Hindawi
Journal of Engineering
Volume 2024, Article ID 3909173, 16 pages
https://doi.org/10.1155/2024/3909173

*Review Article*

# A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis

**Salman Muneer,[1,2] Umer Farooq,[3] Atifa Athar,[4] Muhammad Ahsan Raza,[5] Taher M. Ghazal,[6,7] and Shadman Sakib[8]**

[1]*National College of Business Administration and Economics, Lahore, Pakistan*
[2]*Department of Computer Science, UCP, Lahore, Pakistan*
[3]*Department of Computer Science, Lahore Garrison University, Lahore 54000, Pakistan*
[4]*Department of Computer Science, CUI Lahore Campus, Lahore, Pakistan*
[5]*Department of Information Sciences, University of Education, Multan Campus, Lahore 60000, Pakistan*
[6]*Centre for Cyber Physical Systems, Computer Science Department, Khalifa University, Abu Dhabi, UAE*
[7]*Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi 43600, Selangor, Malaysia*
[8]*Department of Finance and Banking, Jahangirnagar University, Dhaka, Bangladesh*

Correspondence should be addressed to Shadman Sakib; shadman.stu2014@juniv.edu

Received 17 August 2023; Revised 30 November 2023; Accepted 29 January 2024; Published 15 April 2024

Academic Editor: A. S. Madhukumar



Intrusion detection (ID) is critical in securing computer networks against various malicious attacks. Recent advancements in machine learning (ML), deep learning (DL), federated learning (FL), and explainable artificial intelligence (XAI) have drawn significant attention as potential approaches for ID. DL-based approaches have shown impressive performance in ID by automatically learning relevant features from data but require significant labelled data and computational resources to train complex models. ML-based approaches require fewer computational resources and labelled data, but their ability to generalize to unseen data is limited. FL is a relatively new approach that enables multiple entities to train a model collectively without exchanging their data, providing privacy and security benefits, making it an attractive option for ID. However, FL-based approaches require more communication resources and additional computation to aggregate models from different entities. XAI is critical for understanding how AI models make decisions, improving interpretability and transparency. While existing literature has explored the strengths and weaknesses of DL, ML, FL, and XAI-based approaches for ID, a significant gap exists in providing a comprehensive analysis of the specific use cases and scenarios where each approach is most suitable. This paper seeks to fill this void by delivering an in-depth review that not only highlights strengths and weaknesses but also offers guidance for selecting the appropriate approach based on the unique ID context and available resources. The selection of an appropriate approach depends on the specific use case, and this work provides insights into which method is best suited for various network sizes, data availability, privacy, and security concerns, thus aiding practitioners in making informed decisions for their ID needs.

## 1. Introduction

Intrusion detection is monitoring a computer system or network for malicious activity, such as unauthorized access, misuse, or modification of system resources. ID aims to detect such action in real-time or near real-time and take suitable action to protect against further loss or data forfeiture.

Intrusion detection systems (IDS) are designed to analyze system and network activity to identify suspicious patterns that may indicate an attack is underway. These systems can be host- or network-based and may use

approaches like signature-based identification, anomaly-based identification, or behaviour-based detection to recognize potential risks. Once an intrusion is detected, the IDS can alert or notify security personnel or automated response mechanisms, such as firewalls or other security systems, to take appropriate action to contain or mitigate the attack. ID is an essential part of a comprehensive security method and may assist organizations to detect and respond to security incidents promptly and efficiently. ID is a significant aspect of cybersecurity that can be solved with the help of technology [1, 2].

Integrating technology and the Internet into all aspects of life has revolutionized how people live and work. It has created new opportunities for remote work, online learning, and seamless communication. However, with the convenience of technology comes the risk of security threats, such as hacking, cyberattacks, and data breaches. It is crucial to protect personal and sensitive information and stay safe online. This includes being cautious of phishing scams, using strong passwords, and keeping software up-to-date. Regular education on cyber security risks and best practices is also essential. Identifying and detecting network threats and cyber-attacks is crucial in preventing them. This involves staying informed about the latest security risks and being vigilant for signs of suspicious activity. Some common indicators of a cyber-attack include unusual pop-ups or error messages, slow efficiency of the computer or network, unusual network traffic, unauthorized changes to files or settings, and suspicious emails or attachments [3, 4].

Regular security assessments and testing can also help identify vulnerabilities in your network before attackers exploit them. Cyber security protects sensitive information from being stolen, altered, or misused. Common threats include phishing scams, malware, ransomware, and hacking. Individuals and organizations should regularly update their software, use strong passwords, and educate themselves about the latest security risks to stay safe online. Implementing multi-factor authentication, firewalls, and regularly backing up data can also help prevent cyber-attacks [5].

IDS is an essential section of a comprehensive security resolution as it helps to identify security threats in real time and respond to them quickly. It can be either network-based or host-based, depending on where it is deployed in the network. Network-based IDS (NIDS) monitors network traffic for signs of intrusion and operates at the network layer. Host-based IDS (HID) is installed on individual hosts and monitors events on that specific host for signs of intrusion. IDS can operate in two modes: signature-based detection, which uses pre-defined rules to identify known threats, and anomaly-based detection, which uses ML algorithms to identify deviations from normal network behaviour and potential flag intrusions [6].

Attention has been given to addressing issues in the cyber-attack field, specifically IDSs, in the last few decades [3]. It mentions that various ML algorithms have addressed these issues, including decision tree algorithms [5, 7], support vector machine models, k-means, k-nearest neighbour, artificial intelligence approaches, and many others [4, 6, 8, 9]. However, deep neural network solutions have recently gained popularity in this field, including convolutional neural network (CNN), recurrent neural network (RNN), restricted Boltzmann machine (RBM), message-passing neural networks (MPNN), and others [10–14]. These DL models are being applied to IDS in fog, cloud, and IoT-based systems [15] to improve their accuracy and efficiency [16–19].

The modelling of IDSs as a feature selection problem and using traditional classifiers to address it. It also mentions using meta-heuristic (MH) optimization algorithms to tackle complex optimization problems in IDSs. These MH algorithms include particle swarm optimization (PSO) [20], crow search algorithm (CSA) [21], genetic algorithm (GA), random harmony search algorithm, and grey wolf optimizer (GWO) algorithm [22–24]. These algorithms have been applied to enhance the privacy and efficacy of IDSs by optimizing the selection of features used to make predictions [25–27]. Indeed, developing an IDS is a difficult and thought-provoking task as it requires a deep understanding of both benign and malicious activity behaviour in a network environment. Lab-based testing of IDS models can provide valuable insights into the efficiency and accuracy of the model. Still, it can also lead to overfitting, where the model is too closely optimized to the laboratory data and may not perform well in real-world environments. Therefore, validating the IDS model in a real-world environment is critical to ensuring its effectiveness. This can be done by deploying the model in a live network and monitoring its efficiency over time. This will provide a more accurate representation of the actual network environment and help to identify any weaknesses or limitations in the model. Furthermore, ongoing testing and updating of the model is necessary to keep pace with changing security threats and evolving network behaviour. DL has found numerous applications in image classification, object detection, and segmentation and has enabled advancements in areas such as facial recognition and autonomous vehicles industries and fields, including the medical sector, computer vision, finance, marketing advertising, NLP, cybersecurity, and IDS [17, 19, 21].

Different CNN designs for application in IDS have been anticipated. The network model of these designs differs in terms of depth and breadth, kind of convolutional operation, number and size of filters, type and size of pooling, the number of fully associated layers, and the atmosphere in which they are applied. MobileNet, ResNet, NASNet, EfficientNet, MnasNet, and AlexNet are among the models described, all of which strive to improve the accuracy and efficiency of ID. These models were created based on research findings [22, 24].

This study describes a proposed novel IDS model that combines DL and meta-heuristic optimization techniques. The model starts with efficient and simple feature extraction in the CNN model. It uses quite a few convolution blocks to extract useful features and is only employed during the extraction of features. The raw data is transformed into lower-dimensional representations using relevant characteristics, which the CNN learns using simple structures and efficient training methods. The entirely coupled layer with CNN extracts key features and classifies the activity as

malicious or not. Integrating the strengths of DL and metaheuristic optimization methods, the proposed research work intends to enhance the accuracy and efficiency of IDSs [11, 14, 15].

Recently, machine learning and federated learning have played a vital role in IDS. ML refers to a subset of AI that allows computers to learn from information and enhance their performance without being explicitly programmed. In the context of ID, ML can be used to develop algorithms that automatically identify malicious activities and detect network intrusions. Machine learning techniques work by training models on large amounts of historical data and using these models to predict the likelihood of new events being benign or malicious. For example, a machine learning algorithm may learn to identify patterns of behavior that are indicative of an attacker attempting to exploit a vulnerability in a network. Once trained, the algorithm can be used to classify new data points and identify potential intrusions in real time.

Federated learning is a machine learning technique used in scenarios where data is distributed among multiple devices or organizations. In the context of ID, federated learning refers to a method where multiple devices or entities collaboratively train a machine learning model to detect and prevent network intrusions. Instead of centralizing all the data on a single server, federated learning distributes the model training process to multiple devices. Each device contributes its local data and trains a local model based on its data. The local models are then sent to a central server and combined into a global model. The central server aggregates the global model and sends it back to the devices for further training, and this process repeats iteratively.

Federated learning can be particularly useful in ID scenarios, where data privacy and security are crucial. By training the model locally, data is not sent to a central server, which can reduce the risk of data breaches and ensure data privacy. Moreover, by leveraging multiple devices and organizations data, federated learning can improve the accuracy of the ID model.

Intrusion detection systems are essential tools for detecting and preventing malicious activities in computer networks. Machine learning and federated learning [18] are two popular techniques widely used in IDS to improve their accuracy and efficiency. Machine learning algorithms can analyze large amounts of data and identify patterns and anomalies in network traffic to detect potential attacks. On the other hand, Federated learning allows multiple parties to collaborate on building a model without sharing their data, improving privacy and data security. Both techniques have their strengths and weaknesses, and their effectiveness in IDS depends on various factors such as the availability and quality of data, computational resources, and security concerns.

In the realm of securing computer networks, ID plays a pivotal role in protecting against a multitude of malicious attacks. In this ever-evolving landscape of network security, recent technological advancements have propelled machine learning (ML), deep learning (DL) [28–32], federated learning (FL), and explainable artificial intelligence (XAI) into the limelight as promising avenues for enhancing ID. These advancements represent a significant change in the way this work approaches network security, presenting both a wealth of opportunities and a set of challenges.

To navigate this intricate and dynamic terrain effectively, a set of fundamental research questions has emerged. These questions delve into specific facets of these cutting-edge approaches, with the aim of shedding light on their strengths, limitations, and the contexts in which they are most suited. The ultimate goal is to equip network practitioners with the knowledge and insights needed to make informed and strategic decisions as they work to fortify their systems against the ever-present threat of malicious intrusions. In the ongoing pursuit of a more secure digital world, these research questions serve as guiding beacons, illuminating the path toward effective and innovative ID.

RQ1: How can ID be effectively enhanced and secured against malicious attacks using modern technological advancements, including ML, (DL), FL, and XAI?

RQ2: What are the key strengths and limitations associated with DL-based approaches in ID, especially considering their need for labelled data and substantial computational resources for training complex models?

RQ3: In what ways do ML-based approaches for ID differ from DL-based methods in terms of their computational requirements and their ability to generalize to previously unseen data?

RQ4: How does Federated Learning (FL) address the need for privacy and security in ID, and what are the trade-offs in terms of communication resources and computational overhead when aggregating models from diverse entities?

RQ5: What is the role of explainable artificial intelligence (XAI) in enhancing interpretability and transparency in the context of ID?

RQ6: What are the gaps in the existing literature when it comes to a comprehensive analysis of the suitability of DL, ML, FL, and XAI-based approaches for specific use cases and scenarios in ID?

RQ7: How can practitioners determine the most appropriate approach for ID based on their network size, data availability, and privacy and security requirements?

The research questions presented in Tables 1–3 are preliminary to the field of ID. These questions explore cutting-edge technology applications, collectively advancing our understanding and capabilities in detecting and responding to network intrusions. Researchers use these questions to develop more effective and context-aware ID methods, ultimately enhancing network security.

## 2. Literature Review

Previously, multiple researchers have worked on IDS. Some of their works are highlighted in this section.

Table 1: Critical review of machine learning (ML) based approaches in ID.

| Ref | Authors | Year | Cited by | ML approach | Accuracy (%) |
|---|---|---|---|---|---|
| [33] | Ahmed et al. | 2022 | 14 | Random forest (RF) | 95.1 |
| [34] | Singh et al. | 2022 | 15 | Support vector Regression | 98 |
| [35] | Pranto et al. | 2022 | 9 | ML-based ensemble feature selection strategy | 99.5 |
| [36] | Raghuvanshi et al. | 2022 | 48 | SVM | 98 |
| [37] | Albulayhi et al. | 2022 | 28 | ML-based IDS | 99.98 |
| [38] | Asif et al. | 2021 | 79 | ML-based method tangled with the MapReduce-Based intelligent model for ID (MR-IMID) | 97.7 |
| [39] | Çavuşoğlu | 2019 | 112 | Hybrid and layered IDS | 99.7 |
| [40] | Alqahtani et al. | 2020 | 82 | RF | 94 |
| [41] | Liu and Lang | 2019 | 457 | KNN | 99 |
| [42] | Ren et al. | 2019 | 80 | IDS by using hybrid data optimization (DO-IDS) | 92.8 |
| [43] | Bindra and Sood | 2019 | 53 | RF | 96 |
| [44] | Sai Kiran et al. | 2020 | 43 | SVM | 98.95 |
| [45] | Saranya et al. | 2020 | 127 | RF | 99.81 |
| [46] | Logeswari et al. | 2023 | 5 | Hybrid feature selection (HFS-light GBM IDS) | 98.72 |
| [47] | Muhammad and Saleem | 2022 | 39 | Naïve Bayes | 98.6 |

Table 2: Critical review of deep learning based approaches in ID.

| Ref | Authors | Year | Cited by | DL approach | Accuracy (%) |
|---|---|---|---|---|---|
| [48] | Yin et al. | 2017 | 1323 | RNN-IDS | 97.09 |
| [49] | Vani | 2017 | 19 | LSTM based ensemble method | 92.3 |
| [50] | Wang et al. | 2017 | 428 | Hierarchical spatial-temporal features-based IDS (HAST-IDS) with CNN | 99.89 |
| [51] | Loukas et al. | 2017 | 211 | RNN | 86.9 |
| [52] | Shone et al. | 2018 | 1046 | NDAE | 97.85 |
| [53] | Lee et al. | 2018 | 51 | Autoencoder | 98.9 |
| [54] | Al-Qatf et al. | 2018 | 334 | Self-taught learning (STL)-IDS | 99.41 |
| [55] | Ding and Zhai | 2018 | 91 | CNN | 80.13 |
| [56] | Parampottupadam and Moldovann | 2018 | 27 | Deep learning H2O (binomial and multinomial models) | 99.98 |
| [57] | Xin et al. | 2018 | 756 | CNN | 99.41 |
| [58] | Faker and Dogdu | 2019 | 140 | DNN | 99.16 |
| [59] | Laqtib et al. | 2019 | 15 | CNN | 77 |
| [60] | Ge et al. | 2019 | 121 | FFNN | 82 |
| [61] | Khan et al. | 2019 | 237 | Two-stage deep learning (TSDL) model | 99.31 |
| [62] | Gurung et al. | 2019 | 80 | Auto-encoders | 87.2 |
| [63] | Su et al. | 2020 | 153 | BAT model | 84.25 |
| [64] | Gamage and Samarabandu | 2020 | 156 | ANN | 98.25 |
| [65] | Boukhalfa et al. | 2020 | 30 | LSTM | 99.93 |
| [66] | Shende and Thorat | 2020 | 8 | LSTM | 96.92 |
| [67] | Kocher and Kumar | 2021 | 28 | ANN | 99.4 |
| [68] | Mighan and Kahani | 2021 | 65 | ANN | 98.51 |
| [69] | Ashiku and Dagli | 2021 | 33 | DNN | 95.6 |
| [70] | Salih et al. | 2021 | 20 | Bayesian CNN | 99.3271 |
| [71] | Imrana et al. | 2021 | 68 | Bidirectional (BiDLSTM) | 94.26 |
| [72] | Otoum et al. | 2022 | 115 | DL-IDS | 99 |
| [73] | Nasir et al. | 2022 | 13 | DF-IDS | 99.9 |
| [74] | Jasim | 2022 | 23 | Deep belief networks (DBNs) | 99 |
| [75] | Akshay Kumaar et al. | 2022 | 5 | DL-based hybrid framework “ImmuneNet” | 99.2 |
| [76] | Houda et al. | 2022 | 13 | Explainable artificial intelligence (XAI) based DL framework | 99 |
| [77] | Chaganti et al. | 2023 | 0 | LSTM | 97.1 |
| [78] | Figueiredo et al. | 2023 | 0 | LSTM | 99 |
| [79] | Rizvi et al. | 2023 | 2 | 1D-dilated causal neural network (1D-DCNN) | 99.98 |

Table 3: Critical review of federated learning (FL) based approaches in ID.

| Ref | Authors | Year | Cited by | FL approach | Accuracy (%) |
|---|---|---|---|---|---|
| [80] | Supriya and Gadekallu | 2023 | 1 | FL-based approach particle swarm optimization (PSO) | 94.47 |
| [81] | Mu et al. | 2023 | 16 | FedProc: Prototypical contrastive FL | Improves accuracy by 1.6% to 7.9 |
| [82] | Yu et al. | 2023 | 1 | FL-based Iron forge approach | 97 |
| [83] | Nguyen et al. | 2020 | 78 | FL-based IoT IDS | 99.9 |
| [84] | Liu et al. | 2021 | 70 | FL and Blockchain based IDS | >80 |
| [85] | Chen et al. | 2020 | 54 | Federated learning-based attention gated recurrent unit (FedAGRU) | 98.82 |
| [86] | Rahman et al. | 2020 | 119 | FL-based scheme | 83.09 |
| [87] | Mothukuri et al. | 2021 | 173 | FL-based anomaly detection approach | 90.255 |
| [88] | Zhao et al. | 2019 | 94 | Multi-task deep neural network in federated learning (MT-DNN-FL) | 96.54 |
| [89] | Rey et al. | 2022 | 93 | FL-based malware detection framework | 98.59 |
| [90] | Belenguer et al. | 2022 | 6 | FL-based application | 92 |
| [91] | Zhang et al. | 2022 | 9 | SecFedNIDS: Robust defense for poisoning attack against federated learning-based network IDS | Improves 48 |
| [92] | Sarhan et al. | 2023 | 10 | Collaborative cyber threat intelligence sharing scheme | 92 |

In this study [93], the authors highlighted that cyber security has become a critical concern in recent years as information technology has become more widespread. As a result, the field of IDS and their improvement through ML have received significant attention from researchers. Many studies have been conducted in this domain to develop new IDS models and enhance their efficiency in detecting security threats. The aim is to provide a more effective and efficient means of protecting networks and systems against cyber-attacks. This study introduces Passban, an IDS for IoT devices, emphasizing its deployment on low-cost IoT gateways. However, it does not address the challenges of adapting to the rapidly evolving landscape of IoT attacks and the need for continuous updates to counter new threats. Additionally, the paper does not explore the potential scalability issues of deploying such systems across a vast network of diverse IoT devices in various application domains.

In [94], Mojtaba and associates anticipated IDS, an IDS optimized for a limited hardware environment using unsupervised learning. The IDS is designed to detect anomalies in network data and uses unsupervised learning techniques to improve its efficiency. The authors aim to provide a solution that can effectively detect security threats while being optimized for deployment in a limited hardware environment. Using unsupervised learning, the IDS can learn from the data and adapt to changing network behavior without needing labelled data or manual updates. The paper introduces Kitsune as a resource-efficient NIDS, but its real-world scalability and generalization across diverse network environments and attacks remain unverified. Additionally, the extent of human intervention required for setup and maintenance is unclear. In [95], the authors presented an IDS that uses AutoEncoder algorithms for online ID. AutoEncoders are a type of deep-learning algorithm that can detect anomalies in data. The IDS described in this study applies AutoEncoder algorithms to real-time network data, providing an online ID solution. The goal of this IDS is to identify security threats in a fast and efficient manner accurately. AutoEncoder algorithms allow the IDS to learn from the data and adapt to changing network behaviour [39]. The proposed ANN-based sequential classifier aims to balance false positive and false negative rates in ID. However, it introduces potential challenges related to computational overhead, increased detection latency, and the need for fine-tuning. The study lacks an extensive evaluation of its effectiveness against evolving cyber threats.

The authors of [96] investigated the application of ANN and other classification methods for detecting network intrusions. They compared the efficiency of ANNs with other classification algorithms to determine which was the most effective for their specific problem. It was found that an ensemble approach combining multiple classifiers could provide improved efficiency compared to using a single algorithm. This ensemble approach takes advantage of different algorithm's strengths and helps mitigate their weaknesses, leading to improved accuracy and effectiveness in detecting security threats in network data. In this work, the proposed anomaly-based IDS using Genetic Algorithm and Support Vector Machine (SVM) with a new feature selection method offers improved accuracy and reduced false positives. However, the study lacks a comprehensive evaluation of its performance in diverse network environments and against evolving attack strategies. The practical scalability of the model to handle real-world network traffic remains unaddressed.

The authors of [97] suggested a novel network security mechanism that relies on feature extraction. This model uses a GA and a least squares SVM to classify anomalies in security issues. The evaluation outcomes presented that the model has low false-positive rates and high positive rates, making it effective in identifying security issues while avoiding false alarms. Using a proprietary genetic algorithm and least squares, SVM enhances the model's efficiency and accuracy compared to previous techniques. In this work, the two-stage classifier using RepTree algorithm and protocol subset improves ID accuracy, but it may not effectively handle novel or evolving attack patterns not present in the training data. The paper lacks an in-depth analysis of the model's robustness against adversarial attacks, and it does not explore its scalability to handle complex, real-world network environments with a wide range of protocols and attack types.

In [98], a reduced error pruning tree (REPTree) algorithm was established as a method for network security. The proposed model has four key components: a feature selection layer and a protocol grouping sub-layer. The feature selection layer allows users to choose the most relevant features for their security needs. The protocol grouping sub-layer group's network flows into categories based on the protocol used (TCP, UDP, or others). The anomaly detection layer uses the REPTree algorithm to identify unusual network behavior. Finally, the inspection layer examines the detected abnormalities to determine if they represent a security threat. The overall goal of the proposed model is to provide a comprehensive and efficient method for detecting security threats in network data. The authors also explain that CANID, a cascade ensemble-based artificial neural network, is effective for multiclass ID, but it may struggle with novel and rapidly evolving attack techniques. Its scalability and performance in complex, real-world network environments remain unexplored.

In [99], the researchers presented a method that involves feeding the network with feature vectors extracted from network traffic data and training the network to recognize normal and abnormal traffic patterns. During the testing phase, the network is presented with new data, predicting whether the traffic is normal or abnormal based on its training. They used NSL-KDD and UNSW-NB 15 datasets to evaluate the efficiency of ID methods. These datasets consist of feature vectors representing network traffic data labelled as either normal or anomalous. By testing their method on these datasets, the researchers can evaluate the accuracy of their CNN-based ID method. The proposed deep learning binomial classifier shows high accuracy in network ID. Still, it is not clear how well it generalizes to novel, real-world attack scenarios, and the study lacks an assessment of its performance against adversarial attacks or potential

vulnerabilities. In order to take advantage of the capability of CNNs in processing 2D data, the feature vectors were converted into images. This was done by one-hot coding the nominal features, expanding the feature dimensions, and transforming each 8 byte chunk into one pixel. These transformed feature vectors were then turned into $8 \times 8$ pixel images. The researchers implemented a three-layer CNN to classify network attacks. They compared the efficiency of this CNN against other DL networks such as ResNet 50 and GoogLeNet. The results showed a score of 91.14% for the NSL-KDD dataset and 94.9% for the UNSW-NB 15 dataset. The authors have proposed an IDS based on an Artificial Neural Network (ANN) that employs an optimized feature selection approach to maximize operational efficiencies. The method was evaluated on two datasets (UNSW-NB15 and NSL-KDD) and found to be 95.45% accurate, outperforming existing modern approaches. In addition, the authors recommended a mixed ID model that combines Deep Belief Networks (DBN) and SVM [100–102].

The authors [103] presented a novel anomaly-based IDS that leverages gradient-boosted machines (GBM) as the primary detection engine. The authors used a grid search approach to determine the optimal parameters for the GBM. They evaluated their IDS's performance using hold-out and cross-fold validation methods on three distinct datasets: UNSW-NB15, NSL-KDD, and GPRS. Their experimental results demonstrate that the proposed IDS outperforms several other classifiers, such as fuzzy classifiers, GAR forest, and tree-based ensembles, across various performance metrics, including accuracy, specificity, sensitivity, and the area under the curve (AUC). This study demonstrates GBM's superior performance in anomaly-based ID, but it does not assess the model's ability to adapt to emerging or evolving attack strategies. This study's findings could be further validated through additional real-world testing and diverse datasets to assess the model's robustness.

In their study, the authors [104] investigated the performance of a Random Forest (RF) based IDS with regard to accuracy and false alarm rate. The authors used the NSL-KDD, UNSW-NB15, and GPRS datasets for both model training and testing. The proposed IDS was evaluated using different tree-size ensembles, and statistical analysis based on Friedman's ranking revealed that the ensemble of 800 trees achieved the best results, while an ensemble of 20 trees showed the worst performance. Furthermore, the authors demonstrated that the RF-based IDS outperforms other classifiers, such as the ensemble of Random Tree and Naive Bayes, as well as single classifiers, such as NBTree and Multilayer Perceptron. The study highlights the effectiveness of the random forest classifier in ID; however, it lacks a comprehensive analysis of the model's adaptability to new attack patterns and its robustness against adversarial attacks. The evaluation focuses on existing datasets, and the real-world applicability of the model in dynamic and evolving network environments remains unexplored.

In this work, Royet et al. [105] introduce a novel Federated Learning (FL) framework called BrainTorrent, specifically designed for highly dynamic peer-to-peer (P2P) environments. On the other hand, the authors of another research propose a different FL framework, named BAFFLE, that is based on BC and does not require an aggregator. The authors demonstrate their proposed framework's high scalability and computational efficiency in a private Ethereum network. The study introduces BrainTorrent as a federated learning (FL) framework for medical applications, but it does not thoroughly address the potential challenges related to network coordination, security, and scalability in a decentralized, peer-to-peer environment. Additionally, the paper does not explore the real-world complexities and regulatory concerns related to privacy and data protection in a multicentre medical context, which can affect the practicality and adoption of FL solutions.

In this research [106], the authors present a comprehensive overview of the use of Federated Learning (FL) in information security, specifically focusing on ID as one of its applications. Their paper provides explanatory insights into the topic and covers a broader scope than just ID. On the other hand, the authors also focus on Federated Intrusion Detection Systems (FIDSs), but their methodology differs from that of authors. This study highlights the potential of federated learning (FL) for improving cybersecurity, but it lacks a comprehensive exploration of the real-world challenges and complexities of deploying FL in dynamic, real-time environments. It does not provide in-depth insights into the practical implementation hurdles, potential network coordination issues, and the need for robust security measures. Furthermore, the paper does not delve into the regulatory and ethical considerations surrounding the use of FL in handling sensitive data in real-time applications. The authors of [107] compile a list of existing FIDSs and provide a detailed overview of their approaches while also identifying open issues in the field. This study cannot recognize encrypted packets and thus leaves an opportunity for attack. Moreover, the creation of a normal model for enormous dynamic data is extremely challenging, which leads to false alarms.

## 3. Black-Box and White-Box-Based Artificial Intelligence Approaches in Intrusion Detection Systems

In the domain of IDS, two contrasting paradigms develop the black box and white-box AI approaches. Black box methods, such as ML-based IDS and DL-based IDS, use algorithms and neural networks to find patterns and anomalies within data automatically. While ML-based IDS has the advantage of detecting complex and novel attacks with minimal feature engineering, it often lacks transparency in decision-making and vulnerability to adversarial manipulations. Similarly, DL-based IDS excels in detecting complex patterns within large and detailed datasets. However, its need for significant computational resources and the difficulty in understanding how it works emphasize the compromises linked to its black-box nature. On the other side, White box methods, including Rule-Based IDS and Feature Engineering-Based IDS, emphasize interpretability and human domain knowledge.

Rule-Based IDS relies on preset patterns, making it easy to understand and identify known attacks, though it might miss new threats. Feature Engineering-Based IDS empowers experts to create features based on their knowledge, improving interpretability by concerning features to attack types. Nevertheless, the investment in domain expertise and the potential for incomplete pattern coverage are critical considerations. Meanwhile, Federated Learning (FL)-based IDS, a new approach, ensures privacy by training models together on separate devices. FL addresses privacy and teamwork concerns, but communication overhead and potential loss of detailed information during collaboration highlight the complexities of this method. To navigate IDS development effectively, grasping both black-box and white-box concepts is vital for wise choices.

IDSs based on ML, DL, and FL approaches have shown promising results in detecting and mitigating security threats. Machine Learning (ML) is a subfield of AI [108–110]. Many ML techniques are increasingly being used for ID in network security. IDS are used to monitor network traffic and detect any unauthorized or malicious activities. Traditional IDS rely on pre-defined rules and signatures to identify known attacks, but they may fail to detect novel or unknown attacks. ML algorithms can be used to learn the patterns and characteristics of normal network traffic and then detect anomalies or deviations from this normal behavior, which may indicate the presence of an intrusion. Some of the ML approaches are shown in Table 1.

It is shown in Table 1 that ML has developed as a promising technique for ID, and several ML algorithms have been proposed and tested in this area. K Nearest Neighbour (KNNs) and SVMs are the most widely used ML techniques for ID. ANNs can learn patterns from input data and make predictions based on them, while SVMs effectively separate data into different classes. Decision Trees (DTs) and Random Forests (RFs) are popular ML algorithms for ID, as they can handle both categorical and continuous data. Additionally, Deep Learning (DL) methods, such as CNNs and RNNs, have shown promising results for ID due to their potential to learn hierarchical representations of information. However, selecting the best ML algorithm for ID depends on several factors, such as the dataset, the specific problem being addressed, and the resources available for training and deployment.

Deep Learning-based approaches such as CNNs and RNNs have presented high accuracy in identifying intrusions by learning patterns in raw network traffic data. ML-based approaches such as SVMs and DTs can detect intrusions by classifying network traffic data based on previously learned patterns. FL-based approaches allow multiple parties to cooperate in training a global model without exchanging their private data, offering an attractive alternative for ID in sensitive environments. The choice of approach depends on multiple aspects, such as the size and difficulty of the dataset, the level of security and privacy required, and the computational and communication resources available. Ultimately, these approaches effectively detect and mitigate security threats in today's complex and dynamic network environments.

Table 2 presents a comprehensive overview of various DL-based IDSs in cybersecurity. The approaches include DNN, Feed Forward Deep Neural Network (FDDNN), RNN, CNN, ANN, Bayesian Convolutional Neural Network (BCCN), Deep Belief Network (DBN), AutoEncoder (AE), Long Short-Term Memory (LSTM), Self-Taught Learning (STL), Hierarchical Spatial-Temporal Features-based Intrusion Detection System (HAST-ID), Non-Symmetric Deep AutoEncoder (NDAE), Deep Learning H2O, Feed Forward Neural Network (FFNN), Two Stage Deep Learning (TSDL) Model, BAT Model, Bidirectional Long-Short-Term-Memory (BiDLSTM), 1D-Dilated Causal Neural Network (1D-DCNN), Hybrid framework "ImmuneNet," and Explainable Artificial Intelligence (XAI)-based DL Framework. The choice of ID method depends on the task's specific needs. RNN, a type of DL model, is suitable for ID as it can process sequential data. RNNs can analyze network traffic in real-time to identify anomalies and potential threats by using a memory of past inputs created by looping the output back into the network [41, 42, 46, 47, 72, 73, 75, 76, 111–116]. The network can use previous inputs, such as past network traffic patterns, to help identify unusual behavior in the current traffic. Generally, RNNs are a powerful tool for ID, as they can learn complex dependencies in sequential data and help to identify anomalies in real time. Deep Neural Network (DNN), is a type of ML model that uses multiple layers to learn representations of input data. DNNs can be employed in ID to learn characteristics from network traffic data to detect abnormalities and probable breaches. A feed-forward deep neural network is a form of DNN that only operates in one way, from input to output, and does not include loops or recurrent connections. FDDNNs may be used in ID to learn complex features in data from the network.

A CNN is a DL architecture that processes grid-structured data, such as images. CNNs can be leveraged to extract meaningful features from network traffic data, which can then be used to identify patterns indicative of specific types of intrusions. ANN is stimulated by the arrangement and function of the human brain and is a type of ML model that can be used for a wide range of applications. In ID, ANNs can be trained to recognize complex patterns in network traffic data to detect anomalies that may indicate a potential intrusion.

Bayesian convolutional neural networks (BCNNs) are a variant of CNNs that incorporate Bayesian methods to account for uncertainty in the model's predictions. In ID, BCNNs can provide more reliable predictions by modelling the uncertainty associated with the ID query. A Deep Belief Network (DBN) is a DL architecture that uses unsupervised pre-training to detect anomalies in network traffic data for ID. An Autoencoder is a DL model that learns a compact illustration of network flow to detect anomalies and potential intrusions in ID. Both DBNs and Autoencoders are useful for identifying unusual behavior in network traffic data.

In ID, AEs can be used to learn features from network traffic data indicative of normal behavior, which can then be used to identify anomalies and potential intrusions. An

LSTM type of RNN uses gating mechanisms to allow the network to remember or forget information from its memory selectively. In ID, LSTMs can be used to analyze network traffic data in real-time to identify anomalies and potential intrusions, taking into account both short-term and long-term patterns. Self-taught learning is unsupervised learning that uses unlabeled data to learn representations of the data. In ID, STL can be used to learn features from network traffic data without needing labelled data, which can then be used to identify anomalies and potential intrusions. HAST-ID is a DL IDS that leverages hierarchical spatial-temporal features to detect network intrusions. It employs a CNN to extract features from raw network traffic data and LSTM network to model temporal dependencies.

On the other hand, a nonsymmetric deep AutoEncoder (NDAE) uses a nonsymmetric deep auto-encoder to learn the normal actions of a system and recognize deviations from it as potential interferences. Deep Learning H2O is a platform for building, training, and deploying DL models for ID, capable of supporting binomial and multinomial models for classifying network traffic as normal or intrusion. TSDL employs a two-stage learning approach in its DL-based IDS [36, 37, 48, 74, 117].

Using a combination of DNN and RNN in the BAT model for ID is a common approach in the security field. Using a DNN for feature extraction allows for the decrease of dimensionality and abstraction of raw data into a more manageable form for analysis. Using a RNN, specifically the BLSTM, enables the model to capture the temporal relationships and dependencies in the data, which is significant for accurately identifying anomalies and intrusions. The attention mechanism in the BAT model helps the network focus on the most relevant parts of the data, allowing for more accurate and fine-tuned predictions. In general, using such DL approaches in ID processes has shown promising results and has been an active area of research [34, 42, 72]. It is commonly used for ID to analyze time-series data such as network traffic logs. 1D-DCNN is a type of CNN designed to process data sequences. It uses a dilated causal structure that allows the network to process longer sequences of data while still preserving the causal relationship between the data points. ImmuneNet is a hybrid framework for ID that combines DL and immune system-inspired algorithms [46]. It uses a deep neural network (DNN) to extract features from network traffic data and an immune system-inspired algorithm to detect intrusions based on these features. XAI is a field of AI that focuses on developing transparent and interpretable algorithms. In the context of ID, an XAI-based DL framework would use algorithms that provide clear explanations for why a particular instance of network traffic is being classified as normal or as an intrusion.

Table 2 presents a comprehensive evaluation of various DL methods for ID concerning accuracy. The results demonstrate that DL approaches accurately predict cybersecurity threats.

DL techniques [111] have become popular in ID due to their potential to switch complex relationships and extract relevant features from raw data. The examples you mentioned, HAST-ID and Non-symmetric Deep AutoEncoder (NDAE), demonstrate the capability of DL to extract both spatial and temporal features and learn a low-dimensional illustration of the information. Meanwhile, the Deep Learning H2O framework is based on binomial and multinomial models and provides a fast and precise approach to ID. The Feed Forward Neural Network (FFNN) and Two Stage Deep Learning (TSDL) Models use feed-forward neural networks and a two-stage deep learning approach to make predictions about intrusions. The Bidirectional Long-Short-Term-Memory (BiDLSTM), 1D-Dilated Causal Neural Network (1D-DCNN), DL-based Hybrid Framework "ImmuneNet", and Explainable Artificial Intelligence (XAI) based DL Framework all demonstrate promising results in ID by utilizing bidirectional long-short term memory networks, dilated causal neural networks, a hybrid DL framework, XAI-based framework [118], ANN [112], IoT-based devices [113] and machine learning-based framework [114–116].

It is shown in Table 3 that FL has emerged as a promising approach for ID, allowing multiple parties to cooperate in the training of a global model without exchanging their private information. FL offers advantages over traditional centralized machine learning approaches by protecting the privacy of sensitive data and reducing the risk of data breaches. Various FL approaches have been suggested for ID, containing federated SVM (FedSVM), federated extreme learning machine (FedELM), federated ensemble-based anomaly detection (FedEAD), and federated autoencoder (FedAE). However, selecting the best FL approach for ID depends on several factors, such as the number of participating gadgets, the difficulty of the data, the communication and computational resources available, and the level of security and privacy required. Further research is needed to assess the effectiveness of FL in ID and optimize its performance in real-world scenarios. DL, ML, and FL approaches have shown prominent performance in IDSs but have some strengths and weaknesses, as presented in Figure 1.

It is shown in Figure 1 that Explainable AI-based IDSs have several advantages over deep learning, machine learning, and federated learning-based IDS. Firstly, explainable AI-based IDS provides transparency by clearly explaining the decision-making process. This makes it easier to understand how the decision was made and what factors were considered. In contrast, deep learning or machine learning-based IDS can be opaque, making it difficult to understand how the decision was made. Secondly, explainable AI-based IDS can detect and identify any biases in the system, thus improving fairness and accuracy. In contrast, deep learning or machine learning-based IDS can be susceptible to biases that may go unnoticed. Thirdly, explainable AI-based IDS is flexible and can be adapted to various scenarios. This is because the rules governing the decision-making process are transparent and easily modified. Fourthly, explainable AI-based IDS provides insights into the underlying security threats and vulnerabilities, which helps improve the system's security posture. Conversely, deep learning or machine learning-based IDS may not provide such insights, making it difficult to address

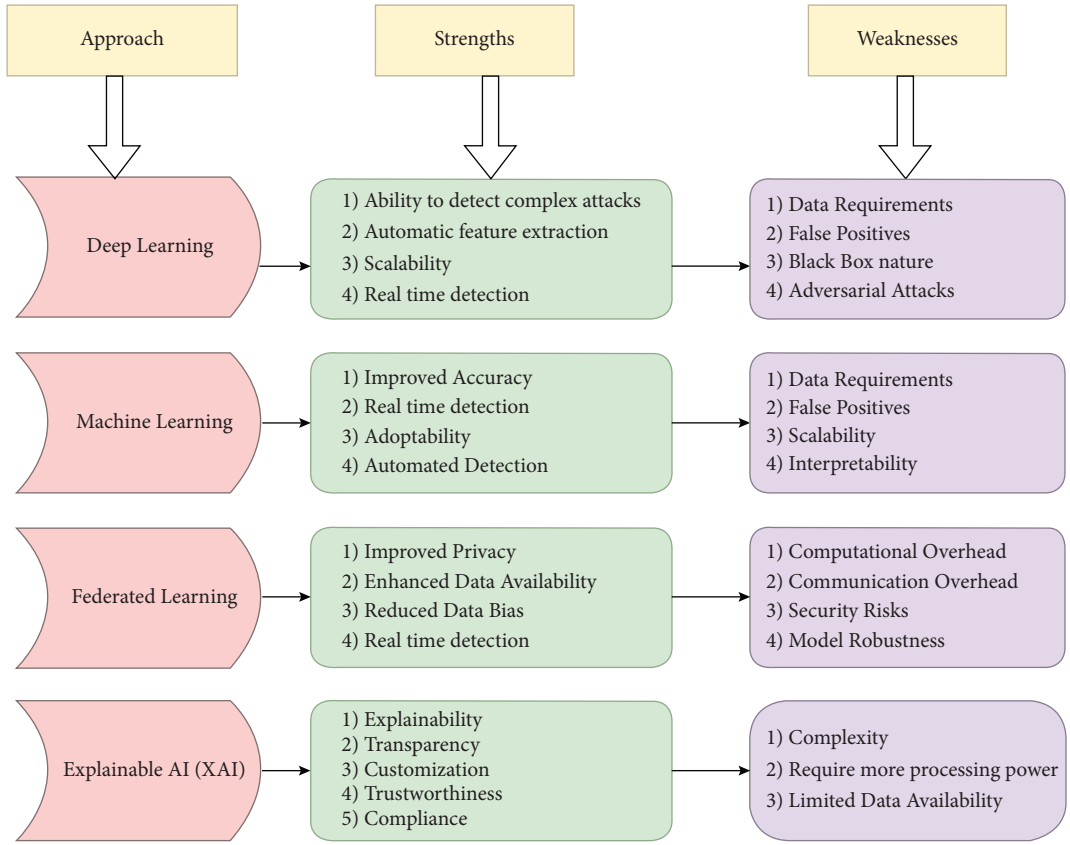


Figure 1: Strengths & weaknesses of DL, ML, FL and XAI approach.

security issues proactively. Lastly, explainable AI-based IDS can help meet regulatory requirements requiring decision-making transparency. Therefore, explainable AI-based IDS may be a better option for ID in many scenarios.

## 4. Conclusion

Intrusion detection in cybersecurity is vital as advanced attacks rise. Innovative technologies like DL, ML, and FL play crucial roles. DL-based approaches have demonstrated high accuracy rates in detecting intrusion attacks. These approaches learn complex network traffic data patterns and can detect known and unknown attacks. But, these methods need a large volume of information and computing resources for training, which can be challenging for some organizations. ML-based approaches are simpler and less resource-intensive than DL-based approaches. They can detect known attacks with high accuracy rates but may not perform well in detecting unknown attacks. FL-based approaches, which leverage collective learning from multiple decentralized devices, offer a promising solution for organizations that cannot share data due to privacy or security concerns. They allow for the training of models on distributed datasets without sharing data. This study systematically explores enhancing and securing ID systems with ML, DL, FL, and XAI. It critically assesses these approaches, with DL achieving high accuracy at the cost of resources. ML, though simpler, has limitations in detecting unknown attacks. FL shows promise for data-sensitive organizations, though further research is necessary. Organizations should carefully assess their needs and resources to select the appropriate IDS technique.

## 5. Future Research Directions and Recommendations

Future research directions in ID can explore the integration of Blockchain technology and XAI with existing techniques like ML, DL, and FL. BCT can offer a decentralized, secure, and tamper-resistant environment for storing and sharing ID data. It can also facilitate the secure exchange of models and updates between different entities involved in the FL-based approach. Additionally, XAI techniques can enhance the interpretability and transparency of the models, enabling security professionals to understand and verify the model's behavior.

One potential research direction could be to explore how Blockchain technology can be used to improve the privacy and security of FL-based IDSs. FL permits several entities to train a model collectively without exchanging their information. However, there may still be concerns about the privacy of the data being utilized to train the model. BCT may offer a protected and transparent platform for data sharing without compromising data privacy.

Another potential research direction could be to develop XAI techniques that can explain the behavior of DL-based

ID models. DL-based models are often highly complex and difficult to interpret, which can make it challenging to understand why a particular intrusion was detected. Developing XAI techniques that can explain the behavior of DL-based models can improve their transparency and interpretability, providing valuable insights into their decision-making process. Generally, the integration of Blockchain technology and XAI with existing ID approaches has the potential to enhance the privacy, security, interpretability, and transparency of these systems. Further research in this area can help to develop more robust and effective IDSs that can better protect computer networks from malicious attacks.

## Data Availability

All the data related to this study will be provided to the corresponding author upon request.

## Conflicts of Interest

The authors declare that there are no conflicts of interest.

## Authors' Contributions

Salman Muneer played a pivotal role in identifying the research problem and formulating potential solutions. On the other hand, Umer Farooq, Atifa Athar, and Muhammad Ahsan Raza provided valuable insights through their thorough review comments and contributed significantly to the comparative analysis. In parallel, Taher M. Ghazal and Shadman Sakib played critical roles in the in-depth comparative analysis. Their individual contributions have enriched the research process, ensuring a comprehensive and well-rounded exploration of the identified problem and proposed solutions.

## References

[1] R. Malik, H. Raza, and M. Saleem, "Towards A Blockchain enabled integrated library managment system using hyperledger fabric: using hyperledger fabric," *International Journal of Computational and Innovative Sciences*, vol. 1, no. 3, pp. 17–24, 2022.

[2] J. A. Malik and M. Saleem, "Blockchain and cyber-physical system for security engineering in the smart industry," in *Security Engineering for Embedded and Cyber-Physical Systems*, pp. 51–70, CRC Press, Boca Raton, FL, USA, 2022.

[3] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion detection techniques in cloud environment: a survey," *Journal of Network and Computer Applications*, vol. 77, pp. 18–47, 2017.

[4] J. Wei, C. Long, J. Li, and J. Zhao, "An intrusion detection algorithm based on bag representation with ensemble support vector machine in cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 24, p. 14, 2020.

[5] K. Peng, V. C. M. Leung, L. Zheng, S. Wang, C. Huang, and T. Lin, "Intrusion detection system based on decision tree over big data in fog environment," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 4680867, 10 pages, 2018.

[6] Q. Schueller, K. Basu, M. Younas, M. Patel, and F. Ball, "A hierarchical intrusion detection system using support vector machine for sdn network in cloud data center," in *Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC)*, p. 6, Sydney, Australia, June 2018.

[7] C. Modi, D. Patel, B. Borisanya, A. Patel, and M. Rajarajan, "A novel framework for intrusion detection in cloud," in *Proceedings of the Fifth International Conference on Security of Information and Networks*, pp. 67–74, Jaipur, India, April 2012.

[8] B. Sundararaman, S. Jagdev, and N. Khatri, "Transformative role of artificial intelligence in advancing sustainable tomato (Solanum lycopersicum) disease management for global food security: a comprehensive review," *Sustainability*, vol. 15, no. 15, Article ID 11681, 2023.

[9] G. Dhanush, N. Khatri, S. Kumar, and P. K. Shukla, "A comprehensive review of machine vision systems and artificial intelligence algorithms for the detection and harvesting of agricultural produce," *Scientific African*, vol. 21, Article ID e01798, 2023.

[10] P. Ghosh, A. K. Mandal, and R. Kumar, "An efficient cloud network intrusion detection system," *Information Systems Design and Intelligent Applications*, Springer, New York, NY, USA, 2015.

[11] P. Deshpande, S. C. Sharma, S. K. Peddoju, and S. Junaid, "HIDS: a host based intrusion detection system for cloud computing environment," *International Journal of System Assurance Engineering and Management*, vol. 9, no. 3, pp. 567–576, 2018.

[12] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[13] T. Mohamed, A. Ibrahim, T. Faiz et al., "Intelligent hand gesture recognition system empowered with CNN," in *Proceedings of the 2022 International Conference on Cyber Resilience (ICCR)*, IEEE, Dubai, United Arab Emirates, July 2022.

[14] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: a survey," *Applied Sciences*, vol. 9, no. 20, p. 4396, 2019.

[15] V. R. Pathmudi, N. Khatri, S. Kumar, A. S. Abdul-Qawy, and A. K. Vyas, "A systematic review of IoT technologies and their constituents for smart and sustainable agriculture applications," *Scientific African*, vol. 19, Article ID e01577, 2023.

[16] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for iot intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, Article ID 102031, 2020.

[17] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: towards secure iot architecture," *Internet of Things*, vol. 34, pp. 82–89, 2018.

[18] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," *Physical Communication*, vol. 42, Article ID 101157, 2020.

[19] O. Alkadi, N. Moustafa, B. Turnbull, and K. K. R. Choo, "A deep Blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463–9472, 2021.

[20] P. Ghosh, A. Karmakar, J. Sharma, and S. Phadikar, "Cs-pso based intrusion detection system in cloud environment," in

*Emerging Technologies in Data Mining and Information Security*, pp. 261–269, Springer, New York, NY, USA, 2019.

[21] R. SaiSindhuTheja and G. K. Shyam, "An efficient metaheuristic algorithm based feature selection and recurrent neural network for dos attack detection in cloud computing environment," *Applied Soft Computing*, vol. 100, Article ID 106997, 2021.

[22] M. T. Nguyen and K. Kim, "Genetic convolutional neural network for intrusion detection systems," *Future Generation Computer Systems*, vol. 113, pp. 418–427, 2020.

[23] M. Gauthama Raman, N. Somu, K. Kirthivasan, R. Liscano, and V. Shankar Sriram, "An efficient intrusion detection system based on hypergraph-genetic algorithm for parameter optimization and feature selection in support vector machine," *Knowledge-Based Systems*, vol. 134, pp. 1–12, 2017.

[24] S. Malhotra, V. Bali, and K. Paliwal, "Genetic programming and k-nearest neighbour classifier based intrusion detection model," in *Proceedings of the 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, pp. 42–46, IEEE, Noida, India, June 2017.

[25] M. Mayuranathan, M. Murugan, and V. Dhanakoti, "Retracted article: best features based intrusion detection system by RBM model for detecting DDoS in cloud environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3609–3619, 2019.

[26] J. Kumar Seth and S. Chandra, "Mids: metaheuristic based intrusion detection system for cloud using k-nn and mgwo," in *Proceedings of the International Conference on Advances in Computing and Data Sciences*, pp. 411–420, Springer, Dehradun, India, June 2018.

[27] S. P. Rm, P. K. Maddikunta, M. Parimala et al., "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Computer Communications*, vol. 160, pp. 139–149, 2020.

[28] F. Ahmed, M. Asif, and M. Saleem, "Identification and prediction of brain tumor using VGG-16 empowered with explainable artificial intelligence," *International Journal of Computational and Innovative Sciences*, vol. 2, no. 2, pp. 24–33, 2023.

[29] M. Saleem, M. S. Khan, G. F. Issa et al., "Smart spaces: occupancy detection using adaptive back-propagation neural network," in *Proceedings of the 2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, pp. 1–6, Dubai, United Arab Emirates, June 2023.

[30] A. Athar, R. N. Asif, M. Saleem, S. Munir, M. R. Al Nasar, and A. M. Momani, "Improving pneumonia detection in chest X-rays using transfer learning approach (AlexNet) and adversarial training," in *Proceedings of the 2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, pp. 1–7, Dubai, United Arab Emirates, July 2023.

[31] A. Abualkishik, M. Saleem, U. Farooq, M. Asif, M. Hassan, and J. A. Malik, "Genetic algorithm based adaptive FSO communication link," in *Proceedings of the 2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, pp. 1–4, Dubai, United Arab Emirates, June 2023.

[32] G. Sajjad, M. B. Shoaib Khan, T. M. Ghazal, M. Saleem, M. F. Khan, and M. Wannous, "An early diagnosis of brain tumor using fused transfer learning," in *Proceedings of the 2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, pp. 1–5, Dubai, United Arab Emirates, June 2023.

[33] H. A. Ahmed, A. Hameed, and N. Z. Bawany, "Network intrusion detection using oversampling technique and machine learning algorithms," *Peer Journal Computer Science*, vol. 8, p. e820, 2022.

[34] A. Singh, J. Amutha, J. Nagar, S. Sharma, and C. C. Lee, "Lt-fs-id: log-transformed feature learning and feature-scaling-based machine learning algorithms to predict the k-barriers for intrusion detection using wireless sensor network," *Sensors*, vol. 22, no. 3, p. 1070, 2022.

[35] M. B. Pranto, M. H. Ratul, M. M. Rahman, I. J. Diya, and Z. B. Zahir, "Performance of machine learning techniques in anomaly detection with basic feature selection strategy-a network intrusion detection system," *Journal of Advances in Information Technology*, vol. 13, no. 1, 2022.

[36] A. Raghuvanshi, U. K. Singh, G. S. Sajja et al., "Intrusion detection using machine learning for risk mitigation in IoT-enabled smart irrigation in smart farming," *Journal of Food Quality*, vol. 2022, Article ID 3955514, 8 pages, 2022.

[37] K. Albulayhi, Q. Abu Al-Haija, S. A. Alsuhibany, A. A. Jillepalli, M. Ashrafuzzaman, and F. T. Sheldon, "IoT intrusion detection using machine learning with a novel high performing feature selection method," *Applied Sciences*, vol. 12, no. 10, p. 5015, 2022.

[38] M. Asif, S. Abbas, M. A. Khan, A. Fatima, M. A. Khan, and S. W. Lee, "MapReduce based intelligent model for intrusion detection using machine learning technique," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 9723–9731, 2022.

[39] Ü Çavuşoğlu, "A new hybrid approach for intrusion detection using machine learning methods," *Applied Intelligence*, vol. 49, no. 7, pp. 2735–2761, 2019.

[40] H. Alqahtani, I. H. Sarker, A. Kalim, S. M. Minhaz Hossain, S. Ikhlaq, and S. Hossain, "Cyber intrusion detection using machine learning classification techniques," in *Proceedings of the InComputing Science, Communication and Security: First International Conference, COMS2 2020*.

[41] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: a survey," *Applied Sciences*, vol. 9, no. 20, p. 4396, 2019.

[42] J. Ren, J. Guo, W. Qian, H. Yuan, X. Hao, and H. Jingjing, "Building an effective intrusion detection system by using hybrid data optimization based on machine learning algorithms," *Security and Communication Networks*, vol. 2019, Article ID 7130868, 11 pages, 2019.

[43] N. Bindra and M. Sood, "Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset," *Automatic Control and Computer Sciences*, vol. 53, no. 5, pp. 419–428, 2019.

[44] K. Sai Kiran, R. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. Karthi, "Building a intrusion detection system for IoT environment using machine learning techniques," *Procedia Computer Science*, vol. 171, pp. 2372–2379, 2020.

[45] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. A. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: a review," *Procedia Computer Science*, vol. 171, pp. 1251–1260, 2020.

[46] G. Logeswari, S. Bose, and T. Anitha, "An intrusion detection system for SDN using machine learning," *Intelligent Automation & Soft Computing*, vol. 35, no. 1, pp. 867–880, 2023.

[47] M. U. Muhammad and A. M. Saleem, "Intelligent intrusion detection system for Apache web server empowered with machine learning approaches," *International Journal of Computational and Innovative Sciences*, vol. 1, no. 1, pp. 1–8, 2022.

[48] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[49] R. Vani, "Towards efficient intrusion detection using deep learning techniques: a review," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3297, p. 2007, 2017.

[50] W. Wang, Y. Sheng, J. Wang et al., "HAST-IDS: learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," *IEEE Access*, vol. 6, pp. 1792–1806, 2018.

[51] 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, 2018.

[52] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE transactions on emerging topics in computational intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[53] B. Lee, S. Amaresh, C. Green, and D. Engels, "Comparative study of deep learning models for network intrusion detection," *SMU Data Science Review*, vol. 1, no. 1, p. 8, 2018.

[54] 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.

[55] Y. Ding and Y. Zhai, "Intrusion detection system for NSL-KDD dataset using convolutional neural networks," *Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence*, vol. 8, pp. 81–85, 2018.

[56] S. Parampottupadam and A. N. Moldovann, "Cloud-based real-time network intrusion detection using deep learning," in *Proceedings of the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1–8, London, UK, May 2018.

[57] Y. Xin, L. Kong, Z. Liu et al., "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[58] O. Faker and E. Dogdu, "Intrusion detection using big data and deep learning techniques," in *Proceedings of the 2019 ACM Southeast Conference*, pp. 86–93, New York, NY, USA, July 2019.

[59] S. Laqtib, K. E. Yassini, and M. L. Hasnaoui, "A deep learning methods for intrusion detection systems based machine learning in manet," *Proceedings of the 4th International Conference on Smart City Applications*, vol. 2, pp. 1–8, 2019.

[60] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," in *Proceedings of the 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 256–25609, Kyoto, Japan, June 2019.

[61] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "TSDL: a two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019.

[62] S. Gurung, M. Kanti Ghose, and A. Subedi, "Deep learning approach on network intrusion detection system using NSL-KDD dataset," *International Journal of Computer Network and Information Security*, vol. 11, no. 3, pp. 8–14, 2019.

[63] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: deep learning methods on network intrusion detection using NSL-KDD dataset," *IEEE Access*, vol. 8, no. 8, pp. 29575–29585, 2020.

[64] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: a survey and an objective comparison," *Journal of Network and Computer Applications*, vol. 169, Article ID 102767, 2020.

[65] A. Boukhalfa, A. Abdellaoui, N. Hmina, and H. Chaoui, "LSTM deep learning method for network intrusion detection system," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, p. 3315, 2020.

[66] S. Shende and S. Thorat, "Long short-term memory (LSTM) deep learning method for intrusion detection in network security," *International Journal of Engineering Research*, vol. 9, no. 06, 2020.

[67] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges," *Soft Computing*, vol. 25, no. 15, pp. 9731–9763, 2021.

[68] S. N. Mighan and M. Kahani, "A novel scalable intrusion detection system based on deep learning," *International Journal of Information Security*, vol. 20, no. 3, pp. 387–403, 2021.

[69] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Procedia Computer Science*, vol. 185, pp. 239–247, 2021.

[70] A. A. Salih, S. Y. Ameen, S. R. Zeebaree et al., "Deep learning approaches for intrusion detection," *Asian Journal of Research in Computer Science*, pp. 50–64, 2021.

[71] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," *Expert Systems with Applications*, vol. 185, Article ID 115524, 2021.

[72] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, 2022.

[73] M. Nasir, A. R. Javed, M. A. Tariq, M. Asim, and T. Baker, "Feature engineering and deep learning-based intrusion detection framework for securing edge IoT," *The Journal of Supercomputing*, vol. 78, no. 6, pp. 8852–8866, 2022.

[74] A. D. Jasim and Ammar D.Jasim, "A survey of intrusion detection using deep learning in internet of things," *Iraqi Journal For Computer Science and Mathematics*, vol. 3, no. 1, pp. 83–93, 2022.

[75] M. Akshay Kumaar, D. Samiayya, P. M. Vincent, K. Srinivasan, C. Y. Chang, and H. Ganesh, "A hybrid framework for intrusion detection in healthcare systems using deep learning," *Frontiers in Public Health*, vol. 9, p. 2295, 2022.

[76] Z. A. E. Houda, B. Brik, and L. Khoukhi, "Why should i trust your ids? An explainable deep learning framework for intrusion detection systems in Internet of Things networks," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1164–1176, 2022.

[77] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," *Information*, vol. 14, no. 1, p. 41, 2023.

[78] J. Figueiredo, C. Serrão, and A. M. de Almeida, "Deep learning model transposition for network intrusion detection systems," *Electronics*, vol. 12, no. 2, p. 293, 2023.

[79] S. Rizvi, M. Scanlon, J. McGibney, and J. Sheppard, *Deep Learning Based Network Intrusion Detection System for Resource-Constrained Environments*, Springer, Berlin, Germany, 2023.

[80] Y. Supriya and T. R. Gadekallu, "Particle swarm-based federated learning approach for early detection of forest fires," *Sustainability*, vol. 15, no. 2, p. 964, 2023.

[81] X. Mu, Y. Shen, K. Cheng et al., "Fedproc: prototypical contrastive federated learning on non-iid data," *Future Generation Computer Systems*, vol. 143, pp. 93–104, 2023.

[82] G. Yu, X. Wang, C. Sun et al., "IronForge: an open, secure, fair, decentralized federated learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 52, 2023.

[83] T. D. Nguyen, P. Rieger, M. Miettinen, and A. R. Sadeghi, "Poisoning attacks on federated learning-based IoT intrusion detection system," *Proceedings 2020 Workshop on Decentralized IoT Systems and Security*, vol. 23, pp. 1–7, 2020.

[84] H. Liu, S. Zhang, P. Zhang et al., "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6073–6084, 2021.

[85] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, and W. Pan, "Intrusion detection for wireless edge networks based on federated learning," *IEEE Access*, vol. 8, pp. 217463–217472, 2020.

[86] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, "Internet of things intrusion detection: centralized, on-device, or federated learning?" *IEEE Network*, vol. 34, no. 6, pp. 310–317, 2020.

[87] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for iot security attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545–2554, 2022.

[88] Y. Zhao, J. Chen, D. Wu, J. Teng, and S. Yu, "Multi-task network anomaly detection using federated learning," *Proceedings of the Tenth International Symposium on Information and Communication Technology- SoICT 2019*, vol. 4, pp. 273–279, 2019.

[89] V. Rey, P. M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet, "Federated learning for malware detection in iot devices," *Computer Networks*, vol. 204, Article ID 108693, 2022.

[90] A. Belenguer, J. Navaridas, and J. A. Pascual, "A review of federated learning in intrusion detection systems for iot," 2022, https://arxiv.org/abs/2204.12443.

[91] Z. Zhang, Y. Zhang, D. Guo, L. Yao, and Z. Li, "SecFedNIDS: robust defense for poisoning attack against federated learning-based network intrusion detection system," *Future Generation Computer Systems*, vol. 134, pp. 154–169, 2022.

[92] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection," *Journal of Network and Systems Management*, vol. 31, no. 1, p. 3, 2023.

[93] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6882–6897, 2020.

[94] Y. Mirsky, T. Doitshman, Y. Elovici, and A. K. Shabtai, "An ensemble of autoencoders for online network intrusion detection," 2018, https://arxiv.org/abs/1802.09089.

[95] H. Zhao, Y. Feng, H. Koide, and K. Sakurai, "An ANN based sequential detection method for balancing performance indicators of IDS," *2019 Seventh International Symposium on Computing and Networking (CANDAR)*, vol. 56, pp. 239–244, 2019.

[96] H. Gharaee and H. Hosseinvand, "A new feature selection IDS based on genetic algorithm and SVM," in *Proceedings of the 2016 8th International Symposium on Telecommunications (IST)*, pp. 139–144, Tehran, Iran, August 2016.

[97] M. Belouch, S. El, and M. Idhammad, "A two-stage classifier approach using reptree algorithm for network intrusion detection," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 389–394, 2017.

[98] M. M. Baig, M. M. Awais, and E. S. M. El-Alfy, "A multiclass cascade of artificial neural network for network intrusion detection," *Journal of Intelligent and Fuzzy Systems*, vol. 32, no. 4, pp. 2875–2883, 2017.

[99] M. Al-Zewairi, S. Almajali, and A. Awajan, "Experimental evaluation of a multi-layer feed-forward artificial neural network classifier for network intrusion detection system," in *Proceedings of the 2017 International Conference on New Trends in Computing Sciences (ICTCS)*, pp. 167–172, Amman, Jordan, May 2017.

[100] S. Guha, S. S. Yau, and A. B. Buduru, "Attack detection in cloud infrastructures using artificial neural network with genetic feature selection," in *Proceedings of the 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress*, pp. 414–419, Auckland, New Zealand, June 2016.

[101] K. K. Nguyen, D. T. Hoang, D. Niyato, P. Wang, D. Nguyen, and E. Dutkiewicz, "Cyberattack detection in mobile cloud computing: a deep learning approach," in *Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Barcelona, Spain, July 2018.

[102] N. Moustafa, G. Misra, and J. Slay, "Generalized outlier Gaussian mixture technique based on automated association features for simulating and detecting web application attacks," *IEEE Trans. Sustain. Comput*, vol. 6, no. 2, pp. 245–256, 2021.

[103] B. A. Tama and K. H. Rhee, "An in-depth experimental study of anomaly detection using gradient boosted machine," *Neural Computing & Applications*, vol. 31, no. 4, pp. 955–965, 2019.

[104] R. Primartha and B. A. Tama, "Anomaly detection using random forest: a performance revisited," in *Proceedings of the 2017 International Conference on Data and Software Engineering (ICoDSE)*, pp. 1–6, Palembang, Indonesia, June 2017.

[105] A. G. Roy, S. Siddiqui, S. Polsterl, N. Navab, and C. Wachinger, "Braintorrent: A peer-to-peer environment for decentralized federated learning," 2019, https://arxiv.org/abs/1905.06731.

[106] M. Alazab, S. P. R M, P. M, P. Reddy, T. R. Gadekallu, and Q.-V. Pham, "Federated learning for cybersecurity: concepts, challenges and future directions," *IEEE Transactions on Industrial Informatics*, vol. 58, 2021.

[107] S. Agrawal, S. Sarkar, O. Aouedi et al., "Federated learning for intrusion detection system: concepts," *Challenges and Future Directions*, vol. 16, 2021.

[108] S. Yamin Siddiqui, M. Adnan Khan, S. Abbas, and F. Khan, "Smart occupancy detection for road traffic parking using deep extreme learning machine," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 3, pp. 727–733, 2022.

[109] A. H. Khan, S. Abbas, M. A. Khan et al., "Intelligent model for brain tumor identification using deep learning," *Applied Computational Intelligence and Soft Computing*, vol. 2022, Article ID 8104054, 10 pages, 2022.

[110] M. F. Khan, T. M. Ghazal, R. A. Said et al., "An iomt-enabled smart healthcare model to monitor elderly people using

machine learning technique," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 2487759, 10 pages, 2021.

[111] R. A. Said, H. Raza, S. Muneer et al., "Skin cancer detection and classification based on deep learning," in *Proceedings of the 2022 International Conference on Cyber Resilience (ICCR)*, pp. 1–11, Dubai, United Arab Emirates, August 2022.

[112] A. Raheem, S. Muneer, M. Amjad, and H. Raza, "Role of artificial neural networks in breast cancer detection," *International Journal of Computational and Innovative Sciences*, vol. 1, no. 4, pp. 9–19, 2022.

[113] H. Raza, M. Amjad, and S. Muneer, "IoT based cyber-physical system in automobile devices with dew computing architecture," *Journal of NCBAE*, vol. 1, no. 1, 2022.

[114] N. S. Naz, M. A. Khan, S. Abbas, A. Ather, and S. Saqib, "Intelligent routing between capsules empowered with deep extreme machine learning technique," *SN Applied Sciences*, vol. 2, no. 1, p. 108, 2020.

[115] M. A. Khan, S. Abbas, A. Atta et al., "Intelligent cloud based heart disease prediction system empowered with supervised machine learning," 2020, https://www.techscience.com/cmc/v65n1/39558.

[116] N. Ali, A. Ahmed, L. Anum et al., "Modelling supply chain information collaboration empowered with machine learning technique," *Intelligent Automation & Soft Computing*, vol. 30, no. 1, 2021.

[117] M. M. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, and J. Li, "A few-shot deep learning approach for improved intrusion detection," in *Proceeedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pp. 456–462, New York, NY, USA, June 2017.

[118] S. Muneer and M. A. Rasool, "AA systematic review: explainable Artificial Intelligence (XAI) based disease prediction," *International Journal of Advanced Sciences and Computing*, vol. 1, no. 1, pp. 1–6, 2022.

[119] A. Howard, M. Sandler, G. Chu et al., "Searching for mobilenetv3," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, Venice, Italy, July 2019.

[120] M. Tan and Q. Le, "Efficientnet: rethinking model scaling for convolutional neural networks," in *Proceedings of the International Conference on Machine Learning*, pp. 6105–6114, Himachal Pradesh, India, June 2019.

[121] M. Tan, B. Chen, R. Pang et al., "Mnasnet: platform-aware neural architecture search for mobile," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Washington, DC, USA, August 2019.

[122] J. Liu, N. Inkawhich, O. Nina et al., "Ntire 2021 multimodal aerial view object classification challenge," in *Proceedings of the 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 588–595, Nashville, TN, USA, July 2021.

[123] A. Ignatov, A. Romero, H. Kim, and T. Radu, "Real-time video super-resolution on smartphones with deep learning, mobile ai 2021 challenge: report," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 2535–2544, Nashville, TN, USA, May 2021.

[124] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations," *Computer Networks*, vol. 184, Article ID 107679, 2021.