A Systematic Review on Intrusion Detection System

Vineeta Shrivastava[1], Deepanjali Joshi[2]

[1]Ph.D. Scholar, [2]Assistant Professor

[1]LNCT University, Bhopal, M.P., India, [2]Barkatullah University Bhopal, M.P., India

[1]shrivastavavinita21@gmail.com, [2]joshideepanjali@gmail.com

Abstract: In the ever-evolving landscape of cyber threats, ensuring the security of internet-connected systems is of paramount importance. This study delves into the realm of cyber security, focusing on Intrusion Detection Systems (IDS) and their categorizations, mainly abuse (signature-based) and anomaly (behavior-based) detection. The article highlights the strengths and weaknesses of both methods and underscores the increasing need for machine learning strategies in cyber intrusion detection. Machine learning techniques offer promise in enhancing detection rates and minimizing false positives. Three main categories of anomaly-based IDS are examined: supervised, unsupervised, and semi-supervised. The study further explores and evaluates the performance of Support Vector Machine (SVM), Random Forest (RF), and Extreme Learning Machine (ELM) on the commonly used KDD dataset. A comprehensive review of recent contributions in the field is also presented, detailing the techniques used, datasets, accuracy rates, and associated limitations.

Keywords: Machine learning, Intrusion Detection System, clustering and outlier-based detection, Support vector machine.

I. Introduction

Cybersecurity involves the protection of internet-connected systems—including networks, computers, software, and data—from cyber threats and unauthorized access. A key tool in this defense strategy is the Intrusion Detection System (IDS). IDS analyzes data from network devices to detect and flag potential security breaches. Depending on their detection approach, IDS can be grouped into two main types: signature-based (or misuse detection) and behavior-based (or anomaly detection).[1]Signature-based detection relies on a set database of known attack patterns. This method is favored for its precision in identifying known threats and its low rate of false alarms. However, it falls short in recognizing new or modified attacks that aren't in its database[2]. As cyber threats evolve rapidly, keeping this database updated becomes a challenging task. Furthermore, this method is ineffective against zero-day exploits, which are attacks targeting software vulnerabilities unknown to those responsible for patching or fixing the software[4]. Anomaly detection systems work by establishing a standard profile based on regular system operations and then identifying variations from this profile as potential threats. Their strength lies in their potential to detect both familiar and novel threats, including those elusive zero-day exploits. However, they come with challenges, such as the necessity for calibration and a tendency to have higher false positive alerts. There's a growing body of research focusing on the integration of machine learning to enhance cyber intrusion detection. The aim is to optimize the balance between detection accuracy and minimizing false alarms. Based on the machine learning approach adopted, anomaly-based IDS can be categorized into:[5]Supervised Learning: Where the system is trained with data where each piece is clearly marked or labeled. Unsupervised Learning: This approach groups data based on similarities or identifies data points that stand out without using pre-labeled data. Semi-supervised Learning: A combination method that uses both labeled and unlabeled data for training.[6,7] In supervised IDS, the model is primed using data that's already been categorized. Classification models in intrusion detection, such as those used in misuse-based and supervised learning approaches, often face a challenge in detecting unknown threats. These models rely heavily on labeled data and require frequent retraining to stay updated with evolving threats, making them less practical due to the difficulty in obtaining sufficient labeled data.Semi-supervised learning approaches in intrusion detection systems (IDS) attempt to mitigate this challenge by utilizing a large volume of unlabeled data, supplemented by a smaller quantity of labeled data, to build models. This approach leverages the available information more effectively to enhance detection capabilities. Unsupervised learning approaches, like clustering algorithms, don’t rely on labeled data or predefined attack signatures. Instead, they organize the input data into clusters based on inherent similarities and differences, enabling the detection of both known and unknown threats. By doing so, unsupervised techniques offer a broader and more adaptable detection scope, as they can identify anomalies without needing explicit knowledge of attack patterns. They also facilitate improved attribution and correlation by incorporating features from multiple sources, enhancing the overall robustness and responsiveness of the IDS.[8] Intrusions pose a

Received 02 December 2022, Accepted 21 February, 2023

significant threat to computer and network systems, as they can lead to rapid data theft, loss, or even damage to the hardware. Beyond these immediate risks, intrusions can result in substantial financial setbacks and compromise critical IT infrastructure, exposing data to further vulnerabilities in potential cyber conflicts. Given the stakes, it's imperative to detect and prevent these intrusions. There exist various methods for intrusion detection, but achieving consistent accuracy remains a challenge. The effectiveness of these methods is often gauged by their detection rates and the frequency of false alarms. Addressing this accuracy dilemma is crucial to enhance the reliability of intrusion detection systems. This challenge was the driving force behind the current research project. In this research, we employ methodologies like the Support Vector Machine (SVM), Random Forest (RF), and Extreme Learning Machine (ELM). These techniques have previously demonstrated efficacy in tackling classification issues. For validation purposes, we tested our intrusion detection algorithms on the widely recognized KDD dataset. Specifically, we utilized the NSL-KDD dataset, an enhanced version of the original KDD, which serves as a standard for evaluating the performance of intrusion detection systems.

II. Related Work

Wisanwanichthan et al.[1] introduced a novel methodology called the Double-Layered Hybrid Approach (DLHA) aimed at addressing the noted challenges. They also delved into the unique attributes of various attack types by employing Principal Component Analysis (PCA). This new approach was benchmarked against other established research methodologies using the NSL-KDD dataset. The findings indicated that DLHA surpassed several contemporary IDS techniques in performance. Notably, it demonstrated marked improvement over singular machine learning classifiers. Especially impressive was DLHA's capability to detect infrequent attacks, registering detection rates of 96.67% for R2L attacks and a perfect 100% for U2R attacks. Guo Pu et al.[2] proposed an innovative unsupervised anomaly detection technique that merges Sub-Space Clustering (SSC) with One Class Support Vector Machine (OCSVM). This method is designed to detect attacks without relying on prior knowledge. To assess its effectiveness, the approach was tested using the prominent NSL-KDD dataset. The results of the experiments revealed that this novel method outperformed several existing techniques in detecting anomalies. When it comes to computation time, the proposed SSC-OCSVM method took 238.88 seconds on the Test mixed subset. In comparison, SSC-EA took 1060.76 seconds, DBSCAN took 8.15 seconds, and K-means took 0.69 seconds. Guezzaz et al.[3] introduced a resilient algorithm aimed at training and recognizing events gathered from network traffic. Their proposed model is straightforward to implement and is versatile enough to be applied to unstructured data, showcasing high accuracy in its operation. Kasongo et al.[4] introduced an intrusion detection system (IDS) leveraging deep learning, specifically utilizing feed-forward deep neural networks (FFDNNs). This system is further enhanced with a filter-based feature selection algorithm. When benchmarked against the NSL-KDD dataset, the performance of FFDNN-IDS was compared with other prevalent machine learning techniques, including support vector machines, decision trees, K-Nearest Neighbors, and Naïve Bayes. The data revealed that FFDNN-IDS outperformed its counterparts in terms of accuracy. For instance, while the RF classifier showed a commendable accuracy of 86.35% on test data, the SVM model trailed slightly with an accuracy rate of 83.83%.Chkirbene et al.[5] presented two innovative models for intrusion detection and classification, namely, the Trust-based Intrusion Detection and Classification System (TIDCS) and its accelerated version, TIDCS-A. These models aim to bolster network security by employing a unique feature selection algorithm that streamlines the input data features. In these models, any identified attack diminishes the trust level of the implicated nodes, facilitating a dynamic purging of the system.Evaluation using the NSL-KDD and UNSW datasets highlighted the proficiency of TIDCS and TIDCS-A in detecting malicious activities. They exhibited enhanced accuracy and detection rates, alongside reduced false alarm rates compared to existing techniques. Specifically, using the UNSW dataset, TIDCS achieved an accuracy of 91%, outperforming other models like online AODE (83.47%), CADF (88%), EDM (90%), TANN (90%), and NB (69.6%). Thus, TIDCS demonstrated superior performance in accuracy and maintained commendable detection and false alarm rates compared to other state-of-the-art techniques. Loukas et al.[6] conducted experiments illustrating the effectiveness of RNN-based deep learning, especially when augmented with LSTM. Their findings revealed that this approach could significantly boost intrusion detection accuracy, achieving 95.4% for a robotic vehicle. This performance is noteworthy, especially when juxtaposed with traditional machine learning classifiers or MLP-based deep learning, which often overlook the time-based nuances of a cyber-attack. Furthermore, by integrating cloud offloading with deep learning-based intrusion detection, this work stands at the crossroads of two evolving fields, poised to gain from advancements in both areas in the coming years. Liu et al.[7] introduced the Difficult Set Sampling Technique (DSSTE) as a new

algorithm to address the challenges posed by class imbalances. To gauge its effectiveness, this model was evaluated on the NSL-KDD and CSE-CIC-IDS2018 datasets. Within the tests, LSTM stood out by securing an impressive accuracy rate of 78.72% and a recall rate of 75.82%. Meanwhile, on the CSE-CIC-IDS2018 dataset, the random forest method showcased stellar results, recording an accuracy of 94.89% and an F1-Score of 94.72% when working with the raw training set. Siddiq et al.[8] introduced a unique statistical technique designed to pinpoint the optimal normalization method for a given dataset. The normalization process identified through this approach proved to significantly enhance the accuracy of an intrusion detection system. When tested on the NSL-KDD dataset, the model showcased impressive results, achieving an accuracy of 99.15%, an F1 score of 99.15%, a precision of 99.16%, and a recall of 99.13. Uhm et al.[9] introduced an innovative method that utilizes service-aware dataset partitioning. This approach not only offers significant scalability to manage large and constantly expanding network data but also enhances the classifier's performance, boosting both accuracy and processing speed. When tested on the Kyoto2016 dataset, the method showcased exemplary results for the Do Hulk category, with an accuracy of 99.99%, precision of 99.99%, recall of 99.97%, and an F1 score of 99.99%. Maseer et al.[10] introduced a comprehensive benchmarking methodology that encompasses multiple stages and utilizes authentic data to provide a robust assessment of IDS performance grounded in ML techniques. This evaluation spans multiple dimensions, incorporating diverse raw network datasets and suggested performance indicators. The outcomes from the proposed model were commendable, with an accuracy of 99.28%, precision of 99.37%, recall of 99.28%, and an F1 score of 99.17Al-Qatf et al.[11] introduced a deep learning method named self-taught learning (STL)-IDS, which is grounded in the STL framework. This method focuses on feature learning and dimension reduction, leading to significant reductions in both training and testing durations. Furthermore, it enhances the predictive accuracy of support vector machines (SVM) concerning cyberattacks. The findings indicate that this method not only sped up SVM's training and testing phases but also delivered superior performance, registering an accuracy of 99.416% when trained and tested on the NSL+KDD dataset Park et al.[12] undertook a study utilizing the Leipzig Intrusion Detection Data Set (LID-DS) — a host-based intrusion detection dataset introduced in 2018. They proposed a host-based intrusion detection framework that encompassed pre-processing, vector-to-image conversion, training, and testing phases to assess and enhance system performance. The outcomes revealed that the model achieved an accuracy of 93%, precision of 81%, recall of 83%, and an F1-score of 82%. Nie et al.[13] introduced an intrusion detection algorithm rooted in deep learning principles. They leveraged the capabilities of the generative adversarial network (GAN) to craft a potent intrusion detection technique. Moreover, they presented a novel intrusion detection model that amalgamates various models targeting individual attacks. By utilizing the GAN-based deep learning framework, they achieved intrusion detection targeting multiple attack types. The data indicates that their model secured an accuracy of 98.53%, a precision of 99.59%, a recall of 98.76%, a false alarm rate of 0.0326, and an F-measure of 99.17%. Assma et al. [14] crafted a model rooted in deep learning principles specifically tailored for identifying replay attacks in smart city environments. The distinctiveness of this approach lies in leveraging deep learning models to enhance the precision in detecting replay attacks. To gauge its effectiveness, this model was tested on an authentic smart city dataset where replay attacks were artificially introduced. The findings indicate that the model adeptly differentiates between regular activities and attack patterns, achieving a commendably high accuracy rate. Congyuan et al.[15] recognized the temporal nature of certain intrusions and, in response, put forth a unique IDS. This system amalgamates a recurrent neural network with gated recurrent units (GRU), a multilayer perceptron (MLP), and a softmax module. Testing on the widely referenced KDD 99 and NSL-KDD datasets revealed that their system delivered top-tier results. Specifically, the detection rates were 99.42% on the KDD 99 dataset and 99.31% on the NSL-KDD dataset, coupled with remarkably low false positive rates of 0.05% and 0.84% respectively. Remarkably, when focusing on denial of service attack detection, the system's performance peaked at detection rates of 99.98% for KDD 99 and 99.55% for NSL-KDD. Seth et al.[16] introduced an ensemble framework designed to adeptly identify varied attack categories. This framework is constructed by assessing and ranking the efficacy of diverse classifiers in pinpointing different attack types. Their results indicate a notable accuracy rate of 96.97%, coupled with a recall of 97.4%. Furthermore, their ensemble approach exhibited a superior attack detection rate compared to the foundational classifiers. Tian et al.[17] introduced a system geared towards detecting web attacks by analyzing URLs. This system, tailored for deployment on edge devices, incorporates two parallel deep learning models. When benchmarked against other existing systems using multiple datasets, it delivered compelling results: an accuracy of 99.410%, a true positive rate (TPR) of 98.91%, and a detection rate for legitimate requests (DRN) of 99.55%. These outcomes underscore the system's efficacy in identifying web-based threats. Manimurugan et al.[18] introduced a method

centered around deep learning, specifically using the Deep Belief Network (DBN) algorithm, tailored for the intrusion detection system. This method showcased superior outcomes across various metrics including accuracy, recall, precision, F1-score, and detection rate. The method registered remarkable accuracies: 99.37% for the normal category, 97.93% for Botnet, 97.71% for Brute Force, 96.67% for Dos/DDoS, 96.37% for Infiltration, 97.71% for Port Scan, and 98.37% for Web attack. These performance metrics were benchmarked against several other classifiers, highlighting the method's robustness. Gao et al.[19] introduced an adaptive ensemble learning approach that tailors the proportion of training data and establishes multiple decision trees, leading to the creation of a MultiTree algorithm. To enhance the overarching detection capabilities, they selected a range of foundational classifiers, encompassing decision tree, random forest, kNN, and DNN, and formulated an ensemble adaptive voting algorithm. Jeeune et al.[20] unveiled a procedure that transforms raw packet flows into input characteristics suitable for machine learning applications. This setup facilitates the rapid integration of diverse algorithms across multiple datasets, enabling a structured comparison of their performance. The experiments conducted yielded results that either aligned with or exceeded current benchmarks, underscoring the promise of their method. Given that raw traffic input features can be more efficiently and cost-effectively extracted than conventional features, they hold potential for incorporation in real-time systems that rely on deep learning. Benaddi et al. [21] introduced a novel IDS for network traffic based on Deep Reinforcement Learning (DRL), utilizing the Markov Decision Process (MDP) to enhance the system's decision-making capabilities. Furthermore, they conducted a detailed examination of the IDS's behavior by modeling the dynamics between the compliant IDS and adversarial entities using Stochastic Game Theory. The performance of their DRL-IDS was benchmarked against standard reinforcement learning (RL) and a range of machine learning techniques using the NSL-KDD dataset. The findings indicate that their DRL-IDS surpasses its counterparts, achieving higher detection rates and accuracy while minimizing false alarms. G.Kaur et al.[22] introduced an image-centric deep neural approach to categorize diverse cyberattacks, utilizing two detailed datasets: CICIDS2017 and CSE-CICIDS2018. In addition to this, they presented a curated list of optimal network flow attributes essential for pinpointing these threats. Employing a convolutional neural network, they were able to effectively classify and detail the nature of various attacks, yielding encouraging evaluation outcomes.. M.Basset et al.[23] introduced a deep learning model tailored for forensics, named Deep-IFS, designed to detect intrusions within IIoT traffic. The model employs the local gated recurrent unit (LocalGRU) to grasp local representations. Additionally, they incorporated a Multi-Head Attention (MHA) layer to effectively capture and assimilate global representations.

Table 1. Recent Contribution of Researchers

Ref	Technique used	Dataset	Accuracy	Precision	Recall	FI score	Limitation
[1]	Double-Layered Hybrid Approach (DLHA)	NSL-KDD	96.67	✓	-	-	High false positive alarms.
[2]	Support Vector Machine and sub space clustering	-	92.4	-	✓	✓	It needs initial training.
[4]	Support vectors machines, decision tree, K-Nearest Neighbor, and Naïve Bayes	NSL-KDD	RF classifier 86.35% and SVM 83.83%.	-	✓	-	Not suitable for detecting multi-step attacks
[5]	Machine learning	NSL-KDD and UNSW datasets	UNSW dataset, 91% UNSW, 83.47%	✓	-	-	Needs a large amount of knowledge of statistics
[8]	Deep Learning	NSL-KDD	99.15	99.16	99.13	99.15	High computational cost
[9]	Deep Learning	Kyto2016	99.99	99.99	99.97	99.99	Unable to detect the zero-day attack.
[10]	Machine learning	NSL-KDD	99.28	99.37	99.28	99.17	Not suitable for detecting multi-step attacks
[11]	Deep Learning and SVM	NSL+KDD	99.416	✓	✓	✓	Not suitable for detecting multi-step attacks

[12]	Machine learning	LID-DS	93	81	83	82	High computational cost
[13]	generative adversarial network (GAN),	-	98.53	99.59	98.76	99.17	It needs to be updated frequently with a new signature.
[15]	recurrent neural network	NSL-KDD	98.98	-	99.58	-	High computational cost
[16]	Deep learning	-	96.97	94	97.4	-	Not suitable for detecting multi-step attacks
[17]	Deep learning	NSL-KDD	99.410	✓	✓	✓	High computational cost
[18]	Deep learning	CSE-CIC-IDS2018	99.37	✓	✓	✓	Unable to detect the multiple attack.

I. Current Challenges and Future Scope

Intrusion Detection Systems (IDS) currently grapple with issues such as high false positive rates, difficulties in detecting zero-day attacks, scalability concerns, substantial computational costs, the continuous need for updates, and the challenge of obtaining labeled data. As attackers grow more sophisticated, even using machine learning to exploit IDS vulnerabilities, the challenges intensify. Looking ahead, the future of IDS lies in harnessing the potential of deep learning and artificial intelligence. Innovations like federated learning, which allows edge-device model training, can address privacy and data transfer challenges. Moreover, there's a growing emphasis on systems that can automatically respond to detected threats, ensuring rapid countermeasures. The eventual integration of quantum computing promises to revolutionize the speed and efficiency of IDS operations.

II. Conclusion

The security of internet-connected systems remains a focal point in the face of growing cyber threats. IDS serves as a critical line of defense, and the application of machine learning techniques in IDS has shown significant potential in enhancing detection capabilities. This study provided an in-depth examination of various IDS categorizations and emphasized the importance of integrating machine learning for more effective intrusion detection. The comparative analysis of the recent contributions showcased the varying approaches and results obtained by researchers in the field. It became evident that while there have been significant advancements, there are still challenges such as high computational costs, the need for frequent updates, and the inability to detect certain types of attacks. Future research endeavors should aim to address these challenges, ensuring more robust and efficient IDS implementations.

Conflict of Interest: The corresponding author, on behalf of all authors, confirms that there are no conflicts of interest to disclose.

Received 02 December 2022, Accepted 21 February, 2023

References

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

[2] G. Pu, L. Wang, J. Shen, and F. Dong, "A hybrid unsupervised clustering-based anomaly detection method," *Tsinghua Sci. Technol.*, vol. 26, no. 2, pp. 146–153, 2021, doi: 10.26599/TST.2019.9010051.

[3] A. Guezzaz, Y. Asimi, M. Azrour, and A. Asimi, "Mathematical validation of proposed machine learning classifier for heterogeneous traffic and anomaly detection," *Big Data Min. Anal.*, vol. 4, no. 1, pp. 18–24, 2021, doi: 10.26599/BDMA.2020.9020019.

[4] S. M. Kasongo and Y. Sun, "A deep learning method with filter based feature engineering for wireless intrusion detection system," *IEEE Access*, vol. 7, pp. 38597–38607, 2019, doi: 10.1109/ACCESS.2019.2905633.

[5] Z. Chkirbene, A. Erbad, R. Hamila, A. Mohamed, M. Guizani, and M. Hamdi, "TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection," *IEEE Access*, vol. 8, pp. 95864–95877, 2020, doi: 10.1109/ACCESS.2020.2994931.

[6] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2017, doi: 10.1109/ACCESS.2017.2782159.

[7] L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning," *IEEE Access*, vol. 9, pp. 7550–7563, 2021, doi: 10.1109/ACCESS.2020.3048198.

[8] M. A. Siddiqi and W. Pak, "An Agile Approach to Identify Single and Hybrid Normalization for Enhancing Machine Learning-Based Network Intrusion Detection," *IEEE Access*, vol. 9, pp. 137494–137513, 2021, doi: 10.1109/ACCESS.2021.3118361.

[9] Y. Uhm and W. Pak, "Service-Aware Two-Level Partitioning for Machine Learning-Based Network Intrusion Detection with High Performance and High Scalability," *IEEE Access*, vol. 9, pp. 6608–6622, 2021, doi: 10.1109/ACCESS.2020.3048900.

[10] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.

[11] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018, doi: 10.1109/ACCESS.2018.2869577.

[12] D. Park, S. Kim, H. Kwon, D. Shin, and D. Shin, "Host-Based Intrusion Detection Model Using Siamese Network," *IEEE Access*, vol. 9, pp. 76614–76623, 2021, doi: 10.1109/ACCESS.2021.3082160.

[13] L. Nie *et al.*, "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 1, pp. 134–145, 2022, doi: 10.1109/TCSS.2021.3063538.

[14] A. A. Elsaeidy, N. Jagannath, A. G. Sanchis, A. Jamalipour, and K. S. Munasinghe, "Replay Attack Detection in Smart Cities Using Deep Learning," *IEEE Access*, vol. 8, pp. 137825–137837, 2020, doi: 10.1109/ACCESS.2020.3012411.

[15] C. Xu, J. Shen, X. Du, and F. Zhang, "An Intrusion Detection System Using a Deep Neural Network With Gated Recurrent Units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018, doi: 10.1109/ACCESS.2018.2867564.

[16] S. Seth, K. K. Chahal, and G. Singh, "A Novel Ensemble Framework for an Intelligent Intrusion Detection System," *IEEE Access*, vol. 9, pp. 138451–138467, 2021, doi: 10.1109/ACCESS.2021.3116219.

[17] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A Distributed Deep Learning System for Web Attack Detection on Edge Devices," *IEEE Trans. Ind. Informatics*, vol. 16, no. 3, pp. 1963–1971, 2020, doi: 10.1109/TII.2019.2938778.

[18] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020, doi: 10.1109/ACCESS.2020.2986013.

[19] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection," *IEEE Access*, vol. 7, pp. 82512–82521, 2019, doi: 10.1109/ACCESS.2019.2923640.

[20] L. Le Jeune, T. Goedemé, and N. Mentens, "Machine Learning for Misuse-Based Network Intrusion Detection: Overview, Unified Evaluation and Feature Choice Comparison Framework," *IEEE Access*, vol. 9, pp. 63995–64015, 2021, doi: 10.1109/ACCESS.2021.3075066.

[21] H. Benaddi, K. Ibrahimi, A. Benslimane, M. Jouhari, and J. Qadir, "Robust Enhancement of Intrusion Detection Systems using Deep Reinforcement Learning and Stochastic Game," *IEEE Trans. Veh. Technol.*, pp. 1–14, 2022, doi: 10.1109/TVT.2022.3186834.

[22] G. Kaur, A. Habibi Lashkari, and A. Rahali, "Intrusion Traffic Detection and Characterization using Deep Image Learning," in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2020, pp. 55–62. doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00025.

{23} M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty, and M. Ryan, "Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment," *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7704–7715, 2021, doi: 10.1109/TII.2020.3025755.