ISSN: 0974-8571 Vol.14 No. 1 June, 2022

International Journal of Computational Intelligence in Control

Network Intrusion Detection by using Machine Learning Technique

Muhammad Fahim[1], Ali Shahid[2], Abdullah Shabib[3], Malik Yasir Abbas Chan[4] , Muhammad Atif Abdulrazzaq [5]
fahimkhan_sehwag@yahoo.com ,Alishahid1984@gmail.com ,abdullahshabib483@gmail.com ,malikyasirabbas@hotmail.com ,muhammad.atif.janjuah@gmail.com

[1]Cloud and Infrastructure Service (CIS), Wipro Arabia Ltd, Al-Khobar, Saudi Arabia
[2]Security Department, SAS Systems Engineering, Jeddah, Saudi Arabia
[3]Huawei IP NOC, Mobile business company, Riyadh, Saudi Arabia
[4] iot & ai DevSecOps, E& Enterprise iot & ai DWC-LLC, Sharjah, UAE
[5]Siemens smart infrastructure, Saudi networker services, Al-Khobar, Saudi Arabia

Corresponding author : alishahid1984@gmail.com

Abstract: **The exponential growth of the World Wide Web, coupled with surging network traffic, has significantly increased the risk of security breaches. Cyber attackers frequently exploit vulnerabilities within network infrastructures to gain unauthorized access to sensitive information. To safeguard digital environments, Network Intrusion Detection Systems (NIDS) play a pivotal role in accurately detecting various cyberattacks and ensuring timely protection of network resources. Incorporating advanced machine learning techniques further enhances the detection of anomalous behavior within network traffic, addressing modern security challenges more effectively. However, with the ever-evolving sophistication of cyber threats, traditional NIDS often struggle to identify newly emerging attacks. In response to this challenge, the present study focuses on detecting network intrusions through a robust machine learning framework, specifically employing the Random Forest algorithm. The NIDS is developed and trained on the comprehensive UNSW-NB15 dataset, which encapsulates diverse and up-to-date instances of network traffic and attack patterns. Additionally, the Extra Trees classifier is utilized to extract the most significant features from the dataset, optimizing the model's performance. The findings reveal that the Random Forest method achieves an impressive accuracy rate of 99.10% in classifying binary network attacks. Extensive experimental evaluations further demonstrate that Random Forest outperforms conventional Machine Learning based approaches in terms of detection efficiency and reliability.**

Keywords: Network Attacks, Network Intrusion Detection System (NIDS), Deep Neural Networks, Extra Tree Classifier, Activation Function, UNSW-NB15 dataset

1. Introduction

In today's highly interconnected and technologically advanced world, data and network security challenges are rising at an exceptional pace. The primary reason behind this surge in security threats are the exponential growth of network traffic and rapid technological developments, both of which

have contributed to the emergence of sophisticated attack vectors that continue to evolve in scale and complexity [1][2]. The modern digital ecosystem faces numerous threats to network security, necessitating the deployment of various Intrusion Detection Systems (IDS) that are specifically designed to detect and mitigate such attacks in real time. An IDS operates as a surveillance mechanism, continuously monitoring network activity to identify abnormal patterns of behavior and issuing alerts when potential intrusions are detected. Upon receiving such alerts, security operations center (SOC) analysts investigate the flagged incidents and undertake appropriate mitigation measures to neutralize the threats.

However, network security remains a critical concern, as IDS and firewalls serve complementary but distinct roles. While IDS solutions are tasked with monitoring both internal and external threats, firewalls primarily function to prevent unauthorized access by filtering external traffic. Although firewalls are effective in blocking intrusions from outside the network, they often fail to detect attacks originating within the internal environment. Given the increasing sophistication and severity of cyber-attacks, security experts have progressively adopted Machine learning techniques to protect organizational data and maintain business integrity. Machine learning offers significant advantages in terms of scalability, enabling the efficient processing of vast datasets while delivering high-performance computational capabilities within reasonable time and cost constraints. Recent studies employing Machine learning-based intrusion detection have predominantly utilized legacy datasets such as KDDCUP99, KDD98, and NSL-KDD7. Unfortunately, these datasets lack representation of contemporary network traffic, which can compromise the practical effectiveness of intrusion detection models. In response to these limitations, this research proposes the development of a modern intrusion detection framework based on the UNSW-NB15 dataset (https://research.unsw.edu.au/projects/unsw-nb15-dataset), which offers a more comprehensive and updated portrayal of current network behaviors and attack scenarios. Considering the persistent challenges in NIDS design, this study aims to investigate the application of Machine learning methodologies for constructing an intelligent intrusion detection model capable of autonomously identifying a wide range of cyberattacks. Specifically, the study utilizes Random Forest model combined with Extra Trees classifiers for efficient feature selection and attack detection within the UNSW-NB15 dataset. Additionally, the research focuses on detecting unknown threats, enhancing detection rates, evaluating overall model performance, and classifying network activities into normal and anomalous categories, thereby extending beyond conventional benchmarks [3].

The remainder of this paper is structured as follows: Section II presents a review of related works; Section III details the methodology and framework development; Section IV discusses the experimental results and analysis; and finally, Section V concludes the study with key findings and future research directions

.

2. Related Work

In recent years, machine learning-based intrusion detection systems (IDS) have attracted significant attention within the cybersecurity research community. Their ability to learn and adapt has positioned them as a promising solution to the growing challenge of detecting sophisticated and previously unknown cyberattacks. This expanding interest is largely due to the scalability and adaptability of machine learning (ML) approaches, which have demonstrated notable success in addressing the alarming rise of novel and evolving threats.

A study published in 2011 applied three distinct machine learning algorithms to the KDD Cup 1999 dataset using the WEKA data mining tool [1]. Similarly, the author [2] conducted a comparative analysis of multiple tree-based classification techniques using the NSL-KDD dataset. Studies such as [3], [4], and [5] provided comprehensive overviews on the application of machine learning techniques in

IDS, highlighting their role in detecting intrusions and designing robust detection systems. A more detailed examination of machine learning models and relevant datasets for network intrusion detection was presented in [6].

The author including [7], [8], [9]and [10] explored the application of deep learning approaches on the KDD-99 dataset for anomaly detection. However, the complexity of the UNSW-NB15 dataset [11] has been emphasized in more recent studies, indicating its superior representation of modern network traffic compared to the older KDD99 dataset.

Innovative frameworks have also emerged, such as the vision-based deep learning model proposed in [12], and a multi-class artificial neural network (ANN) approach presented in [13], both contributing to advancements in network intrusion detection. The proposed models were evaluated on datasets like KDD CUP 1999 and UNSW-NB15, with experimental results confirming their capability in accurately identifying cyberattacks. Further, the author [14] analyzed the application of deep neural networks (DNN) to develop adaptive and efficient intrusion detection systems, while [15] introduced a two-stage classifier utilizing protocol subsets and the RepTree algorithm, achieving detection accuracies of 89.85% on UNSW-NB15 and 88.95% on NSL-KDD datasets. An anomaly-based deep learning IDS was developed in [16], successfully categorizing intrusions into five distinct groups.

Other noteworthy studies include [17], which implemented a machine learning framework to detect botnets using UNSW-NB15, reporting Decision Tree models achieving 93.23% accuracy. A two-stage detection strategy based on GoogleNet Inception and Convolutional Neural Networks (CNN) was proposed in [18], demonstrating enhanced detection reliability. The comparative evaluation of various ML classifiers (SVM, RF, ELM) on NSL-KDD was conducted in [19], while [20] developed a decision tree-based IDS framework for big data environments. In [21], CNN-based models with optimized hyperparameters were proposed, whereas the author [22] explored the impact of feature selection methods on ML algorithms using NSL-KDD. A feature selection-based IDS utilizing Naïve Bayes, KNN, and Decision Trees was proposed in [23] with an emphasis on the pros and cons of modern ML techniques. An extensive review of ML applications in IDS across datasets such as KDD Cup 1999, Gure KDD-cup, and NSL-KDD was undertaken in [24].

Research in [25] provided algorithmic insights alongside comparative evaluations of popular datasets. The increasing adoption of soft computing methods in IDS was highlighted in [26], while [27] examined the advantages and limitations of contemporary machine learning and deep learning techniques. A novel two-stage model combining stacked autoencoders and softmax classifiers was introduced in [28], and anomaly detection using Recursive Feature Elimination and Random Forests on UNSW-NB15 was performed in [29].

Supervised ML methods such as SVM, ANN, and wrapper-based feature selection techniques were evaluated in [30], where ANN demonstrated superior performance. Further, the author [31] proposed an advanced deep learning method showing improvements over previous models. A systematic review of machine and deep learning techniques for IDS was provided in [32], while the author [33] developed deep learning models for both binary and multi-class intrusion classification.

Comparative studies on classical ML approaches requiring extensive feature engineering were conducted in [34], and [35] introduced a multi-class attack detection framework utilizing Random Forest, Decision Tree, Logistic Regression, K-Nearest Neighbors, and ANN.

The brief assessment of related work makes it clear that more research is needed to pinpoint the characteristics of network attacks. Henceforth, finding a general model with greater accuracy for the attacks in the dataset is necessary

3. Research Methodology

The development of efficient Machine learning models for accurate attack detection within datasets holds significant importance. In this context, the present study focuses on employing Random Forest model, a powerful Machine learning approach, to identify network attacks using the UNSW-NB15 dataset. The complete framework illustrating the proposed methodology is presented in Figure 1. The

subsequent sections outline the key steps involved in implementing the Random Forest model within the Network Intrusion Detection System (NIDS).

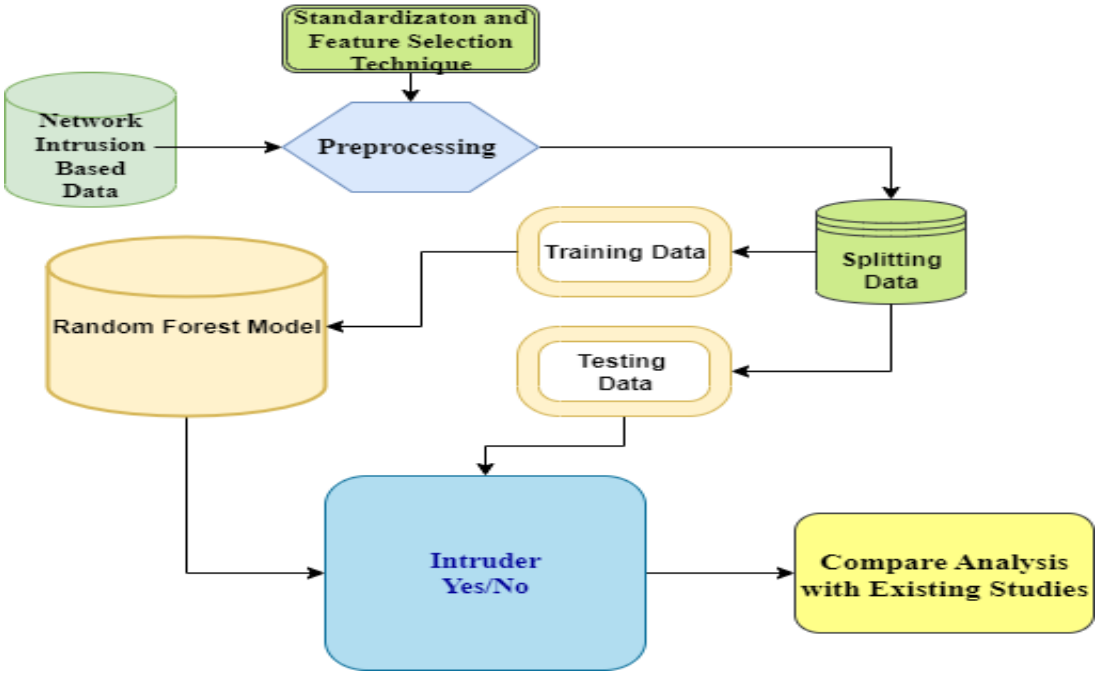

Figure 1: Proposed Model for Network Intrusion Detection

The model illustrated in the diagram represents a systematic approach for network intrusion detection, utilizing the UNSW-NB15 dataset alongside advanced machine learning technique. The process initiates with the input of raw network intrusion-based data, which contains a wide range of features representing both normal and malicious traffic patterns observed in real-world network environments. The first crucial step in this pipeline is preprocessing. During this phase, the raw data undergoes standardization and cleaning procedures to ensure consistency and remove any redundancies or anomalies that could negatively impact the learning process. A feature selection technique, specifically the Extra Trees Classifier, is applied at this stage. Extra Trees Classifier operates as an ensemble learning method, evaluating the importance of each feature based on information gain or Gini index, and selecting the most informative and relevant features from the dataset. This step significantly reduces the dimensionality of the data, improving model performance and minimizing computational complexity while retaining critical features that contribute to accurate intrusion detection. Following preprocessing, the refined dataset is split into two subsets: training data and testing data. The training data is used to develop and optimize the machine learning model, while the testing data is reserved to evaluate the model's performance on unseen data, ensuring it generalizes well to new network traffic scenarios.

The Random Forest model is then employed as the primary classification algorithm. This ensemble model constructs a multitude of decision trees during the training phase. Each tree is trained on a random subset of features and samples, and the final prediction is determined through majority voting across all trees. The Random Forest's capability to handle high-dimensional data and its robustness against overfitting make it a suitable choice for intrusion detection tasks, especially when dealing with complex datasets like UNSW-NB15. Once the Random Forest model is trained, it processes the testing data to classify network activities. The output of the model is a binary decision: it determines whether a

given network instance represents an intrusion (Yes) or legitimate traffic (No). This decision-making capability is central to intrusion detection systems, allowing for the real-time identification and mitigation of security threats. Finally, the performance of the trained model is subjected to comparative analysis against existing studies. This step involves evaluating key performance metrics such as accuracy, precision, recall, and false positive rates, and comparing them with previous research findings. By doing so, the study establishes the effectiveness and superiority of the proposed Random Forest-based approach with Extra Trees feature selection on the UNSW-NB15 dataset, demonstrating improvements in detection accuracy and reliability in identifying cyber threats.

A comparative evaluation supported by statistical significance testing was performed to validate the effectiveness of the proposed model. This validation process utilized a confusion matrix, a standard tool for assessing the performance of classification algorithms. The confusion matrix comprises four key components: True Positives (TP), False Positives (FP), False Negatives (FN), and True Negatives (TN). These values are instrumental in calculating various performance metrics that reflect the model's classification capabilities [41]. Among the performance indicators, **accuracy** represents the proportion of correctly classified instances relative to the total number of instances. It provides a general measure of the model's effectiveness and is mathematically expressed as [42]

:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Precision measures the proportion of correctly predicted positive observations to the total predicted positive observations. It reflects how well the model avoids false positives and is calculated as:

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

Recall (also known as sensitivity) quantifies the model's ability to correctly identify positive cases among all actual positive instances. It is expressed by the following equation :

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

Finally, The **F1-score** provides a balanced measure by calculating the harmonic mean of precision and recall, offering a comprehensive evaluation of the model's performance, especially when dealing with imbalanced datasets. It is mathematically formulated as.

$$F1-score = \frac{2*(Precision*Recall)}{(Precision+Recall)} \quad (4)$$

4. Results

The dataset utilized in this study is the UNSW-NB15, which comprises a total of 80,000 records. Furthermore, a binary classification approach is employed to assess the performance of the model. In this setup, the data is categorized into two classes: Class 0, representing normal (non-attack) traffic, and Class 1, indicating attack traffic. For the training and evaluation process, 70% of the data is allocated for training the model, while the remaining 30% is reserved for testing its performance across various evaluation metrics.

The results of Random Forest Model in terms of accuracy, precision, recall, and f1-score are summarized in **Table 1**.

Table 1: Classification Report of Random Forest Model

	Precision	Recall	F1-score	Support
0	1.00	1.00	1.00	10850
1	1.00	1.00	1.00	13144
Accuracy			99.10	24000
Macro Avg	1.00	1.00	1.00	24000

The table represents the results that have been extracted from different evaluation matrices, and are necessary to validate the performance of the model. The model can be considered relatively good, having an accuracy of 99.10%.

To further confirm the effectiveness of the model, confusion matrices were employed to classify attacks under a binary classification scheme, as illustrated in Figure 2. The Random Forest model was evaluated using a test set consisting of 24,000 data points. Out of these, the model accurately predicted 13,144 instances as Class 1 (attacks) and 10,853 instances as Class 0 (normal traffic).

Predicted True	0	1	All
0	10853	3	10856
1	0	13144	13144
All	10853	13147	24000

Figure 2: Confusion Matrix of Random Forest Model Model

5. Comparison with Benchmarks

The performance of the binary classification models is evaluated against established benchmark studies [35], [6], [18], and [30]. Table 2 presents a comparative analysis of the accuracy scores achieved in this study versus those reported in previous works. The comparison clearly demonstrates that the proposed Random Forest model, enhanced by the Extra Trees Classifier for feature selection, achieves superior accuracy compared to other existing approaches examined in the referenced studies

Table 2: Comparison with Similar Studies

Works	Model	Accuracy	Precision	Recall	F1-Score
[35]	Random Forest	75.38 %	83.30%	75.38%	77.51 %
[6]	Random Forest	86.%	89.5%	86%	86%
[18]	CNN	92.2%	96%	80%	87 %
[30]	ANN	94%	N/A	N/A	N/A
Proposed Method	Random Forest	99.10%	100%	100%	100%

The table shows a comparison of different models based on accuracy, precision, recall, and F1-score. Previous studies using Random Forest, LSTM, and ANN achieved accuracy between 75% to 94%, with varying performance in precision and recall. In contrast, the proposed Random Forest model achieved the highest performance, with 99.10% accuracy and perfect 100% scores in precision, recall, and F1-score, showing superior detection capability with no false positives or false negatives.

6. Conclusion

In this study, Random Forest models were employed to detect network intrusions, with their performance evaluated using the UNSW-NB15 dataset. The proposed approach incorporated several preprocessing techniques, including feature selection and data standardization, to enhance model performance. Notably, the use of the Extra Trees Classifier for feature selection contributed to a significant improvement in accuracy. Experimental results confirmed that the classification models performed exceptionally well across key evaluation metrics, including F1-score, recall, precision, and accuracy. The model achieved an impressive binary classification accuracy of 99.10%, surpassing the outcomes reported in previous studies. The reliability of the results was further validated through ROC curves and confusion matrices for each class.

7. Future Work

The proposed system delivered excellent results, but further improvements are needed to maximize its potential. Future work should focus on extending the model to multiclass classification for better attack differentiation. Advanced feature selection methods like Recursive Feature Elimination (RFE) and Principal Component Analysis (PCA) could enhance performance. Incorporating ensemble techniques like bagging and boosting may improve accuracy and reduce false positives. Transfer learning with pre-trained models can boost efficiency and performance. Real-time testing is crucial for practical validation, and experimenting with activation functions like Swish and GELU, along with optimizers like AdamW, may further optimize results. Enhancing model interpretability, ensuring robustness against adversarial attacks, and applying federated learning will also improve scalability, security, and practical deployment.

References

[1] Y. X. Meng, "The practice on using machine learning for network anomaly intrusion detection," *Proc. - Int. Conf. Mach. Learn. Cybern.*, vol. 2, pp. 576–581, 2011, doi: 10.1109/ICMLC.2011.6016798.

[2] S. Thaseen and C. A. Kumar, "An analysis of supervised tree based classifiers for intrusion detection system," *Proc. 2013 Int. Conf. Pattern Recognition, Informatics Mob. Eng. PRIME 2013*, pp. 294–299, 2013, doi: 10.1109/ICPRIME.2013.6496489.

[3] S. Wagh, A. ali shah, S. Kishor Wagh, V. K. Pachghare, and S. R. Kolhe, "Survey on Intrusion Detection System using Machine Learning Techniques Cite this paper Analysis of Machine Learning Techniques for Int rusion Det ect ion Syst em: A Review Survey on Intrusion Detection System using Machine Learning Techniques," *Int. J. Comput. Appl.*, vol. 78, no. 16, pp. 975–8887, 2013.

[4] O. Y. Al-Jarrah, A. Siddiqui, M. Elsalamouny, P. D. Yoo, S. Muhaidat, and K. Kim, "Machine-learning-based feature selection techniques for large-scale network intrusion detection," *Proc. - Int. Conf. Distrib. Comput. Syst.*, pp. 177–181, 2014, doi: 10.1109/ICDCSW.2014.14.

[5] S. Choudhury and A. Bhowal, "Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection," *2015 Int. Conf. Smart Technol. Manag. Comput. Commun. Control. Energy Mater. ICSTM 2015 - Proc.*, pp. 89–95, 2015, doi: 10.1109/ICSTM.2015.7225395.

[6] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.

[7] Y. Dong, R. Wang, and J. He, "Real-time network intrusion detection system based on deep learning," *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, pp. 1–4, 2019, doi: 10.1109/ICSESS47205.2019.9040718.

[8] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," *Proc. - 2016 15th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2016*, pp. 195–200, 2017, doi: 10.1109/ICMLA.2016.167.

[9] V. K. Rahul, R. Vinayakumar, K. Soman, and P. Poornachandran, "Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security," *2018 9th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2018*, no. November, pp. 1–6, 2018, doi: 10.1109/ICCCNT.2018.8494096.

[10] N. Gao, L. Gao, Q. Gao, and H. Wang, "An Intrusion Detection Model Based on Deep Belief Networks," *Proc. - 2014 2nd Int. Conf. Adv. Cloud Big Data, CBD 2014*, pp. 247–252, 2015, doi: 10.1109/CBD.2014.41.

[11] N. Moustafa and J. Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Inf. Secur. J.*, vol. 25, no. 1–3, pp. 18–31, 2016, doi: 10.1080/19393555.2015.1125974.

[12] Li, A., Yang, X., Dong, H., Xie, Z., & Yang, C. (2018). Machine learning-based sensor data modeling methods for power transformer PHM. *Sensors*, *18*(12), 4430.

[13] M. M. Baig, M. M. Awais, and E. S. M. El-Alfy, "A multiclass cascade of artificial neural network for network intrusion detection," *J. Intell. Fuzzy Syst.*, vol. 32, no. 4, pp. 2875–2883, 2017, doi: 10.3233/JIFS-169230.

[14] 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.

[15] M. Belouch, S. El, and M. Idhammad, "A Two-Stage Classifier Approach using RepTree Algorithm for Network Intrusion Detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, pp. 389–394, 2017, doi: 10.14569/ijacsa.2017.080651.

[16] N. T. Van, T. N. Thinh, and L. T. Sach, "An anomaly-based network intrusion detection system using Deep learning," *Proc. - 2017 Int. Conf. Syst. Sci. Eng. ICSSE 2017*, pp. 210–214, 2017, doi: 10.1109/ICSSE.2017.8030867.

[17] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 235, pp. 30–44, 2018, doi: 10.1007/978-3-319-90775-8_3.

[18] Thanthrige, U. S. K. P. M., Samarabandu, J., & Wang, X. (2016, May). Machine learning techniques for intrusion detection on public dataset. In *2016 IEEE Canadian conference on electrical and computer engineering (CCECE)* (pp. 1-4). IEEE.

[19] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection," *IEEE Access*, vol. 6, pp. 33789–33795, 2018, doi: 10.1109/ACCESS.2018.2841987.

[20] K. Peng, V. C. M. Leung, L. Zheng, S. Wang, C. Huang, and T. Lin, "Intrusion detection system based on decision tree over big data in fog environment," *Wirel. Commun. Mob. Comput.*, vol. 2018, pp. 1–11, 2018, doi: 10.1155/2018/4680867.

[21] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, pp. 108–116. doi: 10.5220/0006639801080116.

[22] P. Maniriho and T. Ahmad, "Analyzing the Performance of Machine Learning Algorithms in Anomaly Network Intrusion Detection Systems," *Proc. - 2018 4th Int. Conf. Sci. Technol. ICST 2018*, vol. 1, pp. 1–6, 2018, doi: 10.1109/ICSTC.2018.8528645.

[23] A. A. Olayemi, Alesa b, "A Machine Learning Approach for Information System Security," *Int. J. Inf. Comput. Secur.*, vol. 16, no. 12, pp. 91–101, 2018.

[24] K. Shashank and M. Balachandra, "Review on Network Intrusion Detection Techniques using Machine Learning," *2018 IEEE Distrib. Comput. VLSI, Electr. Circuits Robot. Discov. 2018 - Proc.*, pp. 104–109, 2019, doi: 10.1109/DISCOVER.2018.8673974.

[25] A. Phadke, M. Kulkarni, P. Bhawalkar, and R. Bhattad, "A review of machine learning methodologies for network intrusion detection," *Proc. 3rd Int. Conf. Comput. Methodol. Commun. ICCMC 2019*, pp. 272–275, 2019, doi: 10.1109/ICCMC.2019.8819748.

[26] M. S. SH.Kok, A.Abdullah, NZ.Jhanjhi, "Intrusion Detection System Using Machine Learning Approach," *Int. J. Eng. Res. Technol.*, vol. 12, no. 1, pp. 8–15, 2019.

[27] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Appl. Sci.*, vol. 9, no. 20, pp. 1–28, 2019, doi: 10.3390/app9204396.

[28] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection," *IEEE Access ·*, vol. 7, no. March 2020, pp. 14–28, 2019, doi: 10.1109/ACCESS.2019.2899721.

[29] S. Meftah, T. Rachidi, and N. Assem, "Network based intrusion detection using the UNSW-NB15 dataset," *Int. J. Comput. Digit. Syst.*, vol. 8, no. 5, pp. 477–487, 2019, doi: 10.12785/ijcds/080505.

[30] K. A. Taher, "Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection," *2019 Int. Conf. Robot. Signal Process. Tech.*, pp. 643–646, 2019.

[31] V. Sstla, V. K. K. Kolli, L. K. Voggu, R. Bhavanam, and S. Vallabhasoyula, "Predictive model for network intrusion detection system using deep learning," *Rev. d'Intelligence Artif.*, vol. 34, no. 3, pp. 323–330, 2020, doi: 10.18280/ria.340310.

[32] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges," *Soft Comput.*, vol. 25, no. 15, pp. 9731–9763, 2021, doi: 10.1007/s00500-021-05893-0.

[33] M. Maithem and G. A. Al-Sultany, "Network intrusion detection system using deep neural networks," *J. Phys. Conf. Ser.*, vol. 1804, no. 1, pp. 1–11, 2021, doi: 10.1088/1742-6596/1804/1/012138.

[34] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE access*, 7, 41525-41550.

[35] Liu, L., Wang, P., Lin, J., & Liu, L. (2020). Intrusion detection of imbalanced network traffic based on machine learning and deep learning. *IEEE access*, 9, 7550-7563.