Journal of Applied Automation Technologies

Review Paper

Network Intrusion Detection Model Based on Data-Driven Algorithm: A Reivew

Ferenc Fekete[1,*], Andrea Lakatos[2], Anna Varga[2]

[1] School of Software Engineering, Budapest University of Technology and Economics, 1111 Budapest, Hungary
[2] Department of Information Technology, Budapest University of Technology and Economics, 1111 Budapest, Hungary
*Corresponding author: f.fekete@bute.edu.hu

Abstract. Network intrusion detection is a key technology for maintaining network security. In the digital era, network attacks are increasingly complex and diverse, and traditional rule-based detection methods are difficult to cope with. Data-driven algorithms demonstrate powerful detection capabilities by analyzing historical data and automatically learning potential patterns. This paper provides a comprehensive overview of the research on network intrusion detection models based on data-driven algorithms. First, it introduces the background and importance of network intrusion detection, and explains its key role in guaranteeing network data integrity and service availability. Then, the application of data-driven algorithms in network intrusion detection is discussed in detail and the principles, advantages and limitations of various algorithms are analyzed from the two dimensions of supervised learning and unsupervised learning. Then, the model performance is evaluated from multiple dimensions such as detection accuracy, precision, recall, F1 score and AUC value, and the performance of different algorithms is compared. The contribution of this paper is to systematically sort out the research lineage in this field, summarize the existing results and shortcomings, and provide a clear starting point for the subsequent research, which helps to improve the intelligence level of network intrusion detection system and enhance the network security protection capability.

Keywords: *Network intrusion detection; Data-driven algorithms; multiple dimensions; learning potential patterns*

Received on 13 March 2025, Accepted on 02 June 2025, Published on 11 June 2025

Introduction

With the increasing sophistication and stealthiness of network attacks, as well as the explosive growth of data size in network environments, traditional rule- and feature-matching based network intrusion detection methods are gradually overstretched [1]. Data-driven algorithms, with their powerful self-learning capabilities and efficient processing of massive data, show great potential for application in the field of network intrusion detection [2,3]. The network intrusion detection model based on data-driven algorithms can automatically identify abnormal patterns and potential threats in network traffic, which helps to realize the timely detection of new types of attacks and variants of attacks, thus effectively improving the timeliness and accuracy of network security protection [4-6]. From the academic point of view, the research in this field involves the cross-fertilization of multiple disciplines, such as data mining, machine learning, deep learning, network security, etc., which is of great significance in expanding and enriching the theoretical system of related disciplines [7-10]. At the practical application level, with the help of these advanced data-driven detection models, enterprises and organizations are able to better protect their network assets and reduce the risk of economic loss and information leakage due to network intrusion, which has non-negligible potential value for maintaining national network security and social stability [11].

The key task of network intrusion detection system is to timely and accurately identify abnormal behaviors and potential threats in the network [12]. Its main research includes: exploring novel data-driven algorithms to

improve detection efficiency and accuracy [13]; optimizing feature extraction and selection methods to better capture key information in network traffic; investigating the model's adaptivity so that it can quickly respond to changes in the network environment and the emergence of new types of attacks [14]; and enhancing the model's interpretability so that security experts can better understand the detection results and take appropriate measures [15].

Currently, research on network intrusion detection has made significant progress. Data-driven algorithms, especially machine learning and deep learning methods, are widely used in this field [16]. These algorithms are capable of processing massive amounts of data and learning complex patterns and features from it. Deep neural networks (DNNs) [17], convolutional neural networks (CNNs) [18], and recurrent neural networks (RNNs) [19] and their variants (e.g., LSTMs and GRUs) [20] perform well in network intrusion detection and are able to efficiently identify both known and unknown attack types. In addition, integrated learning methods [21], such as Random Forest and Support Vector Machine (SVM), have demonstrated strong classification capabilities. However, these algorithms still face many challenges in practical applications, such as the efficiency of real-time detection, the scalability of the model, and the ability to detect unknown attacks [22].

The issue of data quality is a key challenge in the research and application of data-driven algorithms. The complexity and diversity of network data place high demands on data preprocessing and feature engineering [23]. In addition, the balance between model complexity and computational efficiency is also an important issue. Deep learning models usually have high computational complexity and require a large amount of computational resources and time, which may be difficult to meet the demands of real-time detection in practical applications [24]. Meanwhile, the poor interpretability of the models makes it difficult for security experts and system administrators to understand and trust the results [25]. In addition, the dynamics and variability of network attacks require models to be able to quickly adapt to new attack patterns, while the update mechanisms of existing models are often not flexible and efficient enough [26].

This paper provides a comprehensive and systematic overview and summary of key technologies and recent advances in the field of network intrusion detection, which provides a clear starting point and direction for subsequent research. First, this paper comprehensively explains the principles and challenges of network intrusion detection, and clarifies the core position and role mechanism of data-driven algorithms in network intrusion detection. Second, the applications of supervised and unsupervised learning methods in this field are systematically summarized, revealing the advantages and limitations of various types of algorithms. Once again, the detection efficacy of different algorithms is deeply analyzed from multiple key performance indicators. Finally, we look forward to the future of network intrusion detection technology, and put forward forward-looking research proposals, in order to promote the further development of the field.

Network Intrusion Detection Problem Analysis

Network Intrusion Detection Principle

Network intrusion detection is a proactive defense technique designed to monitor network activity in real time and identify potential intrusions [27]. It determines the presence of anomalous behavior or known attack patterns by analyzing network traffic data or system audit records. The network intrusion detection system is mainly composed of data acquisition module, data preprocessing module, detection engine module, and alarm and response module [28], as shown in Table 1.

Table 1. Network intrusion detection system architecture

Module Name	Description	Function
Data Acquisition Module	Collects data from the network including network traffic system logs application logs	Provides the data foundation needed for intrusion detection
Data Preprocessing Module	Performs operations on raw data such as cleaning normalization and feature extraction	Improves data quality and suitability preparing for subsequent analysis
Detection Engine Module	Analyzes data using various analytical techniques such as pattern matching statistical analysis and machine learning	Identifies abnormal behaviors or known attack patterns and serves as the core of intrusion detection
Alarm and	Triggers alarms notifies administrators or related systems	Responds to potential intrusion behaviors

Response Module	and takes appropriate responsive actions	promptly reducing losses

As can be seen from Table 1, the data acquisition module is responsible for collecting data from the network; the data preprocessing module performs operations such as data integrity check, normalization, and feature extraction on the collected raw data to eliminate noise and inconsistencies in the data and convert the data into a format suitable for analysis [29-31]; the detection engine module analyzes the preprocessed data using various analytical techniques to identify any anomalous behaviors or known attack patterns [32]; the alarm and response module triggers an alarm to notify the administrator or the relevant system and take appropriate response measures [33].

Analysis of Factors Affecting Network Intrusion Detection

The performance of network intrusion detection is affected by a variety of factors, which can be categorized into data-related factors, network environment-related factors and system resource-related factors [34], as shown in Table 2.

Table 2. MOEA/D optimization algorithm parameter settings

No	Category	Specific Factors
1	Data-Related Factors	Data Quality Data Dimensionality Data Scale
2	Network Environment-Related Factors	Network Topology Communication Protocols Device Types
3	System Resource-Related Factors	Computational Power Storage Capacity Network Bandwidth

Among the data-related factors, high-quality data should have accuracy, completeness, consistency, and timeliness, which will affect the accuracy and reliability of the detection model if the data have problems such as noise, missing values, or inconsistency of data from multiple sources [35]; high-dimensional data usually contain a large number of features, which may include many irrelevant or redundant features, which will increase the complexity and training time of the model, as well as decrease the detection efficiency [36]; large-scale data, on the other hand, puts higher demands on the system's storage and computational capabilities [37].

Among the factors related to the network environment, network topology, communication protocols, and device types can have an impact on intrusion detection [38]. Complex network topology may lead to the diversity of data transmission paths, which increases the difficulty of data collection and analysis; different communication protocols have different data formats and behavioral characteristics, which need to be analyzed and detected in a targeted manner; and the type and number of devices in the network also affect the data generation and transmission characteristics, which puts forward different requirements for the design and optimization of intrusion detection systems.

Among the system resource-related factors, network intrusion detection systems usually need to operate with limited system resources, such as computing power, storage capacity, and network bandwidth [39]. Insufficient computing power may lead to slower training and inference of detection models, which cannot meet the requirements of real-time detection [40]; limited storage capacity may not be able to save enough historical data, which affects the analysis of long-term trends and complex attack patterns [41]; and limitations in network bandwidth may affect real-time data transmission and collection, leading to data loss or delay, which in turn affects the timeliness and accuracy [42].

Detection of anomaly pattern analysis

Detecting anomaly patterns is crucial in the field of network security. It identifies anomalies that significantly deviate from the normal pattern by analyzing the characteristics of network traffic and system behavior, thus discovering potential intrusions [43]. Common types of detection anomaly patterns and their analysis counterparts are shown in Table 3.

Table 3. Comparison of network intrusion detection anomaly pattern analysis

No	Anomaly Detection Pattern	Specific Manifestation	Detection Method

1	Traffic Feature Anomaly	Sudden increase or decrease in network traffic abnormal proportion of specific protocol packets	Traffic Monitoring Statistical Analysis
2	Behavior Sequence Anomaly	Frequent login failures multiple attempts to access specific ports in a short period	Sequence Analysis Pattern Matching
3	Association Pattern Anomaly	Similar attacks from multiple source addresses to the same target address identical abnormal behavior across different devices	Association Rule Mining Clustering Analysis

As can be seen from Table 3, the common detection anomaly patterns include traffic feature anomaly [44], behavior sequence anomaly [45], association pattern anomaly [46], etc., which are represented and analyzed as follows:(1) Traffic feature anomaly pattern. A sudden increase or decrease in network traffic may be a sign of intrusion behaviors such as network scanning and DDoS attacks. A large number of connection requests from different source IP addresses may indicate an ongoing DDoS attack [47]. In addition, anomalies in the percentage of protocol-specific packets may also suggest potential threats, e.g., an abnormal increase in TCP connections may be associated with port scanning activities [48]. (2) Behavioral sequence anomalies. In a normal network environment, the behavior of users and systems usually follows a certain pattern and sequence. Behavioral sequence anomalies such as frequent login failures and multiple attempts to access specific ports within a short period of time may be indications of brute-force password cracking or unauthorized access attempts [49]. A user entering an incorrect password several times in a row within a short period of time may indicate that his account is under attack [50]. (3) Anomalous association patterns. Association pattern anomalies such as multiple source addresses launching similar attacks on the same target address over a short period of time, and the same sequence of anomalous behaviors on different devices, may indicate the presence of a coordinated attack or malware propagation [51]. Multiple devices all showing scanning behavior on specific ports within a short period of time may suggest that these devices are controlled by the same attacker and are performing a coordinated attack [52].

Network Intrusion Detection Models Based on Data-Driven Algorithms

Supervised learning-based network intrusion detection methods

Supervised learning is able to construct models that classify or predict new data by using labeled historical data for training, which makes it effective in the field of network intrusion detection to identify known types of network attacks [53]. A variety of supervised learning algorithms are commonly used in network intrusion detection tasks today with significant results.

Traditional machine learning algorithms in network intrusion detection

Traditional machine learning algorithms applied to network intrusion detection problems include decision trees [54], plain Bayes [55], support vector machines (SVM) [56], etc., and the comparative analysis is shown in Table 4.

Table 4. Comparison of traditional machine learning algorithms

Algorithm	Advantages	Disadvantages	Training Time
Decision Tree	Strong interpretability	Prone to overfitting	Short
Naive Bayes	Low computational resource consumption	Limited detection accuracy	Short
Support Vector Machine	Strong ability to process high-dimensional data	Time-consuming sensitive to parameters	Long

The decision tree algorithm, which is notable for its strong interpretability, constructs a tree structure to classify network traffic through feature selection. Feature selection methods such as information gain and Gini index can effectively identify features that are important for classification, and then construct an efficient classification model [54]. The tree structure of the decision tree model clearly shows the classification rules, and administrators can intuitively understand how the model classifies and makes decisions about network traffic [57]. However, decision tree algorithms are prone to overfitting problems on large-scale datasets [58]. Large-scale datasets often contain complex feature relationships and noise, which can lead to overly complex decision tree models that fit too closely to the training data and thus become less generalizable on new data. In addition,

the detection speed of decision trees is relatively slow, especially when dealing with high-dimensional data, and the process of feature selection and tree construction consumes more computational resources and time [59].

The plain Bayesian algorithm is based on Bayes' theorem, which assumes that features are independent of each other. It utilizes Bayes' theorem to predict the category of a new sample by calculating the probability distribution of each feature under different categories [55]. However, the feature independence assumption of the plain Bayesian algorithm is often difficult to fulfill in real network data. In network traffic data, there is usually some correlation between different features, and port number and protocol type may jointly affect the nature of network traffic [60]. This feature correlation reduces the detection accuracy of the plain Bayesian algorithm, limiting its performance in complex real-world data [61].

Support Vector Machines (SVMs) achieve differentiation between different classes of data by finding the optimal classification hyperplane [56]. The SVM algorithm has a significant advantage in dealing with high-dimensional data, and is especially suitable for feature-rich datasets in network intrusion detection. It can effectively utilize the kernel function trick to map non-linearly differentiable data to a high-dimensional space, making it linearly differentiable in the high-dimensional space. However, the SVM algorithm has a long training time on large-scale datasets [62]. This is because the SVM algorithm needs to solve a quadratic programming problem to determine the optimal classification hyperplane, and the difficulty of solving this problem increases accordingly as the data size increases [63]. In addition, the SVM algorithm is more sensitive to parameter selection, and different kernel functions, regularization parameters, etc. can significantly affect the performance of the model [64].

Deep learning algorithms in network intrusion detection

Deep learning algorithms applied in network intrusion detection problems include convolutional neural network (CNN) algorithm [65], plain Bayes [66], support vector machine (SVM) [67], etc., and the comparative analysis is shown in Table 5.

Table 5. Comparison of deep learning algorithms

Algorithm	Advantages	Disadvantages	Applicable Scenarios
Convolutional Neural Network	Strong ability to automatically extract spatial features	High model complexity	Network traffic data visualized as images
Recurrent Neural Network	Able to process sequential data and capture temporal dependencies	Complex training process sensitive to hyperparameters	Network data with significant time-series features

Convolutional neural network (CNN) algorithm can automatically extract spatial features in network data, and its classification accuracy can reach about 92% for network traffic data that has been imaged [68-69]. The CNN algorithm progressively extracts features in the data through the combination of convolutional, pooling, and fully connected layers [68]. For the matrix of network traffic data pictorialization, CNN can identify specific patterns and features in it, such as sudden traffic peaks and other features in DDoS attacks, so as to achieve effective identification of attacks [70]. However, the model structure of CNN algorithm is complex, and the training process requires a large amount of computational resources and time support. Large-scale training of network traffic data consumes a lot of computational power and the training time is long.

Recurrent neural network (RNN) and its variants (LSTM, GRU) algorithms are able to efficiently process sequential data and capture temporal dependencies in network intrusion detection [71]. The LSTM algorithm performs well in dealing with intrusion detection data with time-series characteristics, and its detection accuracy can reach 91% for attacks with obvious temporal sequences such as port scanning [72]. The RNN algorithm enables the network to memorize and utilize the historical information in the sequence data through a cyclic structure, and LSTM and GRU, as improved variants of RNN, can better solve the gradient vanishing problem, thus capturing long-term dependencies more effectively [73]. When detecting time-series attacks in a network, the LSTM algorithm can memorize the network traffic characteristics of the previous time step, thus better determining whether the current traffic is an attack. However, the training process of RNN and its variants is relatively complex and sensitive to the choice of hyperparameters. The unreasonable setting of hyperparameters may lead to problems such as poor model training effect or slow convergence of the training

process [74]. Meanwhile, due to its complex model structure, it requires a large amount of data and computational resources to support the training and inference process, which limits its application in resource-constrained environments to some extent [75].

Although supervised learning methods can accurately identify known attack types in network intrusion detection, most of the traditional machine learning algorithms rely on manual feature extraction, which limits their generalization ability in the face of complex and variable network data. Although deep learning algorithms have strong automatic feature extraction capability, they have high model complexity, high consumption of training resources, poor interpretability, and performance bottlenecks in detecting new unknown attacks.

Network Intrusion Detection Method Based on Unsupervised Learning

Unsupervised learning does not need to rely on labeled data, and is able to automatically identify anomalies and clusters in network traffic based on the intrinsic structure and distribution characteristics of the data, which enables it to show unique advantages in the field of network intrusion detection in the face of unknown attack detection, zero-day attack discovery, and the utilization of unlabeled data, which effectively compensates for the shortcomings of supervised learning methods, and has become one of the key directions of the network intrusion detection research.

Clustering algorithms are widely used in network intrusion detection.K-Means algorithm with its simple and efficient characteristics, can quickly cluster the data, sensitive to the initial center point, different initial centers may lead to a large difference in the clustering results, and its contour coefficient is usually around 0.4 when dealing with network data, and the clustering effect needs to be improved [76]; DBSCAN algorithm is good at identifying clusters of arbitrary shapes in dealing with data sets with obvious density differences, and can effectively identify attacks with specific density distribution such as intranet penetration, but it is less efficient in processing high-dimensional data and large-scale data [77].

Generative models have received increasing attention in recent years. Generative Adversarial Networks (GANs) and their variants are trained through the confrontation of generators and discriminators, which generate realistic network traffic data, while the discriminators are used to differentiate between real and generated data, thus realizing the learning of normal data distribution and anomaly detection, and are able to achieve a detection accuracy of about 88% on unlabeled data, although their training process is unstable and prone to pattern collapse problems [78,79]; Variable Auto-Encoder (VAE) maps the data to the latent space through an encoder, and then the decoder reconstructs the data and uses the reconstruction error to identify anomalies, which has limitations in the reconstruction error assessment when dealing with high-dimensional network data, and is not accurate enough in capturing the features of complex network attacks [80].

Unsupervised learning methods get rid of the dependence on labeled data, can autonomously discover hidden patterns and unknown attack types in data, have strong generalization ability and adaptability, and provide new perspectives and solutions for network intrusion detection [81]. However, the unsupervised learning algorithm still has a certain gap in detection accuracy and stability compared with the supervised learning method, and its performance is greatly affected by the characteristics of data distribution, and its ability to detect multiple types of attacks in complex network environments needs to be further improved [82].

Problems

The field of network intrusion detection still faces many challenges, including problems of data quality, contradiction between model complexity and computational efficiency, poor model interpretability, inflexible model updating mechanism, privacy and security, and limitation of system resources. These issues limit the effective application and further development of the technology: 1) data quality issues are a key challenge in network intrusion detection, network traffic data is usually of high dimensionality, large scale and complexity, and there are noise and missing values, these data quality issues directly affect the training effect of the model and the detection performance; 2) the contradiction between the model complexity and the computational efficiency is especially prominent in the deep learning model, the The complex model structure requires a large amount of computational resources and time for training, and it is difficult to meet the demand for real-time

detection. 3) The poor interpretability of the model makes it difficult for security experts and system administrators to understand the basis of the detection results, which reduces the degree of trust in the model. 4) The dynamics and variability of cyber-attacks require that the model be able to quickly adapt to the new attack patterns, and the updating mechanism of the existing model is not flexible enough to respond to the emergence of new types of attacks in a timely manner. 5) The model can be updated to meet the demands of the new attack patterns. Existing model update mechanism is often not flexible enough to respond to the emergence of new types of attacks in a timely manner; 5) privacy and security issues should not be ignored, the network intrusion detection system handles a large amount of data containing sensitive user information, once leaked may lead to serious consequences; 6) the limitations of the system resources also limit the complexity and performance of the model, affecting the detection accuracy and real-time performance.

Conclusion

Data-driven algorithms show great potential and application prospects in the field of network intrusion detection. Supervised learning methods can effectively identify known types of network attacks, while unsupervised learning methods have unique advantages in unknown attack detection and zero-day attack discovery. However, current techniques still face challenges in various aspects such as data quality, model complexity, interpretability, attack dynamics, privacy and security.

Future research should focus on the following directions: first, improve data preprocessing and feature engineering techniques to improve data quality and model training efficiency; second, develop efficient model optimization algorithms to reduce computational complexity and improve the real-time performance of the model; third, improve the interpretability of the model to enhance users' trust in the model and promote its wide application; in addition, build adaptive and online learning models to quickly respond to new attack patterns; at the same time, strengthening privacy protection and model security research to ensure data privacy and system reliability; and finally, exploring the integration with other technologies (e.g., SDN, NFV, and blockchain) to achieve a more comprehensive network security solution.

Through in-depth exploration and technological innovation in these research directions, it is expected to further enhance the performance and reliability of the network intrusion detection system, provide a more solid guarantee for cybersecurity, and contribute to the security and stability of cyberspace.

References

[1] Gondhalekar R , Chattamvelli R .A Comprehensive Review of Dimensionality Reduction Techniques for Real-time Network Intrusion Detection with Applications in Cybersecurity[J].Defence science journal, 2024(2):74.

[2] Wang L , Xu J , Jia L ,et al.Multi-strategy RIME optimization algorithm for feature selection of network intrusion detection[J].Computers & Security, 2025, 153.DOI:10.1016/j.cose.2025.104393.

[3] Huan S , Zhang X , Shang W ,et al.T-Shaped CAN Feature Integration With Lightweight Deep Learning Model for In-Vehicle Network Intrusion Detection[J].IEEE transactions on intelligent transportation systems, 2024(12):25.DOI:10.1109/TITS.2024.3478371.

[4] Wang Y , Liu Z , Zheng W ,et al.A Combined Multi-Classification Network Intrusion Detection System Based on Feature Selection and Neural Network Improvement[J].Applied Sciences-Basel, 2023, 13(14):16.DOI:10.3390/app13148307.

[5] Azizan A H , Mostafa S A , Mustapha A ,et al.A Machine Learning Approach for Improving the Performance of Network Intrusion Detection Systems[J].Annals of Emerging Technologies in Computing, 2021, 5(5):201-208.DOI:10.33166/AETiC.2021.05.025.

[6] Maseer Z K , Yusof R , Mostafa S A ,et al.DeepIoT.IDS:Hybrid Deep Learning for Enhancing IoT Network Intrusion Detection[J]. Computers, Materials, and Continues (in English), 2021(12):22.

[7] Haugerud H , Tran H N , Aitsaadi N ,et al.A dynamic and scalable parallel Network Intrusion Detection System using intelligent rule ordering and Network Function Virtualization[J].Future Generation Computer Systems, 2021, 124(4).DOI:10.1016/j.future.2021.05.037.

[8] Maithem M , Al-Sultany G A .Network intrusion detection system using deep neural networks[J].Journal of Physics: Conference Series, 2021, 1804(1):012138 (11pp).DOI:10.1088/1742-6596/1804/1/012138.

[9] Ponnuviji N P , Nirmala E , Mary H F F ,et al.ALRN-RCS: Advanced Approach to Network Intrusion Detection Using Attention Long-Term Recurrent Networks and Chaotic Optimization[J].IETE journal of research, 2024(11):70.

[10] Doriguzzi-Corin R , Knob L A D , Savi S M .Introducing packet-level analysis in programmable data planes to advance Network Intrusion Detection[J].Computer networks, 2024, 239(Feb.):110162.1-110162.14.DOI:10.1016/j.comnet.2023.110162.

[11] Kumar N , Kumar U .Artificial intelligence for classification and regression tree based feature selection method for network intrusion detection system in various telecommunication technologies[J].Computational intelligence, 2024, 40(1):e12500.1-e12500.23.DOI:10.1111/coin.12500.

[12] Liu J , Guo M .DIGNN-A: Real-Time Network Intrusion Detection with Integrated Neural Networks Based on Dynamic Graph[J].Computers, Materials & Continua, 2025, 82(1).DOI:10.32604/cmc.2024.057660.

[13] Fan S .Network Intrusion Detection Based on Deep Belief Network Broad Equalization Learning System[J].Electronics, 2024, 13.DOI:10.3390/electronics13153014.

[14] Cerasuolo F , Bovenzi G , Ciuonzo D ,et al.Attack-adaptive network intrusion detection systems for IoT networks through class incremental learning[J].Computer Networks, 2025, 263.DOI:10.1016/j.comnet.2025.111228.

[15] Kalidindi A , Koti B R , Srilakshmi C ,et al.Advanced Machine Learning Techniques for Enhancing Network Intrusion Detection and Classification Using DarkNet CIC2020[J].International Journal of Online & Biomedical Engineering, 2024, 20(15).DOI:10.3991/ijoe.v20i15.50873.

[16] Chavan V D , Kaladeep Yalagi P C .Network Intrusion Detection System Using Reptile Search with Whale Optimization Algorithm and Multi Head Attention Long Short Term-Memory in IoT[J].International Journal of Intelligent Engineering & Systems, 2025, 18(1).DOI:10.22266/ijies2025.0229.14.

[17] Shebl A , Elsedimy E I , Ismail A ,et al.DCNN: a novel binary and multi-class network intrusion detection model via deep convolutional neural network[J].EURASIP Journal on Information Security, 2024, 2024(1).DOI:10.1186/s13635-024-00184-1.

[18] Taotao L , Yu F U , Kun W ,et al.Network intrusion detection method based on VAE-CWGAN and fusion of statistical importance of feature[J].Journal on Communication / Tongxin Xuebao, 2024, 45(2).DOI:10.11959/j.issn.1000-436x.2024013.

[19] Ghadermazi J , Hore S , Shah A ,et al.GTAE-IDS: Graph Transformer-Based Autoencoder Framework for Real-Time Network Intrusion Detection[J].IEEE Transactions on Information Forensics and Security, 2025.DOI:10.1109/TIFS.2025.3557741.

[20] Al-Absi G A , Fang Y , Qaseem A A .STC-GraphFormer: Graph spatial-temporal correlation transformer for in-vehicle network intrusion detection system[J].Vehicular Communications, 2025(Feb.):51.DOI:10.1016/j.vehcom.2024.100865.

[21] He J , Li X , Zhang X ,et al.A Synthetic Data-Assisted Satellite Terrestrial Integrated Network Intrusion Detection Framework[J].IEEE Transactions on Information Forensics and Security, 2025.DOI:10.1109/TIFS.2025.3530676.

[22] Devaraju S , Soni D , Jawahar S ,et al.Performance Exploration of Network Intrusion Detection System with Neural Network Classifier on The KDD Dataset[J].International Journal of Safety & Security Engineering, 2024, 14(5).DOI:10.18280/ijsse.140510.

[23] Lin Z Z , Pike T D , Bailey M M ,et al.A Hypergraph-Based Machine Learning Ensemble Network Intrusion Detection System[J].IEEE transactions on systems, man, and cybernetics. Systems, 2024(11 Pt.2):54.

[24] Ren K , Yuan S , Zhang C ,et al.CANET: A hierarchical CNN-Attention model for Network Intrusion Detection[J].Comput. Commun. 2023, 205:170-181.DOI:10.2139/ssrn.4243555.

[25] Abodayeh K , Raza A , Rafiq M ,et al.Development of PCCNN-Based Network Intrusion Detection System for EDGE Computing[J].Computers, Materials & Continua, 2022.DOI:10.32604/cmc.2022.018708.

[26] Harazeem A O , Ait T T , Kayode S Y ,et al.XIDINTFL-VAE: XGBoost-based intrusion detection of imbalance network traffic via class-wise focal loss variational autoencoder[J].The Journal of Supercomputing, 2024.

[27] Sushma E A T .A Review of the cluster based Mobile Adhoc Network Intrusion Detection System[J].Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021, 12(2):2070-2076.DOI:10.17762/turcomat.v12i2.1811.

[28] Khurana J , Aggarwal V , Singh H .A Comparative Study of Deep Learning Models for Network Intrusion Detection[J].International Journal of Computer Applications, 2021, 174:38-46.DOI:10.5120/IJCA2021921135.

[29] R. R , M. P. A .Network Intrusion Detection Using Feature Selection Techniques: Bacterial Forage Optimization Algorithm[J].International Journal of Intelligent Engineering & Systems, 2024, 17(5).DOI:10.22266/ijies2024.1031.48.

[30] Xu C , Zhan Y , Chen G ,et al.Elevated few-shot network intrusion detection via self-attention mechanisms and iterative refinement[J].PLOS ONE, 2025, 20(1).DOI:10.1371/journal.pone.0317713.

[31] Ortega-Fernandez I , Sestelo M , Burguillo J C ,et al.Network intrusion detection system for DDoS attacks in ICS using deep autoencoders[J].Wireless Networks (10220038), 2024, 30(6).DOI:10.1007/s11276-022-03214-3.

[32] Zha C , Wang Z , Fan Y ,et al.A-NIDS: Adaptive Network Intrusion Detection System Based on Clustering and Stacked CTGAN[J].IEEE transactions on information forensics and security, 2025:20.DOI:10.1109/TIFS.2025.3551643.

[33] Mills G A , Acquah D K , Sowah R A ,et al.Network Intrusion Detection and Prevention System Using Hybrid Machine Learning with Supervised Ensemble Stacking Model[J].Journal of Computer Networks & Communications, 2024, 2024.DOI:10.1155/2024/5775671.

[34] Wu H .Feature-Weighted Naive Bayesian Classifier for Wireless Network Intrusion Detection[J].Security & Communication Networks, 2024.DOI:10.1155/2024/7065482.

[35] Mohy-Eddine M , Guezzaz A , Benkirane S ,et al.An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection[J].Multimedia tools and applications, 2023.DOI:10.1007/s11042-023-14795-2.

[36] Nayak N K S , Bhattacharyya B .MAC Protocol Based IoT Network Intrusion Detection Using Improved Efficient Shuffle Bidirectional COOT Channel Attention Network[J].IEEE Access, 2023, 11:77385-77402.DOI:10.1109/ACCESS.2023.3299031.

[37] Security A C N .Retracted: Design of Network Intrusion Detection Model Based on TCA[J].Security & Communication Networks, 2023.DOI:10.1155/2023/9827541.

[38] Ibaisi T A , Kuhn S , Kaiiali M ,et al.Network Intrusion Detection Based on Amino Acid Sequence Structure Using Machine Learning[J].Electronics, 2023, 12(20):25.DOI:10.3390/electronics12204294.

[39] Manjunath H , Kumar S .Network Intrusion Detection System using Convolution Recurrent Neural Networks and NSL-KDD Dataset[J].Fusion: Practice & Applications, 2023, 13(1).DOI:10.54216/FPA.130109.

[40] Li J , Zhang H , Liu Z ,et al.Network intrusion detection via tri-broad learning system based on spatial-temporal granularity[J].The Journal of Supercomputing, 2023, 79(8):9180-9205.DOI:10.1007/s11227-022-05025-x.

[41] Jmila H , Ibn Khedher M .Adversarial machine learning for network intrusion detection: A comparative study[J].Computer networks, 2022.DOI:10.1016/j.comnet.2022.109073.

[42] Lawrence H , Ezeobi U , Tauil O ,et al.CUPID: A labeled dataset with Pentesting for evaluation of network intrusion detection[J].Journal of systems architecture, 2022.DOI:10.1016/j.sysarc.2022.102621.

[43] Zexuan M A , Jin L I , Yanli L U ,et al.Network intrusion detection method based on WaveNet and BiGRU[J].Systems Engineering & Electronics, 2022, 44(8).DOI:10.12305/j.issn.1001-506X.2022.08.31.

[44] Siddiqi M A , Pak W .An Optimized and Hybrid Framework for Image Processing Based Network Intrusion Detection System[J].Computers, materials & continua, 2022, 73(2 Pt.3):3921-3949.DOI:10.32604/cmc.2022.029541.

[45] Dao T N , Nguyen H , Vu V .A Network Intrusion Detection Architecture Based on Class Parallelism on Distributed Switches[J].2022 13th International Conference on Information and Communication Technology Convergence (ICTC), 2022:1284-1289.DOI:10.1109/ICTC55196.2022.9952903.

[46] Wen Q .Design of Network Intrusion Detection Model Based on TCA[J].Security & Communication Networks, 2022.DOI:10.1155/2022/9248853.

[47] Zhang C , Chen Y , Meng Y ,et al.A Novel Framework Design of Network Intrusion Detection Based on Machine Learning Techniques[J].Security and Communication Networks, 2021.DOI:10.1155/2021/6610675.

[48] Toldinas J , Venkauskas A , Damaeviius R ,et al.A Novel Approach for Network Intrusion Detection Using Multistage Deep Learning Image Recognition[J].Electronics, 2021, 10(15):1854.DOI:10.3390/electronics10151854.

[49] Uhm Y , Pak W .Service-Aware Two-Level Partitioning for Machine Learning-based Network Intrusion Detection with High Performance and High Scalability[J].IEEE Access, 2021, PP(99):1-1.DOI:10.1109/ACCESS.2020.3048900.

[50] Singh N B , Singh M M , Sarkar A ,et al.A novel wide & deep transfer learning stacked GRU framework for network intrusion detection[J].Journal of information security and applications, 2021(Sep.):61.DOI:10.1016/j.jisa.2021.102899.

[51] Deng H , Yang T .Network Intrusion Detection Based on Sparse Autoencoder and IGA-BP Network[J].Wireless Communications and Mobile Computing, 2021.DOI:10.1155/2021/9510858.

[52] Tang Y , Li C .An Online Network Intrusion Detection Model Based on Improved Regularized Extreme Learning Machine[J].IEEE Access, 2021, PP(99):1-1.DOI:10.1109/ACCESS.2021.3093313.

[53] Sarhan M , Layeghy S , Portmann M .Towards a Standard Feature Set for Network Intrusion Detection System Datasets[J].Mobile Networks and Applications, 2021, 27:357-370.DOI:10.1007/s11036-021-01843-0.

[54] Wang Z , Li Z , Wang J ,et al.Network Intrusion Detection Model Based on Improved BYOL Self-Supervised Learning[J].Security & Communication Networks, 2021.DOI:10.1155/2021/9486949.

[55] Aliyu I , Feliciano M C , Engelenburg S V ,et al.Blockchain-based Federated Forest for SDN-enable In-vehicle Network Intrusion Detection System[J].IEEE Access, 2021, PP(99):1-

[56] Seniaray S , Jindal R .Machine Learning-Based Network Intrusion Detection System[J].Computer Networks and Inventive Communication Technologies, 2021.DOI:10.1007/978-981-16-3728-5_13.

[57] Jeune L L , Goedeme T , Mentens N .Machine Learning for Misuse-Based Network Intrusion Detection: Overview, Unified Evaluation and Feature Choice Comparison Framework[J].IEEE Access, 2021, 9:63995-64015.DOI:10.1109/ACCESS.2021.3075066.

[58] Siddiqi M , Pak W .An Agile Approach to Identify Single and Hybrid Normalization For Enhancing Machine Learning Based Network Intrusion Detection[J].IEEE Access, 2021.DOI:10.1109/ACCESS.2021.3118361.

[59] Bertoli G D C , Pereira L A , Saotome O ,et al.An end-to-end framework for machine learning-based network intrusion detection system[J].IEEE Access, 2021, PP(99):1-1.DOI:10.1109/ACCESS.2021.3101188.

[60] Dao T N , Lee H J .Stacked Autoencoder-based Probabilistic Feature Extraction for On-Device Network Intrusion Detection[J].IEEE Internet of Things Journal, 2021, PP(99):1-1.DOI:10.1109/JIOT.2021.3078292.

[61] Andresini A M D .Autoencoder-based deep metric learning for network intrusion detection[J].Information Sciences: An International Journal, 2021, 569(1).DOI:10.1016/j.ins.2021.05.016.

[62] Qi G , Chen Z , Zhao H ,et al.Construction and Application of Machine Learning Model in Network Intrusion Detection[J].Journal of Physics: Conference Series, 2021, 1883(1):012001 (7pp).DOI:10.1088/1742-6596/1883/1/012001.

[63] Rajagopal S , Kundapur P P , Hareesha K S .Towards Effective Network Intrusion Detection: From Concept to Creation on Azure Cloud[J].IEEE Access, 2021, PP(99):1-1.DOI:10.1109/ACCESS.2021.3054688.

[64] Zou S , Zhong F , Han B ,et al.Network intrusion detection method based on deep learning[J].Journal of Physics: Conference Series, 2021, 1966(1):012051 (5pp).DOI:10.1088/1742-6596/1966/1/012051.

[65] Sithungu S , Ehlers E M .GAAINet: A Generative Adversarial Artificial Immune Network Model for Intrusion Detection in Industrial IoT Systems[J].Journal of Advances in Information Technology, 2022.DOI:10.12720/jait.13.5.456-461.

[66] Keller J .Deep Learning for Network Intrusion Detection in Virtual Networks[J].Electronics, 2024, 13.DOI:10.3390/electronics13183617.

[67] Kumar V , Kumar K , Singh M ,et al.NIDS-DA: Detecting functionally preserved adversarial examples for

[68] Kim H Y .Making a Real-Time IoT Network Intrusion-Detection System (INIDS) Using a Realistic BoT–IoT Dataset with Multiple Machine-Learning Classifiers[J].Applied Sciences, 2025, 15.DOI:10.3390/app15042043.

[69] Hassen S I , Abdlrazaq A A .Contextual Deep Semantic Feature Driven Multi-Types Network Intrusion Detection System for IoT-Edge Networks[J].ZANCO Journal of Pure & Applied Sciences, 2024, 36(6).DOI:10.21271/ZJPAS.36.6.14.

[70] Chuang P J , Huang P Y .Enhancing network intrusion detection by employing Mondrian forests to achieve multiple attack classification[J].The Journal of Supercomputing, 2025, 81(4):1-24.DOI:10.1007/s11227-025-07123-y.

[71] Mahdi W G , Hammood D A , Abed L H ,et al.NIDS-ML-PSO: Network Intrusion Detection System based on Machine Learning Classifiers and Particle Swarm Optimization[J].Journal of Qadisiyah Computer Science

[72] Qiu L , Xu Z , Lin L ,et al.Design and Optimization of Hybrid CNN-DT Model-Based Network Intrusion Detection Algorithm Using Deep Reinforcement Learning[J].Mathematics (2227-7390), 2025, 13(9).DOI:10.3390/math13091459.

[73] Kumar V , Kumar K , Singh M .Generating practical adversarial examples against learning-based network intrusion detection systems[J].Annals of telecommunications, 2025(3/4):80.DOI:10.1007/s12243-024-01021-9.

[74] Daniel N , Kaiser F K , Giladi S ,et al.Labeling Network Intrusion Detection System (NIDS) Rules with MITRE ATT&CK Techniques: Machine Learning vs. Large Language Models[J].Big Data & Cognitive Computing, 2025, 9(2).DOI:10.3390/bdcc9020023.

[75] Aceto G , Giampaolo F , Guida C ,et al.Synthetic and privacy-preserving traffic trace generation using generative AI models for training Network Intrusion Detection Systems[J].Journal of Network and Computer Applications, 2024, 229.DOI:10.1016/j.jnca.2024.103926.

[76] Gondhalekar R , Chattamvelli R .A Comprehensive Review of Dimensionality Reduction Techniques for Real-time Network Intrusion Detection with Applications in Cybersecurity[J].Defence Science Journal, 2024, 74(2).DOI:10.14429/dsj.74.18953.

[77] Puzis R .Labeling Network Intrusion Detection System (NIDS) Rules with MITRE ATT&CK Techniques: Machine Learning vs. Large Language Models[J].Big Data and Cognitive Computing, 2025, 9.DOI:10.3390/bdcc9020023.

[78] Luo Y , Chen R , Li C ,et al.An Improved Binary Simulated Annealing Algorithm and TPE-FL-LightGBM for Fast Network Intrusion Detection[J].Electronics (2079-9292), 2025, 14(2).DOI:10.3390/electronics14020231.

[79] Walling S , Lodh S .An Extensive Review of Machine Learning and Deep Learning Techniques on Network Intrusion Detection for IoT[J].Transactions on Emerging Telecommunications Technologies, 2025(2):36.DOI:10.1002/ett.70064.

[80] Yao W , Hu L , Hou Y .A Distributed Parallel Network Intrusion Detection System Based on Ray Framework With GPU Acceleration[J].Concurrency & Computation: Practice & Experience, 2025, 37.DOI:10.1002/cpe.70021.

[81] Turukmane A V , Devendiran R .M-MultiSVM: An efficient feature selection assisted network intrusion detection system using machine learning[J].Computers & Security, 2024, 137(000):14.DOI:10.1016/j.cose.2023.103587.

[82] Firat M , Bakal G , Akba A .Machine Learning Based Network Intrusion Detection with Hybrid Frequent Item Set Mining[J].Journal of Polytechnic, 2024, 27(5).

[83] Kolukisa B , Dedeturk B K , Hacilar H ,et al.An efficient network intrusion detection approach based on logistic regression model and parallel artificial bee colony algorithm[J].Computer Standards & Interfaces, 2024, 89(000):9.DOI:10.1016/j.csi.2023.103808.

[84] Sajith P J , Nagarajan G .Retraction Note: Network intrusion detection system using ANFIS classifier[J].Soft Computing - A Fusion of Foundations, Methodologies & Applications, 2024, 28.DOI:10.1007/s00500-024-09974-8.

[85] Chen Z , Zou H , Hu T ,et al.HC-NIDS: Historical contextual information based network intrusion detection system in Internet of Things[J].Computers & Security, 2025, 152.DOI:10.1016/j.cose.2025.104367.