.996

TABLE IV. COMPARISON OF ACCURACY USING DIFFERENT DL ALGORITHMS ON KDD CUP 99 DATASET

S.N.	DL algorithms	Accuracy	Time in Seconds
1	**RNN**	53.1857%	47.92
2	**LSTM**	64.2628%	24.99

The difference in performance accuracy between these algorithms was huge, and the RNN algorithm was ineffective in this dataset. When the LSTM algorithm is implemented, the model performance improves well; as shown in Table III, the accuracy of LSTM is 64.26 % which is higher than the accuracy of RNN with an accuracy of 53.18%. As explained in table IV, LSTM can detect IDS attacks more precisely the RNN algorithm.

TABLE V. RESULT OF ALL EVALUATION METRICS BY USING ISTM

Class	TP Rate	FP Rate	Precision	Recall	F-Measure
Normal	0.113	0.217	0.113	0.113	0.113
U2R	0.000	0.000	0.000	0.000	0.000
Dos	0.783	0.880	0.773	0.783	0.778
R2L	0.000	0.000	0.000	0.000	0.000
Probe	0.000	0.000	0.000	0.000	0.000

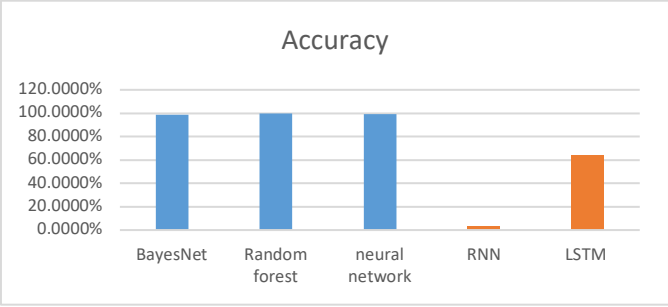

Fig. 8. Accuracy analysis of all algorithms

When implementing the ML and DL methods that we chose and experimented with on the KDD cup 99 datasets, it was found that machine learning performed better on this dataset, while Deep learning spent less time implementing the model while Neural network took the longest time because it contains four-layer, but It also recorded the second-highest accuracy. While the algorithm **Random forest** recorded the highest accuracy 99.3583% and the algorithm **RNN** the least accurate 53.1857%.

VII. CONCLUSION

Intrusion Detection System plays a very important and vital role in the field of network security. The performance of the classifier is degrading by using intrusive patterns, accuracy and also, it's time-consuming. Bayes Net, Random Forest, Neural Network, RNN, and LSTM are among the ML and DL algorithms considered for IDS. The KDDcup99 dataset used to value these accounts. With the KDD cup 99 dataset's aid, we proposed a DL and ML approach. By looking at the results that depend on accuracy, the powerful classifier can be identified. It seems reasonable that the random forest classifier outperforms better with accuracy of 99.98% based on the results.

REFERENCE

[1] R. A. K. AlMeshal, "A comparative study for Intrusion Detection Metods Using Machine Learning," p. 13.

[2] M. H. Ali, B. A. D. Al Mohammed, A. Ismail, and M. F. Zolkipli, "A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization," IEEE Access, vol. 6, pp. 20255–20261, 2018, doi: 10.1109/ACCESS.2018.2820092.

[3] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2018, doi: 10.1109/TETCI.2017.2772792.

[4] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[5] D. Agrawal, C. Agrawal, and H. Yadav, "A Machine Learning Based Intrusion Detection Framework Using KDDCUP 99 Dataset," vol. 4, no. 6, p. 11.

[6] R. Taheri, M. Ahmadzadeh, and M. R. Kharazmi, "A New Approach For Feature Selection In Intrusion Detection System," p. 15.

[7] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, "A new feature selection model based on ID3 and bees algorithm for intrusion detection system," p. 8.

[8] D. M. Abdulqader, A. M. Abdulazeez, and D. Q. Zeebaree, "Machine Learning Supervised Algorithms of Gene Selection: A Review," vol. 62, no. 03, p. 13, 2020.

[9] R. Vijayanand, D. Devaraj, and B. Kannapiran, "A Novel Deep Learning Based Intrusion Detection System for Smart Meter Communication Network," in *2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, Tamilnadu, India, Apr. 2019, pp. 1–3. doi: 10.1109/INCOS45849.2019.8951344.

[10] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Systems with Applications*, vol. 42, no. 5, pp. 2670–2679, Apr. 2015, doi: 10.1016/j.eswa.2014.11.009.

[11] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1690–1700, Mar. 2014, doi: 10.1016/j.eswa.2013.08.066.

[12] F. A. M. Bargarai, A. M. Abdulazeez, V. M. Tiryaki, and D. Q. Zeebaree, "Management of Wireless Communication Systems Using Artificial Intelligence-Based Software Defined Radio," *Int. J. Interact. Mob. Technol.*, vol. 14, no. 13, p. 107, Aug. 2020, doi: 10.3991/ijim.v14i13.14211.

[13] D. M. Manimekalai and G. Anupriya, "A Novel Intrusion Detection System using Data Mining Techniques," vol. 6, no. 6, p. 5, 2019.

[14] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2018, doi: 10.1109/TETCI.2017.2772792.

[15] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "TSDL: A Two-Stage Deep Learning Model for Efficient Network Intrusion Detection,"

IEEE Access, vol. 7, pp. 30373–30385, 2019, doi: 10.1109/ACCESS.2019.2899721.

[16] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," *IEEE Access*, vol. 7, pp. 42210–42219, 2019, doi: 10.1109/ACCESS.2019.2904620.

[17] H. Yao, D. Fu, P. Zhang, M. Li, and Y. Liu, "MSML: A Novel Multilevel Semi-Supervised Machine Learning Framework for Intrusion Detection System," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1949–1959, Apr. 2019, doi: 10.1109/JIOT.2018.2873125.

[18] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[19] G. Andresini, A. Appice, N. D. Mauro, C. Loglisci, and D. Malerba, "Multi-Channel Deep Feature Learning for Intrusion Detection," *IEEE Access*, vol. 8, pp. 53346–53359, 2020, doi: 10.1109/ACCESS.2020.2980937.

[20] J. Gu and S. Lu, "An effective intrusion detection approach using SVM with naïve Bayes feature embedding," *Computers & Security*, vol. 103, p. 102158, Apr. 2021, doi: 10.1016/j.cose.2020.102158.

[21] A. M. Abdulazeez and F. S. Khamo, "A Proposed Data Security Algorithm Based on Cipher Feedback Mode and its Simulink Implementation," vol. 4, no. 9, p. 10, 2013.

[22] H. Wang, J. Gu, and S. Wang, "An effective intrusion detection framework based on SVM with feature augmentation," *Knowledge-Based Systems*, vol. 136, pp. 130–139, Nov. 2017, doi: 10.1016/j.knosys.2017.09.014.

[23] N. Gao, L. Gao, Q. Gao, and H. Wang, "An Intrusion Detection Model Based on Deep Belief Networks," p. 6.

[24] A. Pal Singh and M. Deep Singh, "Analysis of Host-Based and Network-Based Intrusion Detection System," *IJCNIS*, vol. 6, no. 8, pp. 41–47, Jul. 2014, doi: 10.5815/ijcnis.2014.08.06.

[25] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[26] M. E. Aminanto and K. Kim, "Deep Learning in Intrusion Detection System: An Overview," p. 12.

[27] K. Alrawashdeh and C. Purdy, "Toward an Online Anomaly Intrusion Detection System Based on Deep Learning," in *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Anaheim, CA, USA, Dec. 2016, pp. 195–200. doi: 10.1109/ICMLA.2016.0040.

[28] S. KishorWagh, V. K. Pachghare, and S. R. Kolhe, "Survey on Intrusion Detection System using Machine Learning Techniques," *IJCA*, vol. 78, no. 16, pp. 30–37, Sep. 2013, doi: 10.5120/13608-1412.

[29] D. Q. Zeebaree, A. M. Abdulazeez, D. A. Zebari, H. Haron, and H. N. A. Hamed, "Multi-Level Fusion in Ultrasound for Cancer Detection Based on Uniform LBP Features," p. 21, 2021.

[30] K. A. Taher, B. Mohammed Yasin Jisan, and Md. M. Rahman, "Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection," in *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*, Dhaka, Bangladesh, Jan. 2019, pp. 643–646. doi: 10.1109/ICREST.2019.8644161.

[31] S. M. Sohi, J.-P. Seifert, and F. Ganji, "RNNIDS: Enhancing network intrusion detection systems through deep learning," *Computers & Security*, vol. 102, p. 102151, Mar. 2021, doi: 10.1016/j.cose.2020.102151.

[32] C. Kalimuthan and J. Arokia Renjit, "Review on intrusion detection using feature selection with machine learning techniques," *Materials Today: Proceedings*, vol. 33, pp. 3794–3802, 2020, doi: 10.1016/j.matpr.2020.06.218.

[33] C. A. M. and R. K., "Performance evaluation of data clustering techniques using KDD Cup-99 Intrusion detection data set," *IJINS*, vol. 1, no. 4, pp. 294–305, Sep. 2012, doi: 10.11591/ijins.v1i4.821.

[34] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," *Applied Sciences*, vol. 9, no. 20, p. 4396, Oct. 2019, doi: 10.3390/app9204396.

[35] Y. Xin *et al.*, "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[36] Y. Jia, M. Wang, and Y. Wang, "Network intrusion detection algorithm based on deep neural network," *IET Information Security*, vol. 13, no. 1, pp. 48–53, Jan. 2019, doi: 10.1049/iet-ifs.2018.5258.

[37] J. Li, Y. Qu, F. Chao, H. P. H. Shum, E. S. L. Ho, and L. Yang, "Machine Learning Algorithms for Network Intrusion Detection," in *AI in Cybersecurity*, vol. 151, L. F. Sikos, Ed. Cham: Springer International Publishing, 2019, pp. 151–179. doi: 10.1007/978-3-319-98842-9_6.

[38] Y. Pacheco and W. Sun, "Adversarial Machine Learning: A Comparative Study on Contemporary Intrusion Detection Datasets:," in *Proceedings of the 7th International Conference on Information Systems Security and Privacy*, Online Streaming, --- Select a Country ---, 2021, pp. 160–171. doi: 10.5220/0010253501600171.

[39] B. Charbuty and A. Abdulazeez, "Classification Based on Decision Tree Algorithm for Machine Learning," *JASTT*, vol. 2, no. 01, pp. 20–28, Mar. 2021, doi: 10.38094/jastt20165.

[40] G. Meena and R. R. Choudhary, "A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA," in *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, Jaipur, India, Jul. 2017, pp. 553–558. doi: 10.1109/COMPTELIX.2017.8004032.

[41] P. S. Bayerl, R. Karlović, B. Akhgar, and G. Markarian, Eds., *Community Policing - A European Perspective: Strategies, Best Practices and Guidelines*. Cham: Springer International Publishing, 2017. doi: 10.1007/978-3-319-53396-4.

[42] A. Özgür and H. Erdem, "A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015," PeerJ Preprints, preprint, Apr. 2016. doi: 10.7287/peerj.preprints.1954v1.

[43] R. Prasad and V. Rohokale, *Cyber Security: The Lifeline of Information and Communication Technology*. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-31703-4.

[44] O. Ahmed and A. Brifcani, "Gene Expression Classification Based on Deep Learning," in *2019 4th Scientific International Conference Najaf (SICN)*, Al-Najef, Iraq, Apr. 2019, pp. 145–149. doi: 10.1109/SICN47020.2019.9019357.

[45] N. Asaad Zebari, D. Asaad Zebari, D. Qader Zeebaree, and J. Najeeb Saeed, "Significant features for steganography techniques using deoxyribonucleic acid: a review," *IJEECS*, vol. 21, no. 1, p. 338, Jan. 2021, doi: 10.11591/ijeecs.v21.i1.pp338-347.

[46] Zajmi, L., Ahmed, F. Y., & Jaharadak, A. A. (2018). Concepts, methods, and performances of particle swarm optimization, backpropagation, and neural networks. Applied Computational Intelligence and Soft Computing, 2018.

[47] Ahmed, F. Y., al Thiruchelvam, M., & Fong, S. L. (2019, June). Improvement of Vehicle Management System (IVMS). In 2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS) (pp. 44-49). IEEE.

[48] Ahmed, F. Y., Sreejith, R., & Abdullah, M. I. (2021, April). Enhancement of E-Commerce Database System During the COVID-19 Pandemic. In 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) (pp. 174-179). IEEE.

[49] Alkawaz, M. H., Segar, S. D., & Ali, I. R. (2020). A Research on the Perception and use of Electronic Books Among it Students in Management & Science University. In 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA) (pp. 52-56). IEEE.

[50] Alkawaz, M. H., Rajandran, H., & Abdullah, M. I. (2020). The Impact of Current Relation between Facebook Utilization and E-Stalking towards Users Privacy. In 2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS) (pp. 141-147). IEEE.