Machine Learning-Based Intrusion Detection of Imbalanced Traffic on the Network: A Review

S. V. Sugin and M. Kanchana

Abstract Cyber threats are a very widespread problem in today's world, and because there are an increasing number of obstacles to effectively detecting intrusions, security services, such as data confidentiality, integrity, and availability, are harmed. Day by day, attackers discover new sorts of threats. First and foremost, the type of attack should be carefully assessed with the aid of Intrusion Identification Methods (IIMs) for the prevention of these types of attacks and to provide the exact solution. IIMs that are crucial in network security have three main features: first, they gather data, then they choose a feature, and finally, they choose an engine. As the amount of data produced grows every day, so does the number of data-related threats. As a result of the growing number of data-related attacks, present security applications are insufficient. In this research, the Modified Nearest Neighbor (MNN) and the Technique for Sampling Difficult Sets (TSDS) are two machine learning techniques that have been suggested to detect assault in this research. It is intended to employ an IIM technique based on a machine learning (ML) algorithm by comparing literature and giving expertise in either intrusion detection or machine learning algorithms.

Keywords IIM · Imbalanced traffic network · Technique for Sampling Difficult Sets · ML · DL

1 Introduction

The use of the internet has been steadily expanding recently. It offers a lot of possibilities in applications, considering education, business, healthcare, and a variety of other industries. Everyone has access to the internet. This is where the primary issue arises. The information we obtain from the internet must be protected. This Intrusion

S. V. Sugin (✉) · M. Kanchana
Department of Computing Technologies, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chennai, India
e-mail: sugin.sv@gmail.com; ss9372@srmist.edu.in

M. Kanchana
e-mail: kanchanm@srmist.edu.in

Y. Singh et al. (eds.), *Proceedings of International Conference on Recent Innovations in Computing*, Lecture Notes in Electrical Engineering 1011,
https://doi.org/10.1007/978-981-99-0601-7_57

Identification (IIM) ensures data security over the network and system. Firewalls and other traditional ways of implementing, for the sake of security, authentication procedures have been implemented [1]. The first level of protection for data was considered, and the second level of protection was studied.

IIM is used to detect illegal or aberrant conduct. An attack is initiated on a network that is exhibiting unusual activity. Attackers take advantage of network flaws such as poor security procedures and practices, as well as program defects such as buffer overflows, to cause network breaches [2]. It is possible that the attackers are less accessible component services on the lookout to get more control of access or black hat attackers looking to check on regular internet users for critical information. Methods for identifying intrusion can be centered on detecting misuse or based on detecting anomalies. Misuse-based IIM examines traffic on the network and compares it to a set of criteria in a database of predefined malicious activity signatures. Attacks are identified in the identification of anomalies method.

2 Intrusion Identification Methods (IIMs)

Access to the network or a hacker's use of a resource is referred to as an intrusion. An intrusion is used to diminish the integrity, confidentiality, and availability of a resource. In the current world, an intruder tries to obtain entry to illegal metrics and causes harm to the hacker actions that are identified [3] (Fig. 1).

Intrusion Identification Methods (IIMs) detect all of these types of harmful actions on a network and alert the network administrator to secure the information needed to defend against these attacks [2]. The development of IIM has increased security in a network and the protection of service data.

As a result, an Intrusion Identification Method (IIM) is a network and computer security solution that keeps track of network traffic [4]. Firewall security is provided by an IIM. A firewall protects an enterprise by detecting dangerous internet activity, whereas an IIM detects attempts to breach firewall protection or gain access, and

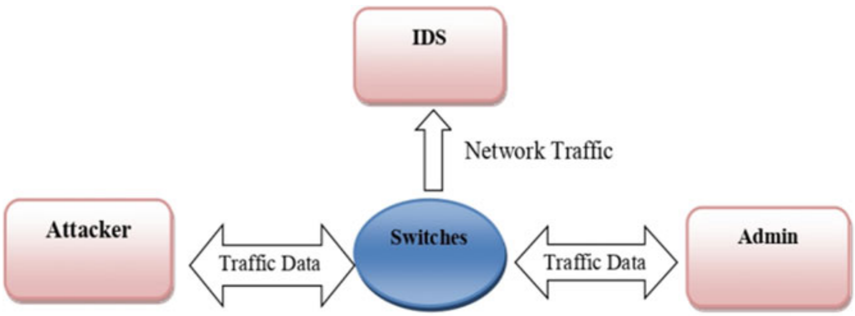

Fig. 1 Intrusion identification methods (IIMs)

it quickly notifies the administrator that something needs to be done. As a result, IIMs are security systems that detect various attacks on the network and ensure the security of our systems.

3 Network Intrusion Identification Model Framework

Faced with this unbalanced traffic on the internet, we suggested the Technique for Sampling Difficult Sets (TSDS) algorithm, which compresses the majority class samples, while in tough situations, enhancing the quantity of minority samples is a must to decrease the training set's imbalance and allow the Intrusion Identification Method to improve category performance [5]. For classification models, as classifiers, employ RF, SVM, k-NN, and Alex Net.

The intrusion identification model presented in Fig. 2 was proposed. Data preprocessing such as processing of duplicates, incomplete data, and missing data is done first in our intrusion identification structure [6]. The test and training sets were then partitioned, with the sets of practice being treated for metrics balance with the help of our suggested TSDS algorithm. We utilize StandardScaler to normalize and digitize the sample labels and analyze the data before modeling to speed up the convergence [7]. Likewise, the practice set is processed and utilized for the training data to be constructed, which is then evaluated using the test set.

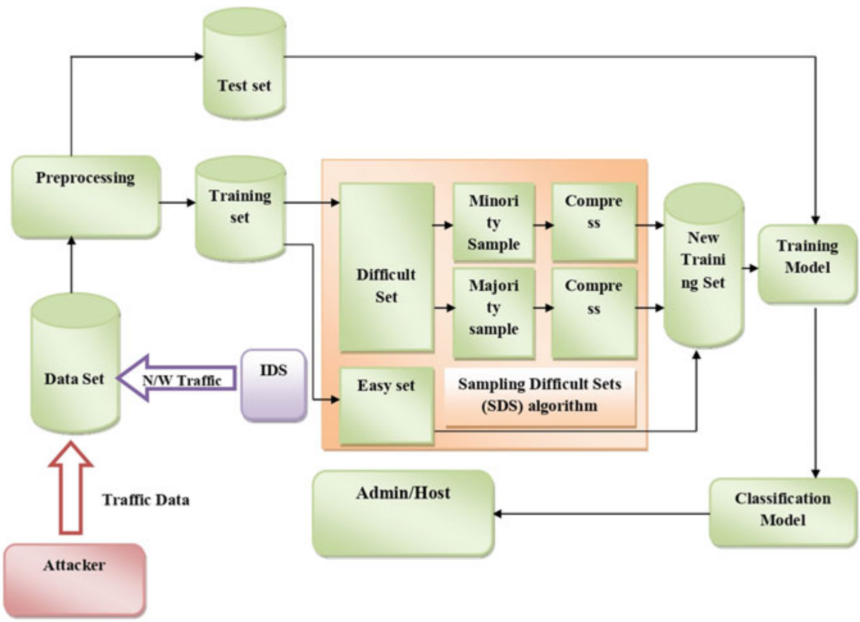

Fig. 2 Network intrusion identification system model framework

Several traffic data types have comparable patterns in imbalanced network traffic, and minority attacks, in particular, might be hidden within a significant tough for the classifier to understand the distinctions between them during the training phase because there is a lot of typical traffic [8]. The redundant noise data is the majority class in the unbalanced training set's comparable samples. Because the majority class's number is substantially greater than the class of the minority predictor, who is not able to understand the minority class's spread, the majority level is compact. Discrete traits in the minority class remain constant, but constant attributes change [9]. As a result, the continuous qualities of the minority class are magnified to provide data that adheres to the genuine distribution. As a result, we propose the TSDS algorithm as a means of redressing the imbalance.

First, using the Modified Nearest Neighbor (MNN) technique, the near-neighbor and far-neighbor sets were created from an unbalanced set of data [10]. Because the samples from the collection of near-neighbors are so similar, the classifier has a hard time recognizing the distinctions between the groups. In the identification process, we refer to them as "exhausting instances and extracts." Then, in the tough set, they move in and out of the samples from the minority. Likewise, the augmentation samples from the easy set and the toughest set's minorities are merged to make a new set of exercises. In the MNN method, the K-neighbors are used as the availability aspect for the complete algorithm [11]. The number of problematic samples grows as the scaling factor K increases, as does the compression.

3.1 Comparison of Accuracy on Datasets

See Table 1 and Fig. 3.

3.2 Comparison of Various ML-Based IDS Approaches

See Table 2.

4 Discussions

The research trends in benchmark datasets for evaluating NIDS models are also graphically illustrated. The KDD Cup '99 dataset is shown to be the most popular, followed by the NSL-KDD dataset. However, the KDD '99 dataset has the issue of being quite old and not resembling present traffic data flow. Other datasets are accessible as well, but the research trend in these datasets is quite low due to the new dataset's lack of appeal in research. It is suggested that researchers can be encouraged

Table 1 Comparison of accuracy on datasets

S. No.	Author	Attack	Dataset	Accuracy (%)
1	L. Liu, IEEE Access [1]	Denial of Service (DoS)	NSL-KDD	78.24
2	J. Alikhanov, IEEE Access [3]	Distributed Denial of Service (DDoS)	NSL-KDD,AWSCIC-IDS	84.61
3	T. Kim, IEEE Access[2]	Distributed Denial of Service (DDoS)	CSE-CIC-IDS2018	88.97
4	Z. K. Maseer, IEEE Access [12]	Denial of service (DOS)	CIC-IDS2017	85.88
5	M. Wang, IEEE Access[8]	Neptune	NSL-KDD	89
6	A. Kavousi, IEEE Transactions[10]	Havex Malware	LUBE-SOS	82.83
7	Z. Chkirbene, IEEE Systems [13]	Denial of service (DOS)	NSL-KDD	80
8	M. A. Siddiqi, IEEE Access[6]	Botnet	ISCX-IDS2012	96.51
9	G. De Carvalho Bertoli, IEEE Access [14]	Malware	AB-TRAP	54
10	Y. Uhm, IEEE Access [9]	Denial of service (DOS)	CIC-IDS2017	97.78
11	D. Han, IEEE [4]	Botnet, Distributed Denial of Service (DDoS)	Kitsune	81.65, 79.55
12	L. Jeune, IEEE Access[7]	Botnet, Distributed Denial of Service (DDoS)	DARPA1998	86.34, 80
13	S. Wang, IEEE Access[15]	Distributed Denial of Service (DDoS)	UNSW-NB15	90
14	M. Injadat, IEEE Transactions [16]	Distributed Denial of Service (DDoS)	UNSW-NB2015	74
15	W. Seo, IEEE Access[17]	Distributed Denial of Service (DDoS)	UNSW-NB15	95.8
16	D. Gumusbas, IEEE Journal [11]	Denial of service (DOS)	AWID2018	78.4

(continued)

Table 1 (continued)

S. No.	Author	Attack	Dataset	Accuracy (%)
17	C. Liu, IEEE Access[18]	Distributed Denial of Service (DDoS)	NSL-KDD, CIS-IDS2017	99.87
18	Y. Li, IEEE Access[19]	Denial of service (DOS)	NSL-KDD	94.25
19	Y. Tang, IEEE Access [20]	Denial of service (DOS)	UNSW-NB15	88.53
20	G. Siewruk, IEEE Access [21]	Denial of service (DOS)	NSL-KDD	98
21	W. Xu, IEEE Access[22]	Denial of service (DOS)	NSL-KDD	90.61
22	A. G. Roselin, IEEE Access [23]	Distributed Denial of Service (DDoS)	NSL-KDD	81.82
23	A. R. Gad, IEEE Access[24]	Distributed Denial of Service (DDoS)	NSL-KDD, KDD-CUP99	80.65
24	Z. Li, IEEE Journal [5]	Denial of service (DOS)	NSL-KDD, CIC-IDS2017	93.12
25	L. Le Jeune, IEEE Access [7]	Distributed Denial of Service (DDoS)	NSL-KDD	94.7
26	Y. D. Lin, IEEE Access [25]	Denial of service (DOS)	CSE-CIC-IDS2018	97
27	M. D. Rokade, (ESCI) [26]	Denial of service (DOS)	NSL-KDD-CUP-1999	88.50
28	P. F. Marteau, IEEE Transactions [27]	Denial of service (DOS)	CIDDS	80
29	W. Wan, Z. Peng, (ICCEA) [28]	Denial of service (DOS)	NS-KDD	80.49
30	M. Lopez-Martin, IEEE Access[29]	Distributed Denial of Service (DDoS)	UNSW-NB15	91

to use modern datasets with more detailed attributes that are more relevant to today's environment.

5 Conclusion

In this review, we studied the dataset assault through machine learning techniques. It reviewed ML models from different assaults available in the dataset. As a result of

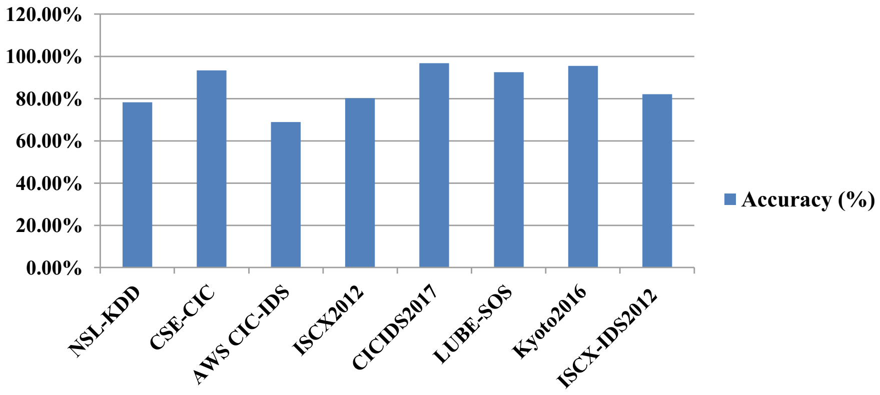

Fig. 3 Comparison of classifier accuracy on datasets

Table 2 Comparison of the related works

S. No.	Authors	Key findings	Techniques used	Dataset	Limitations
1	L. Liu, IEEE Access [1]	Demonstrating advantages over existing methods and the high potential for usage in emerging NIDS	To present a novel Difficult Set Sampling Technique (DSSTE) method	NSL-KDD, CSE-CIC	Intrusion detection systems have a hard time predicting the distribution of malicious attempts
2	J. Alikhanov, IEEE Access [3]	On the NIDS detection rate, different extraction strategies are applied	Sketch-Guided Sampling (SGS) techniques are used	NSL-KDD, AWS CIC-IDS	The impact of sampling on NIDS based on anomalies should be less evaluated
3	T. Kim, IEEE Access[2]	Through pattern matching with incoming packets, the NIDS attacks and detects intrusions very efficiently	The classification detection rate and classification speed may both be increased by using ML-NIDS	ISCX2012, CSE-CIC-IDS2018	The ML-NIDS defects may be exploited to dramatically enhance prediction
4	Z. K. Maseer, IEEE Access [12]	Anomaly-based IDS (AIDS) can identify malware and violent attacks by analyzing the sent data in depth	Implementing anomaly-based IDS (AIDS) dataset	CIC-IDS2017	Increase the vulnerability of AIDS

(continued)

Table 2 (continued)

S. No.	Authors	Key findings	Techniques used	Dataset	Limitations
5	M. Wang, IEEE Access [8]	An Improved Conditional Variational Autoencoder (ICVAE) with a enhance detection rates	Framework uses SHapley Additive exPlanations (SHAP)	NSL-KDD	Framework not in real time
6	A. Kavousi, IEEE Transactions [10]	Anomaly Detection Model based on LUBE and SOS	The use of prediction intervals (PIs) is used to develop an intelligent anomaly detection approach	LUBE-SOS	Malicious attacks with different severities, data can attack easily
7	Z. Chkirbene, IEEE Systems [13]	Unsupervised and supervised learning approaches are used to create triangle area-based closest neighbors (TANN)	The Euclidean distance map (EDM) is a novel method for detecting anomalies using sequential algorithms	UNSW-NB, NSL-KDD	In compared to modern system procedures, the EDM technique has a lower warning rate
8	M. A. Siddiqi, IEEE Access [6]	The detection rate of intrusion detection is high when guided ML methods are used	IDS approaches based on a random forest were utilized	CIC-IDS2017, ISCX-IDS2012	The reinforcing procedure provided less efficiency
9	G. De Carvalho Bertoli, IEEE Access [14]	The AB-TRAP is used to identify attackers in both local (LAN) and global (internet) aspects	AB-TRAP organizes the process of designing and implementing NIDS systems	AB-TRAP	Applying machine learning algorithms to give fresh techniques is a key point in favor of not recycling old datasets
10	Y. Uhm, IEEE Access [9]	To reduce the minority class problem, a service-aware partitioning method was developed	Random forest (RF) and decision tree (DT), as well as deep neural networks (DNNs), are used to build NIDS	CIC-IDS2017, Kyoto2016	Improve the real-time intrusion prevention algorithm that has been presented

(continued)

Table 2 (continued)

S. No.	Authors	Key findings	Techniques used	Dataset	Limitations
11	D. Han, IEEE [4]	Network Intrusion Identification Methods based on anomaly also use machine learning (ML) techniques	Particle Swarm Optimization (PSO) based on algorithm for traffic mutation	Kitsune	The scalability of ML-focused NIDS is being improved
12	L. Jeune, IEEE Access [7]	Intrusion Detection Expert System (IDES) and HIDS	The botnet was utilized in a large-scale (DDoS) effort on the (DNS)	DARPA1998, NSL-KDD	Real-world scenario is not synthesized in the datasets
13	S. Wang, IEEE Access [15]	To protect networks against malicious access	Used firewalls, deep packet inspection systems and intrusion detection systems	NSL-KDD, UNSW-NB15	The performance validated by UNSW-NB15 cannot be clearly categorized
14	M. Injadat, IEEE Transactions [16]	SMOTE is done to increase the training model's performance and decrease network traffic data class imbalance	In order to apply Z-score normalization and SMOTE, data preprocessing is required	CIC-IDS2017, UNSW-NB2015	When compared to the CBFS approach, the IGBFS method had a higher detection accuracy
15	W. Seo IEEE Access [17]	In signature-based detection and anomaly detection, cyberattacks have made significant progress	Convolutional neural networks' (CNNs) algorithm is used	UNSW-NB15	To develop real-time IPSs and identify current network system vulnerabilities
16	D. Gumusbas, IEEE Journal [11]	Artificial Neural Networks (ANNs) and Deep Belief Networks	Packet CAPture (PCAP) and the NetFlow protocol	AWID2018, CIC-IDS2017	To do classification, another ML model is required
17	C. Liu, IEEE Access [18]	Adaptive Synthetic Sampling (ADASYN)	Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM)	NSL-KDD, CIS-IDS2017	It takes a long time and has a low efficiency
18	Y. Li, IEEE Access [19]	Domain Generation Algorithm (DGA)	Hidden Markov model (HMM)	NSL-KDD	DNN model classification should be improved

(continued)

Table 2 (continued)

S. No.	Authors	Key findings	Techniques used	Dataset	Limitations
19	Y. Tang, IEEE Access [20]	Randomly initializing weights and deviations increases the speed of an extreme learning machine (ELM)	Improved particle swarm optimized online regularized extreme learning machine (IPSO-IRELM)	NSL-KDD, UNSW-NB15	To increase IRELM's capacity to classify data
20	G. Siewruk, IEEE Access [21]	Context-aware software vulnerability classification system	Continuous Integration and Continuous Deployment (CICD)	NSL-KDD	Improve the vulnerability performance
21	W. Xu, IEEE Access [22]	The network is recreated using Mean Absolute Error (MAE)	Autoencoder (AE)-based deep learning approaches	NSL-KDD	Improve the performance of the dataset
22	A. G. Roselin, IEEE Access [23]	To identify malicious network traffic, BIRCH clustering technique is used	Optimized Deep Clustering (ODC)	NSL-KDD	ODC technique has a lower detection rate of anomalies
23	A. R. Gad, IEEE Access [24]	Synthetic minority oversampling technique (SMOTE)	The Chi-square (Chi^2) approach was used to pick features. ODC technique has a lower detection rate of anomalies	NSL-KDD, KDD-CUP99	Less complexity
24	Z. Li, IEEE Journal [5]	Gated Recurrent Unit and Long Short-Term Memory	Broad Learning System	NSL-KDD, CIC-IDS2017	Less accuracy BLS algorithms
25	L. Le Jeune, IEEE Access [7]	PCCN-based approaches are used	Intrusion Detection Expert System	NSL-KDD	IDES performance should be improved
26	Y. D. Lin, IEEE Access [25]	Variational autoencoder and multilayer perception model are used	Range-based sequential search algorithm	CSE-CIC IDS2018	Improve the categorization of segmentation
27	M. D. Rokade, (ESCI) [26]	SVM-IDS approach based on deep learning	Artificial Neural Network algorithm	KKDDCUP99, NLS-KDD	Classification and detection of high-class objects should be improved

(continued)

Table 2 (continued)

S. No.	Authors	Key findings	Techniques used	Dataset	Limitations
28	P.F.Marteau IEEE Transactions [27]	One-class SVM classifier (1C-SVM) is used	Semi-supervised DiFF-RF algorithm	CIDDS	Inaccurate datasets
29	W. Wan, Z. Peng,(ICCEA) [28]	All single DNN classifiers are integrated using the AdaBoost technique	Generative Adversarial Networks (GAN)	KDD99, NS-KDD	Increase the sample deduction accuracy rate
30	M. Lopez-Martin, IEEE Access [29]	Radial Basis Function (RBF) is implemented	Radial Basis Function Neural Networks (RBFNNs)	NSL-KDD, UNSW-NB15	Improve the suggested dataset's performance metrics

the growing number of data-related assaults, present security applications are insufficient. In this research, the Modified Nearest Neighbor (MNN) and the Technique for Sampling Difficult Sets (TSDS) are two machine learning techniques that have been suggested to detect assault in this research. More recent and updated datasets must be utilized in future research in order to assess deployed algorithms in order to deal with more current harmful intrusions and threats.

References

1. Liu L, Wang P, Lin J, Liu L (2021) Intrusion detection of imbalanced network traffic based on machine learning and deep learning. IEEE Access 9:7550–7563. https://doi.org/10.1109/ACCESS.2020.3048198
2. Kim T, Pak W (2022) Robust network intrusion detection system based on machine-learning with early classification. IEEE Access 10:10754–10767. https://doi.org/10.1109/ACCESS.2022.3145002
3. Alikhanov J, Jang R, Abuhamad M, Mohaisen D, Nyang D, Noh Y (2022) Investigating the effect of traffic sampling on machine learning-based network intrusion detection approaches. IEEE Access 10:5801–5823. https://doi.org/10.1109/ACCESS.2021.3137318
4. Han D et al (2021) Evaluating and improving adversarial robustness of machine learning-based network intrusion detectors. IEEE J Sel Areas Commun 39(8):2632–2647. https://doi.org/10.1109/JSAC.2021.3087242
5. Li Z, Rios ALG, Trajkovic L (2021) Machine learning for detecting anomalies and intrusions in communication networks. IEEE J Sel Areas Commun 39(7):2254–2264. https://doi.org/10.1109/JSAC.2021.3078497
6. Siddiqi MA, Pak W (2021) An agile approach to identify single and hybrid normalization for enhancing machine learning-based network intrusion detection. IEEE Access 9:137494–137513. https://doi.org/10.1109/ACCESS.2021.3118361
7. Le Jeune L, Goedemé T, Mentens N (2021) Machine learning for misuse-based network intrusion detection: overview, unified evaluation and feature choice comparison framework. IEEE Access 9:63995–64015. https://doi.org/10.1109/ACCESS.2021.3075066

8. Wang M, Zheng K, Yang Y, Wang X (2020) An explainable machine learning framework for intrusion detection systems. IEEE Access 8:73127–73141. https://doi.org/10.1109/ACCESS.2020.2988359
9. Uhm Y, Pak W (2021) Service-aware two-level partitioning for machine learning-based network intrusion detection with high performance and high scalability. IEEE Access 9:6608–6622. https://doi.org/10.1109/ACCESS.2020.3048900
10. Kavousi-Fard A, Su W, Jin T (2021) A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids. IEEE Trans Industr Inf 17(1):650–658. https://doi.org/10.1109/TII.2020.2964704
11. Gumusbas D, Yıldırım T, Genovese A, Scotti F (2021) A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. IEEE Syst J 15(2):1717–1731. https://doi.org/10.1109/JSYST.2020.2992966
12. Maseer ZK, Yusof R, Bahaman N, Mostafa SA, Foozy CFM (2021) Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. IEEE Access 9:22351–22370. https://doi.org/10.1109/ACCESS.2021.3056614
13. Chkirbene Z et al (2021) A weighted machine learning-based attacks classification to alleviating class imbalance. IEEE Syst J 15(4):4780–4791. https://doi.org/10.1109/JSYS.2020.3033423
14. De Carvalho Bertoli G et al (2021) An end-to-end framework for machine learning-based network intrusion detection system. IEEE Access 9:106790–106805.https://doi.org/10.1109/ACCESS.2021.3101188
15. Wang S, Balarezo JF, Kandeepan S, Al-Hourani A, Chavez KG, Rubinstein B (2021) Machine learning in network anomaly detection: a survey. IEEE Access 9:152379–152396. https://doi.org/10.1109/ACCESS.2021.3126834
16. Injadat M, Moubayed A, Nassif AB, Shami A (2021) Multi-stage optimized machine learning framework for network intrusion detection. IEEE Trans Netw Serv Manage 18(2):1803–1816. https://doi.org/10.1109/TNSM.2020.3014929
17. Seo W, Pak W (2021) Real-time network intrusion prevention system based on hybrid machine learning. IEEE Access 9:46386–46397. https://doi.org/10.1109/ACCESS.2021.3066620
18. Liu C, Gu Z, Wang J (2021) A hybrid intrusion detection system based on scalable K-means+ random forest and deep learning. IEEE Access 9:75729–75740. https://doi.org/10.1109/ACCESS.2021.3082147
19. Li Y, Xiong K, Chin T, Hu C (2019) A machine learning framework for domain generation algorithm-based malware detection. IEEE Access 7:32765–32782. https://doi.org/10.1109/ACCESS.2019.2891588
20. Tang Y, Li C (2021) An online network intrusion detection model based on improved regularized extreme learning machine. IEEE Access 9:94826–94844. 10.1109/ ACCESS. 2021.3093313
21. Siewruk G, Mazurczyk W (2021) Context-aware software vulnerability classification using machine learning. IEEE Access 9:88852–88867. https://doi.org/10.1109/ACCESS.2021.3075385
22. Xu W, Jang-Jaccard J, Singh A, Wei Y, Sabrina F (2021) Improving performance of auto encoder-based network anomaly detection on NSL-KDD dataset. IEEE Access 9:140136–140146. https://doi.org/10.1109/ACCESS.2021.3116612
23. Roselin AG, Nanda P, Nepal S, He X (2021) Intelligent anomaly detection for large network traffic with optimized deep clustering (ODC) algorithm. IEEE Access 9:47243–47251. https://doi.org/10.1109/ACCESS.2021.3068172
24. Gad AR, Nashat AA, Barkat TM (2021) Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT Dataset. IEEE Access 9:142206–142217. https://doi.org/10.1109/ACCESS.2021.3120626
25. Lin YD, Liu Z-Q, Hwang R-H, Nguyen V-L, Lin P-C, Lai Y-C (2022) Machine LEARNING with variational autoencoder for imbalanced datasets in intrusion detection. IEEE Access 10:15247–15260. https://doi.org/10.1109/ACCESS.2022.3149295
26. Rokade MD, Sharma YK (2021) MLIDS: a machine learning approach for intrusion detection for real time network dataset. In: 2021 International conference on emerging smart computing and informatics (ESCI), pp 533–536. 10.1109/ ESCI50559.2021. 9396829

27. Marteau PF (2021) Random partitioning forest for point-wise and collective anomaly detection-application to network intrusion detection. IEEE Trans Inf Forensics Secur 16:2157–2172. https://doi.org/10.1109/TIFS.2021.3050605
28. Wan W, Peng Z, Wei J, Zhao J, Long C, Du G (2021) An effective integrated intrusion detection model based on deep neural network. In: 2021 International conference on computer engineering and application (ICCEA), pp 146–152. 10.1109/ ICCEA53728. 2021.00037
29. Lopez-Martin M, Sanchez-Esguevillas A, Arribas JI, Carro B (2021) Network intrusion detection based on extended RBF neural network with offline reinforcement learning. IEEE Access 9:153153–153170. https://doi.org/10.1109/ACCESS.2021.3127689