International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

Supervised Learning Approach for Intrusion Detection System in Imbalanced Network

Laxmi Gour
M. Tech. Scholar, Department of Computer Science and Engineering, TIT & Science, Bhopal, M.P., India
Mr. Rakesh Kumar Lodhi
Assistant Professor, Department of Computer Science and Engineering, TIT & Science, Bhopal, M.P., India
Mr. Rakesh Kumar Tiwari
Assistant Professor, Department of Computer Science and Engineering, TIT & Science, Bhopal, M.P., India
Dr. Vikas Gupta
Professor, Department of Computer Science and Engineering, TIT & Science, Bhopal, M.P., India

Abstract
In the era of increasing cyber threats, Intrusion Detection Systems (IDS) play a crucial role in safeguarding network infrastructures. Traditional IDS solutions often struggle to detect sophisticated attacks, particularly in the presence of highly imbalanced network traffic where malicious activities are significantly outnumbered by normal behavior. This study presents a supervised learning-based approach for intrusion detection that addresses the challenges posed by imbalanced datasets. Benchmark datasets such as NSL-KDD and CICIDS are utilized for model training and evaluation. Various supervised learning algorithms, including Decision Trees, Random Forests, Support Vector Machines, and Artificial Neural Networks, are employed to classify network traffic. To tackle the imbalance issue, data-level techniques like SMOTE (Synthetic Minority Over-sampling Technique) and algorithm-level approaches such as cost-sensitive learning are incorporated. Performance is evaluated using precision, recall, F1-score, and ROC-AUC to ensure effectiveness in identifying minority class intrusions. Results demonstrate that combining supervised learning with imbalance handling significantly improves detection accuracy for rare attack types. This work highlights the importance of

model selection and data preprocessing in enhancing IDS performance. Future directions include leveraging deep learning and real-time traffic analysis to further strengthen intrusion detection capabilities in complex and dynamic network environments.

Keywords: - IDS, Imbalance, Balance, Machine Learning

1. INTRODUCTION

One of the resources that is used the most is the Internet. People are carrying out digitized transactions as a result of the huge increase in internet usage. The expansion in number of web clients is 4% to 6% consistently. It has been observed that the growth is much higher in developing nations like India. A huge amount of data is being generated online as a result of high levels of computer and internet technology adoption [1, 2]. It is difficult to find a person who does not have an online presence because these technologies have also become essential components of human life. Expansion in on the web presence has likewise leaded to sharing or support of individual data on the web. Albeit this acquires enormous comfort terms of access, they are additionally helpless against assaults or interruptions. These intrusions may result in significant financial losses as well as the disclosure of private information to unintentional users [3].

Currently, more people are entering the digital realm thanks to the use of mobile devices. Additionally, there has been an increase in the number of web pages served and optimized for mobile devices. Numerous users have chosen mobile-based commerce applications due to the widespread use of mobile devices. The high reception levels of Web and cell phones as well as the expansion in web based business an exchange happening by means of organizations has brought about the expansion in huge number of cybercrimes.

Worldwide, cybercrime has cost 1,418 million dollars. (Source: www.statista.com). This demonstrates the growing significance of intrusion detection models in enhancing online user security. It moreover orders the utilization of better interruption discovery frameworks and displays the absence of proficiency in the current interruption discovery frameworks.

The process of identifying unauthorized anomalous activities on computer systems is referred to as "intrusion detection." An Intrusion Detection System (IDS)'s primary function is to classify users' actions as normal or abnormal based on the data they transmit.

Conventional insurance frameworks utilized firewalls, information encryption and verification strategies. However, the current intrusion scenarios are extremely sophisticated and have the ability to easily breach the security mechanisms that are enforced by conventional security

measures. This has come about in a colossal expansion in the quantity of specialists working in this space and has too expanded the quantity of examination commitments in this space [4]. In various industry scenarios, IDS models have multiple applications and requirements. The process of intrusion detection in personal systems, or distributed scenarios, is a major application. The architecture of current operating systems includes intrusion detection mechanisms. However, the systems' handling capabilities remain a mystery. As a result, for added security, the majority of users tend to use commercial intrusion detection models. In addition, there is a demand for server-based IDS that can be used in clustered environments.

2. LITERATURE REVIEW

MdLiakat Ali et al. [1], this study investigate the application of deep learning-based intrusion detection systems (IDSs) in large-scale network environments in response to the rising volume of network traffic and the increasing complexity of cyber threats. Accurate threat detection is hampered by issues with traditional IDS, including high false positive rates, intricate feature engineering, and class imbalances in datasets. In order to get around these restrictions, we combine common machine learning algorithms like logistic regression, naive Bayes, random forest, K-nearest neighbors, and decision trees with a variety of deep learning models, such as multilayer perceptron (MLP), convolutional neural network (CNN), and long short-term memory (LSTM). The use of the synthetic minority over-sampling technique (SMOTE) to rectify class imbalance and improve the representativeness of the learning process is a noteworthy contribution of this study. Furthermore, we do a thorough performance comparison of the models, optimizing detection accuracy through hyperparameter tweaking and correlation-based feature selection. With accuracy rates exceeding 98%, our findings show that deep learning models—in particular, CNN and LSTM—perform better than conventional machine learning techniques in cyber threat identification. Random forest, on the other hand, shows its efficacy in structured intrusion detection tasks by achieving the greatest accuracy of 99.9%. Additionally, we explore the trade-offs between accuracy and resource consumption while assessing computational efficiency and practical implementation factors. These results solve important issues like interpretability and processing overhead while demonstrating the potential of deep learning-based intrusion detection systems for extensive network security applications. Based on particular network settings and security objectives, the study offers practical insights for choosing the best IDS models.

Alars et al. [2], in today's interconnected world, network security is crucial due to the increasing sophistication and pervasiveness of cyberthreats. Due to their limited detection scope and reliance on preset signatures, traditional Network Intrusion Detection Systems (NIDS) typically fall short, revealing significant gaps in effectively identifying novel and unexpected intrusions. In order to improve NIDS performance, this study combines advanced deep learning algorithms with network and host traffic data. Our method is based on meticulous data collecting, preprocessing, and feature extraction using the Network Intrusion Detection dataset, which includes several intrusion scenarios that are repeated in a military network setting. To evaluate these data, we used a convolutional neural network (CNN), improving model performance by strict feature selection and dimensionality reduction. The results show that our deep learning-based NIDS outperforms existing methods and effectively addresses real-world cybersecurity issues with an astounding detection accuracy of 98.5%. The development of intrusion detection systems is aided by this comprehensive approach, which not only advances NIDS technology but also offers a workable way to improve network security for a variety of applications.

Selvam et al. [3], smart Cities were established as a result of the widespread use of the Internet of Things (IoT) concept in recent years. IoT has been a major force in several fields, such as home automation, smart transportation, Industry 4.0, and healthcare. A relatively recent idea, "smart cities" effectively make use of adaptive optimization of available resources to provide residents with exceptional amenities. IoT devices are made to collect data from their environment and transmit it to other systems via the Internet. This could lead to cybersecurity issues like brute-force attacks, denial-of-service attacks, and unauthorized access. The tenants' privacy and safety are the most urgent issues that need to be addressed. A variety of attack types are included in the data collected from popular datasets such as CIC-IDS 2017 and CIC-IDS 2018. Pre-processing eliminates missing values and normalizations through the use of algorithms. Random Forest (RF) is used to pick and remove most of the time stamps from an assault dataset. After that, among those numerous features, essential attributes are extracted from those data using Deep Autoencoder (AE). For each deep learning system tested in this paper, a suitable comparison of the first two datasets yielded positive results. In CIC IDS 2017, the precision, recall, and F1-score measurements were 99.5%, 98.7%, and 99.8%, respectively. For all algorithms, the precision, F1-score, and recall for CIC IDS 2018 were 99.5%. The best results are obtained with our Novel CNN approach.

Kezhou Ren et al. [4], network attacks pose significant threats to network services' security. Therefore, it is essential to make use of brand-new technical approaches in order to boost the effectiveness of intrusion detection systems. In recent years, a number of reinforcement learning algorithms for network intrusion systems, such as Markov and others, have been developed to meet the IDS's needs for both intelligent and unmanned systems. A deep feed-forward neural network approach is used in conjunction with a deep Q-learning-based network intrusion detection model that incorporates reinforcement learning to provide continuous automatic learning capability for network environments. To test the model's performance, experiments were carried out with the CSE-CIC-IDS2018 dataset, which contains a comprehensive collection of actual network traffic. The results of the experiments show that the proposed model can successfully identify threats in the network, outperforms standard machine learning methods, and has promising potential as an unmanned IDS in complex network settings.

R. Ahsan et al. [5], the issue of anomaly detection in imbalanced datasets is examined in this work within the context of network intrusion detection. To deal with the class-imbalance issue, a novel anomaly detection solution that takes into account both data-level and algorithm-level approaches is proposed. The oversampling capabilities of a Conditional Generative Adversarial Network (CGAN) and the auto-learning capabilities of reinforcement learning are combined in this approach. To additionally explore the capability of a CGAN, in imbalanced order undertakings, the impact of CGAN-put together oversampling with respect to the accompanying classifiers is inspected: Logistic Regression, Multilayer Perceptron, Random Forest, and Naive Bayes The experimental results show that the proposed method and CGAN-based oversampling in general perform better than other oversampling methods like the Synthetic Minority Oversampling Technique and Adaptive Synthetic. The Authors in 2021 Cyber-Physical Systems from IET: Hypothesis and Applications distributed by John Wiley and Children Ltd for The Establishment of Designing and Innovation.

Lansky et al. [6], these days, security experts are incorporating various machine learning techniques to safeguard the data and reputation of enterprises due to the growing complexity and severity of security threats on computer networks. One of the innovative methods that intrusion detection systems, or IDS, have been using extensively lately to improve their efficacy in protecting hosts and computer networks is deep learning. In-depth research and categorization of deep learning-based intrusion detection systems are the main topics of this

survey paper. The main background ideas of IDS architecture and different deep learning methods are initially presented. After that, it groups these schemes based on the kinds of deep learning techniques that are applied in each of them. It explains how the intrusion detection process uses deep learning networks to precisely identify intrusions. Lastly, a thorough examination of the examined IDS frameworks is given, along with closing thoughts and recommendations for the future.

S. Dong et al. [7], our production life has been greatly improved by the rapid development of Internet technology, but as a result, security issues have become increasingly prevalent. Users' privacy is at risk, and many aspects of society, including politics, the economy, culture, and people's means of subsistence, face significant security risks as a result of these issues. The development of the data transmission rate grows the extent of assaults and gives a more assault climate to interlopers. Strange location is a compelling security assurance innovation that can screen network transmission continuously, really sense outside assaults, and give reaction choices to pertinent chiefs. A technology for detecting abnormal traffic has also emerged as a result of advances in machine learning. The objective has been to use powerful and quick learning algorithms to respond immediately to shifting threats. The vast majority of the flow unusual identification research depends on reproduction, utilizing public and notable datasets. From one viewpoint, the dataset contains high-layered enormous information, which customary AI strategies can't be handled. However, the labeling cost is extremely high because the dataset's labels are all manually labeled and the labeled data scale is far behind the application requirements. This paper proposes a semi-directed Twofold Profound Q-Organization (SSDDQN)- based improvement strategy for network strange traffic location, mostly founded on Twofold Profound Q-Organization (DDQN), a delegate of Profound Support Learning calculation. The current network in SSDDQN uses a deep neural network as a classifier before using the autoencoder to reconstruct the traffic features. K-Means clustering is used by the target network's unsupervised learning algorithm first, followed by deep neural network prediction. For training and testing, the experiment makes extensive use of the NSL-KDD and AWID datasets and compares them to existing machine learning models. The experimental results demonstrate that SSDDQN performed well in a variety of evaluation metrics and has some advantages in terms of time complexity.

Lau lin et al. [8], in imbalanced organization traffic, pernicious digital assaults can regularly stow away in a lot of typical information. It displays a serious level of covertness and jumbling

in the internet, making it hard for Network Intrusion Detection System(NIDS) to guarantee the precision and practicality of discovery. This paper explores AI and profound learning for interruption recognition in imbalanced organization traffic. It proposes an original Difficult Set Sampling Technique (DSSTE) calculation to handle the class awkwardness issue. To start with, utilize the Edited Nearest Neighbor(ENN) calculation to separate the imbalanced preparing set into the troublesome set and the simple set. Then, utilize the KMeans calculation to pack the larger part tests in the troublesome set to diminish the larger part. Zoom in and out the minority tests' persistent characteristics in the troublesome set integrate new examples to expand the minority number.

Problem formulation:-

Following are the problems which is to be consider in a IDS based on machine learning approach (base paper) are as follows-

- Inferior detection accuracy in actual environments- Machine learning methods has a certain ability to detect intrusions, but they do not often perform well on completely unfamiliar data. When data set does not cover all typical real world samples it would decrease the accuracy.
- Low efficiency- most studies emphasizes the detection results; therefore they usually employ complicated models and extensive data processing methods, leading to low efficiency.

Lacking of available data sets is another major problem because the main task of machine learning is to extract the valuable information of data set. So if data sets are not available then it would be problem in detection.

3. INTRUSION DETECTION SYSTEM

Like other security measures like antivirus software, firewalls, and access control plans, Intrusion Detection Systems (IDS) are designed to improve the security of information and Internet of Things communication systems. The firewall's primary function is to sort packets according to allow/deny rules based on information in the header fields. The filtering of packets that pass through particular hosts or network ports, which are typically open on the majority of computer systems, is the firewall's primary function. It doesn't do deep analysis, which is like finding malicious code in a packet, and it treats each packet as a separate thing. An anti-virus

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

program is a running process that, rather than monitoring network traffic, examines executables, worms, and viruses in the memory of protected computer/network systems [6].

While IDS requires more embedded intelligence than other security products like antivirus programs, it analyzes the information it collects and derives useful results [7]. This is the difference between IDS and other security products like antivirus programs. DARPA established the CIDF (Common Intrusion Detection Framework) working group in 1998 with the primary goal of coordinating and defining a common framework in the IDS field. This group has produced noteworthy work [8]. A general IDS architecture based on the consideration of the four kinds of functional modules depicted in Figure 1 was developed by the group, which was incorporated into the IETF in the year 2000 and adopted the brand-new acronym IDWG ('Intrusion Detection Working Group').

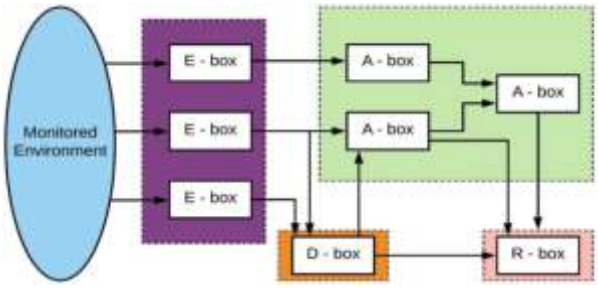

Figure 1: General CIDF architecture for IDS

Contingent upon the sort of examination did, interruption location frameworks are delegated by the same token signature-based or abnormality based displayed in Figure 2. Signature-based plans (additionally indicated as abuse based) look for characterized examples, or marks, inside the dissected information. A signature database that corresponds to known attacks is specified a priori for this purpose. Anomaly-based detectors, on the other hand, attempt to estimate the "normal" behavior of the system that needs to be protected and issue an anomaly alarm whenever the difference between a specific observation and the normal behavior exceeds a predetermined threshold. Modeling the system's "abnormal" behavior and sending an alert when the difference between what is seen and what is expected falls below a certain threshold is another option.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

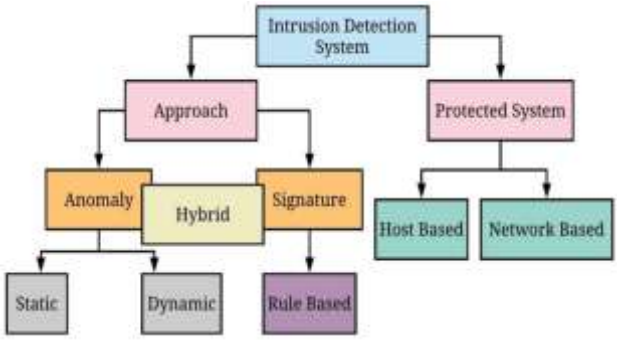

Figure 2: IDS Classifications

For specific, well-known attacks, signature-based schemes provide excellent detection results. Even if they are designed as minimal variants of attacks that are already known, they are unable to detect new, unknown intrusions. Contrarily, the main advantage of anomaly-based detection methods [5] is that they can pick up on intrusions that haven't been seen before.

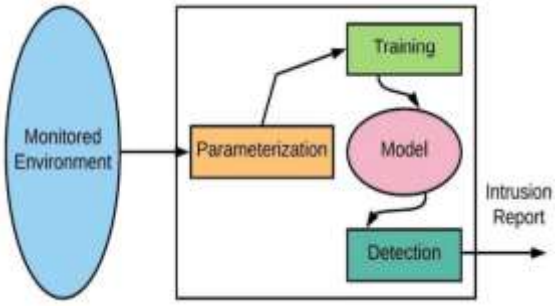

Figure 3: Generic Anomaly based IDS Functional Architecture

Anomaly-based Intrusion Detection Systems (A-IDS) are currently the primary focus of intrusion detection research and development due to their promising capabilities. Numerous novel plans are being considered, and numerous new systems with A-IDS capabilities are becoming available. Although there are a variety of A-IDS approaches, the fundamental modules or stages depicted in Figure 3 are common to all of them.

4. ML ALGORITHM

Supervised learning is two stage forms, in the initial step: a model is fabricate depicting a foreordained arrangement of information classes or ideas. The model developed by investigating database tuples portrayed by traits. Each tuple is expected to have a place with a

predefined class, as dictated by one of the qualities, called to have a place with a reclassified class, as controlled by one of the traits called the class name characteristic. The information tuple are dissected to fabricate the model all things considered from the preparation dataset.

Learning

The main property of an ML is its capability to learn. Learning or preparing is a procedure by methods for which a neural system adjusts to a boost by making legitimate parameter modifications, bringing about the generation of wanted reaction. Learning in an ML is chiefly ordered into two classes as [9].

- Supervised learning
- Unsupervised learning

Supervised Learning

Regulated learning is two stage forms, in the initial step: a model is fabricated depicting a foreordained arrangement of information classes or ideas. The model developed by investigating database tuples portrayed by traits. Each tuple is expected to have a place with a predefined class, as dictated by one of the qualities, called to have a place with a reclassified class, as controlled by one of the traits called the class name characteristic. The information tuple are dissected to fabricate the model all things considered from the preparation dataset.

Unsupervised learning

It is the kind of learning in which the class mark of each preparation test isn't knows, and the number or set of classes to be scholarly may not be known ahead of time. The prerequisite for having a named reaction variable in preparing information from the administered learning system may not be fulfilled in a few circumstances.

Data mining field is a highly efficient techniques like association rule learning. Data mining performs the interesting machine-learning algorithms like inductive-rule learning with the construction of decision trees to development of large databases process. Data mining techniques are employed in large interesting organizations and data investigations. Many data mining approaches use classification related methods for identification of useful information from continuous data streams.

Nearest Neighbors Algorithm

The Nearest Neighbor (NN) rule differentiates the classification of unknown data point because of closest neighbor whose class is known. The nearest neighbor is calculated based on

estimation of k that represents how many nearest neighbors are taken to characterize the data point class. It utilizes more than one closest neighbor to find out the class where the given data point belong termed as KNN. The data samples are required in memory at run time called as memory-based technique. The training points are allocated weights based on their distances from the sample data point. However, the computational complexity and memory requirements remained key issue. For addressing the memory utilization problem, size of data gets minimized. The repeated patterns without additional data are removed from the training data set.

Naive Bayes Classifier

Naive Bayes Classifier technique is functioned based on Bayesian theorem. The designed technique is used when dimensionality of input is high. Bayesian Classifier is used for computing the possible output depending on the input. It is feasible to add new raw data at runtime. A Naive Bayes classifier represents presence (or absence) of a feature (attribute) of class that is unrelated to presence (or absence) of any other feature when class variable is known. Naïve Bayesian Classification Algorithm was introduced by Shinde S.B and Amrit Priyadarshi (2015) that denotes statistical method and supervised learning method for classification. Naive Bayesian Algorithm is used to predict the heart disease. Raw hospital dataset is employed. After that, the data gets preprocessed and transformed. Finally by using the designed data mining algorithm, heart disease was predicted and accuracy was computed.

Support Vector Machine

SVM are used in many applications like medical, military for classification purpose. SVM are employed for classification, regression or ranking function. SVM depends on statistical learning theory and structural risk minimization principal. SVM determines the location of decision boundaries called hyper plane for optimal separation of classes as described in figure 1.4. Margin maximization through creating largest distance between separating hyper plane and instances on either side are employed to minimize upper bound on expected generalization error. Classification accuracy of SVM not depends on dimension of classified entities. The data analysis in SVM is based on convex quadratic programming. It is expensive as quadratic programming methods need large matrix operations and time consuming numerical computations.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

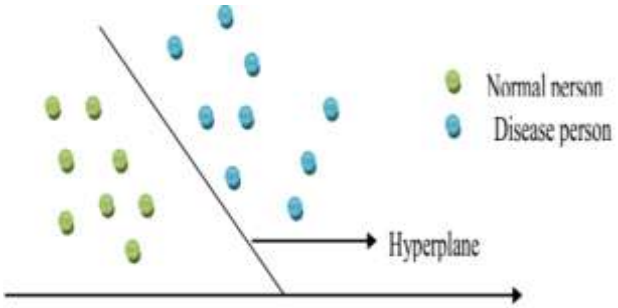

Figure 4: Support Vector Classification

5. CONCLUSION

In Detection System (IDS) was developed and evaluated for detecting network intrusions in an imbalanced data environment. The inherent challenge of class imbalance, which is common in real-world network traffic where malicious activities are significantly underrepresented, was effectively addressed using data-level and algorithm-level strategies such as SMOTE and cost-sensitive learning. Various supervised classifiers, including Decision Tree, Random Forest, SVM, and ANN, were implemented and compared. The experimental results demonstrated that the performance of these models, particularly in detecting minority class intrusions, significantly improved when imbalance mitigation techniques were applied.

Among the models tested, ensemble methods like Random Forest showed strong and consistent performance in terms of recall, F1-score, and ROC-AUC, indicating their suitability for handling imbalanced classification tasks. This research highlights this study, a supervised learning-based Intrusion that careful preprocessing, model selection, and evaluation using appropriate metrics is critical for building an effective IDS.

The findings suggest that supervised learning, when enhanced with proper imbalance handling, can significantly contribute to more accurate and reliable intrusion detection. Future work may focus on incorporating deep learning models, hybrid approaches, and real-time IDS deployment to further enhance security in dynamic network environments.

REFERENCES

[1] MdLiakat Ali, Kutub Thakur, Suzanna Schmeelk, Joan Debello and Denise Dragos, “Deep Learning vs. Machine Learning for Intrusion Detection in Computer Networks: A Comparative Study”, MDPI 2025.

[2] Alars, E.S.A.; Kurnaz, S. Enhancing network intrusion detection systems with combined network and host traffic features using deep learning: Deep learning and IoT perspective. Discov. Comput. 2024, 27, 39.

[3] Selvam, R.; Velliangiri, S. An Improving Intrusion Detection Model Based on Novel CNN Technique Using Recent CIC-IDS Datasets. In Proceedings of the 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT), Bengaluru, India, 15–16 March 2024; pp. 1–6.

[4] Kezhou Ren, Maohuan Wang, Yifan Zeng and Yingchao Zhang, *"*An Unmanned Network Intrusion Detection Model Based on Deep Reinforcement Learning*"*, IEEE International Conference on Unmanned Systems (ICUS), IEEE 2022.

[5] R. Ahsan, W. Shi, X. Ma, and W. L. Croft, "A comparative analysis of CGAN-based oversampling for anomaly detection," *IET* Cyberphysical Systems: Theory & Applications, vol. 7, no. 1, pp. 40–50, Mar. 2022.

[6] Lansky, J.; Ali, S.; Mohammadi, M.; Majeed, M.K.; Karim, S.H.T.; Rashidi, S.; Hosseinzadeh, M.; Rahmani, A.M. Deep learning based intrusion detection systems: A systematic review. IEEE Access 2021, 9, 101574–101599.

[7] S. Dong, Y. Xia, and T. Peng, "Network Abnormal Traffic Detection Model Based on Semi-Supervised Deep Reinforcement Learning," IEEE Transactions On Network And Service Management, vol. 18, no. 4, pp. 4197–4212, Dec. 2021.

[8] Lan Liu, Pengcheng Wang , Jun Lin, and Langzhou Liu, "Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning", IEEE Access 2020.

[9] Chiba, Z.; Abghour, N.; Moussaid, K.; Rida, M. Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms. Comput. Secur. 2019, 86, 291–317.

[10] A. Raghavan, F. D. Troia, and M. Stamp, ``Hidden Markov models with random restarts versus boosting for malware detection," *J. Comput. Virol. Hacking Techn.*, vol. 15, no. 2, pp. 97107, Jun. 2019.

[11] Zhiyou Zhang and Peishang Pan "A hybrid intrusion detection method based on improved fuzzy C-Means and SVM", IEEE International Conference on Communication Information System and Computer Engineer (CISCE), pp. no. 210-214, Haikou, China 2019.

[12] Afreen Bhumgara and Anand Pitale, "Detection of Network Intrusion Using Hybrid Intelligent System", IEEE International Conferences on Advances in Information Technology, pp. no. 167-172, Chikmagalur, India 2019.

[13] Ritumbhira Uikey and Dr. Manari Cyanchandani "Survey on Classification Techniques Applied to Intrusion Detection System and its Comparative Analysis", IEEE 4th International Conference on Communication $ Electronics System (ICCES), pp. no. 459-466, Coimbatore, India 2019.

[14] Aditya Phadke, Mohit Kulkarni, Pranav Bhawalkar and Rashmi Bhattad "A Review of Machine Learning Methodologies for Network Intrusion Detection", IEEE 3rd National Conference on Computing Methodologies and Communication (ICCMC), pp. no. 703-709, Erode, India 2019.

[15] S. Sivantham, R.Abirami and R.Gowsalya "Comapring in Anomaly Based Intrusion Detection System for Networks", IEEE International conference on Vision towards Emerging Trends in Communication and Networking (ViTECon), pp. no. 289-293, Coimbatore, India 2019.

[16] Azar Abid Salih and Maiwan Bahjat Abdulrazaq "Combining Best Features selection Using Three Classifiers in Intrusion Detection System", IEEE International Conference on Advanced science and Engineering (ICOASE), pp. no. 453-459, Zakho - Duhok, Iraq 2019.

[17] Lukman Hakim and Rahilla Fatma Novriandi "Influence Analysis of Feature Selection to Network Intrusion Detection System Performance Using NSL-KDD Dataset", IEEE International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE), pp. no. 330-336, Jember, Indonesia 2019.

[18] T. Sree Kala and A. Christy, "An Intrusion Detection System Using Opposition Based Particle Swayam Optimization Algorithm and PNN", IEEE International Conference on Machine Learning, Big Data, Cloud and Parallel Computing, pp. no. 564-569, Coimbatore, India 2019.

[19] Xiaoyan Wang and Hanwen Wang "A High Performance Intrusion Detection Method Based on Combining Supervised and Unsupervised Learning", IEEE Smart World, Ubiquitous Intelligence $ Computing Advanced $ Trusted Computing, Scalable Computing, Internet of People and Smart City Innovations, pp. no. 889-897, Guangzhou, China 2018.