The Intrusion Detection System by Deep Learning Methods: Issues and Challenges

Ola Surakhi
Department of Computer Science
Middle East University,
Jordan
osurakhi@meu.edu.jo

Antonio García
Department of Telematics and Communications
University of Granada,
Spain
amorag@ugr.es

Mohammed Jamoos
Department of Telematics and Communications
University of Granada,
Spain
jamoos@staff.alquds.edu

Mohammad Alkhanafseh
Department of Computer Science
Birzeit University,
Palestine
malkhanafseh@birzeit.edu

Abstract**:** *Intrusion Detection Systems (IDS) are one of the major research application problems in the computer security domain. With the increasing number of advanced network attacks, the improvement of the traditional IDS techniques become a challenge. Efficient ways and methods of identifying, protecting, and analyzing data are needed. In this paper, a comprehensive survey on the application of Machine Learning (ML) and Deep Learning (DL) methods on the IDS to increase detection accuracy and reduce error rate is proposed. The recent research papers that have been published between 2018 and 2021 in the area of applying ML and DL in the IDS are analyzed and summarized. Four main analyzing aspects are presented as follows: (1) IDS concepts and taxonomy. (2) The strength and weaknesses of ML and DL methods. (3) IDS benchmark datasets. (4) Comprehensive review of the most recent articles that used ML and DL to improve IDS with highlighting the strengths and weaknesses of each work. Based on the analysis of the literature review papers, a framework for the application of ML and DL in the IDS is proposed. Finally, the current limitations are discussed and future research directions are provided*.

Keywords**:** *Artificial intelligence, dataset, deep learning, intrusion detection, machine learning, security.*

Received April 2, 2022; accepted April 28, 2022
https://doi.org/10.34028/iajit/19/3A/10

1. Introduction

Cyber security became an important field of research with the rapid development of internet and network technologies. It includes antivirus software, firewalls, and an Intrusion Detection System (IDS) to protect the system from internal and external attacks [59]. IDS is a detection system that monitors the network traffic for any suspicious behaviour to provide desired security in a network [26].

The IDS idea was proposed first by Jim Anderson in 1980 [6]. Since then, many IDS were proposed to satisfy the need for networks security. However, the large expansion of the network size and the increasing number of applications that are handled by network nodes resulted in a huge amount of data that are shared and transferred over the network, which caused a serious harmful attack and raised the need to improve the security of the network. Thus, many researchers paid attention to improving IDS by increasing the detection rate of new or old attacks and reducing the False Alarm Rate (FAR).

There are many classification methods used in the literature for the task of classifying anomaly data in the IDS. some of these methods include decision trees, rule-based systems, support vector machines, naïve Bayes, and nearest-neighbours.

Recently, researchers began to use machine learning methods to improve IDS in detecting malicious attacks. Machine Learning (ML) is a subset of the Artificial Intelligence (AI) field that can efficiently extract useful information from a given dataset [35]. ML methods can be used in the IDS to identify and classify the different types of attacks from a huge amount of data. Deep Learning (DL) is a subset of ML methods that are better in dealing with big data. DL has multiple hidden layers which provide them with the ability to learn complex feature representation from row data and achieve outstanding performance.

The purpose of this paper is to provide a comprehensive survey about the recent trend in the development of IDS based ML and DL methods. In this paper, we selected the representative research papers published from 2018 to 2021 that reflect the progress of the IDS based ML and DL methods. The main contributions of this paper are 3-folds:

1. It summarized the benchmark datasets of IDS that are used repeatedly by researchers to evaluate the performance of their proposed methodology.

2. It selected the recent journal articles that are published from 2018 to 2021 and applied ML and DL in IDS, we reviewed the methodology, evaluation metrics and datasets used by each one.
3. It analyzed the strength and weaknesses of each article. Lastly, and based on the observations, we provided the results and challenges in IDS based ML and DL methods for future direction research in the same domain.

Several research studies (surveys) have been conducted in the literature for those who used ML and DL for IDS [2, 30, 45]. These surveys focused on the classification of ML methods, which can be useful for the research scope of ML technology. This survey differed from other previous surveys in two aspects:

1. We studied the most benchmark datasets used by researchers to improve IDS while highlighting the strength and weaknesses of each dataset and how they can affect the performance of IDS.
2. We followed a systematic overview of the research paper articles and focused on the recent articles that have been published recently. We analysed these articles according to the ML or DL methods, evaluation metrics, datasets used and the results conducted by each one. Then, a summary of the strengths and weaknesses of each method used to improve IDS was given. This survey can answer the following questions:

1. Which dataset represents different attacks?
2. What type of machine learning algorithm can provide a highly accurate detection rate?
3. What are the challenges that may face researchers who are interested in improving IDS?

A new framework for the application of ML/DL methods on the IDS is proposed. The framework consists of two main phases: the first phase illustrates the dataset handling and the second one gives the ML/DL model development for the IDS.

The rest of this paper is organized as follows: section 2 provides the basic concepts about IDS. section 3 introduces the ML and DL methods used to improve IDS with the strength and weaknesses of each method. The evaluation metrics and benchmark datasets are summarized in section 4. section 5 introduces the frequent research papers that used ML and DL in IDS, their method, evaluation metrics, and datasets. section 6 analyses the research paper and provides the challenges of IDS based ML and DL design. Finally, section 7 presents conclusions and future research scope.

2. IDS: Concepts and Taxonomy

This section explains the concepts of IDS and provides detailed information about its taxonomy.

2.1. IDS Concept

In the IDS, intrusion refers to any attempt from unauthorized users to access the information in the computer network systems to influence its integrity, confidentiality or availability [15, 37]. Detection is a security method that is deployed to catch such illegal activities. Therefore, IDS is the security system that is monitors the network traffic and host constantly to detect any security violations or suspicious behavior. IDS generates alerts for any intrusion detection and then responds to this behaviour [10]. The IDSs are usually deployed near the network nodes in order to monitor network hosts and to let the network traffic pass through the system.

2.1. IDS Taxonomy

IDS is classified either by the detection method used in the IDS or by the deployment method used in IDS. The IDS is subclassified into two groups based on detection methods; anomaly detection based IDS and signature-based IDS. And from the deployment method-based IDS perspective, the IDS is subclassified as host-based IDS and network-based IDS. The details are given in the next subsections.

a) Detection Method based IDS

The detection method based IDS is subdivided into two main groups: Signature-based IDS (SIDS) and Anomaly-based IDS (AIDS). SIDS works based on the idea of saving a signature for each attack pattern in the database and comparing any suspicious data patterns with these stored signatures for any signature attack detection [3]. For any known attack, the SIDS is able to detect it with high accuracy. However, for unknown or new attack, the system fails to identify the attack pattern as it cannot be matched it with any of the stored signature patterns in the database. Another disadvantage for SIDS is that it is resource consuming system for large signature database, the comparison between stored signatures and data packet may increase time complexity which reduces overall performance [62].

AIDS, which is also called behaviour-based IDS, depends on creating a profile for each normal activity and defines the abnormal activity as the degree of deviation from the normal activity profile [31]. Despite the ability of AIDS in detecting abnormal attacks in the network, it suffers from a high False Alarm Rate (FAR) as it cannot determine the boundaries between normal and abnormal attack profiles accurately [7].

b) Deployment Method based IDS

The IDS is either Host-based-IDS (HIDS) or Network-based-IDS (NIDS) [63]. In the HIDS, the IDS is deployed separately on every single host in the network. It is responsible on monitoring the activities of this host and detecting any suspicious behavior. The main disadvantage of this type is the extra-processing overhead that results from the deployment of IDS at each host in the network which reduces the overall

performance of the system [19]. NIDS is deployed over the network and is responsible for monitoring the traffic in the network to detect any attack that passes through the network in a real-time. NIDS is deployed in the major hosts in the network, and it can be applied in different operating system environments. A summary of the main advantages and disadvantages of each type of IDS is given in Table 1.

Table 1. Advantages and disadvantages of different IDS.

IDS	Advantages	Disadvantages
SIDS	High detection accuracy.	Detect only known attacks, less performance with big database.
AIDS	Strong generalizability with the ability to detect unknown attacks.	High FAR.
HIDS	Can detect the behaviour of the significant object.	Difficult to deploy, depends on the operating system of every host, depends on the host resources.
NIDS	Can be applied in the different operating system environments, can detect an attack in real time.	Monitors only the traffic path of the network.

3. ML and DL Algorithms for IDS

Machine learning can be classified into two main groups: supervised and unsupervised learning. Supervised learning depends on data label to extract useful information. Classification is the one of the main tasks in supervised learning. Unsupervised learning extracts useful information from unlabeled data. This section presents a summary of machine learning methods used to propose IDS in the reviewed articles.

In general, machine learning methods can be classified into two main groups:

1. Traditional machine learning algorithms
2. Deep learning algorithms.

The traditional machine learning algorithms are also called Shallow learning include many methods that have been used to improve IDS. It includes Artificial Neural Network (ANN), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and more.

The DL algorithms include many layers in the architecture to the characteristics of the data and learn more features on their own. Some of the deep learning methods include DNN, RNN, CNN, Generative Adversarial Networks (GAN), and more. More details about each method used by the collected literature review researches used in this paper with the strengths and weaknesses for each method are summarized in Tables 2 and 3.

Table 2. Shallow learning methods.

Method	Description	Strength	Weakness
Decision Tree (DT)	A supervised methods which is used for both classification and regression problems. Its structure consists of nodes, branches and leaf. Each node represents a feature, the branch is a rule and the leaf is the possible class. DT automatically build the tree by selecting the best features, then apply a pruning operation to remove irrelevant branches [8]. RF and XGBoost are more advanced learning algorithms that are made of multiple DT.	Selects features automatically	Results of classification skew to the majority class.
Multi-Layer Perceptron (MLP)	It is a feed forward neural network that consists of three sequential layers: input, hidden and output. The hidden layer processes data from input layer and pass it to the hidden layer [66].	Works with non-linear data.	Time consuming with local optima problem.
K-Nearest Neighbour (KNN)	It is a machine learning classifier that predicts the class of a data based on the idea of feature similarity. KNN identifies a sample based on its distance from the neighbours. The parameter *k* effects on KNN performance [68].	Works with non-linear data and robust to noise.	Sensitive to the parameter *k*.
Naïve Bayes	Bayesian classifier is based on the assumption of conditional probability for different classed. The sample of data is then classified to the maximum probability class [33].	Can learn incrementally with strong deal with noise.	Does not perform well in real data.
Ensemble	It is a combination of more than learning algorithm where each has its strength and weakness then a voting is performed to obtain the final result [56].	Perform better than single classifier.	Time consuming for big datasets.

Table 3. Deep learning methods.

Method	Description	Strength	Weakness
Recurrent Neural Networks (RNN)	RNNs is a deep neural network that consists of input layer, output layer and hidden layer with one or more feedback loops. The hidden layer contains states and memory block to store, remember and process past data for a long period of time [55].	RNN remember the previous information and use them to predict future.	Performance depends on the time lag value.
Convolutional Neural Networks (CNN)	CNN is a deep learning algorithm that consists of convolutional and pooling layers. CNN is designed to operate with multi-dimensional image data [44].	Powerful in detecting and extracting complex features.	Performance depends on the kernel size. Time consuming for large data.
Auto encoder	A specific type of neural network with three components: encoder, code and decoder. The encoder compresses the data to produce code and decoder reconstruct the input using this code [43].	Reduce dimensionality of the data.	Time consuming for large data.
Generative Adversarial Networks (GAN)	GAN is a generative modelling that uses deep learning algorithm such as CNN to extract patterns from input data and use it to generate new samples [39].	Learn the internal representation of the data.	Optimizing the network requires many trial-and-error attempts.

DL methods are robust and powerful in the learning ability because of its internal structure with multi hidden layers that enable the model to extract a useful feature from a complex and huge dataset. The performance of DL methods is superior to ML methods. On the other hand, there are some differences between DL and ML

methods that make the choice of which method to use dependable on the application domain, the resources and the expert knowledge and experience. These differences can be summarized as follows:

- Running time: because of multi hidden layer architecture, DL methods consume more running time for learning.
- Hyperparameters tuning: DL methods contain more hyperparameters that are need to be tunned efficiently before training the model.
- Learning capacity: DL methods are robust and can learn from a large volume of data because of its complex structure.
- Interpretability: DL methods are black-box models that generate the output without an interpretation.

4. Evaluation Metrics and Benchmark Datasets

The evaluation metrics that are used by most of researchers to evaluate their proposed work are illustrated in this section. Then, the benchmark IDS dataset is summarized and analyzed in the next subsection.

4.1. Evaluation Metrics

An explanation of the most commonly used evaluation metrics that are used for measuring the performance of machine learning classification problems is illustrated here.

- Confusion Matrix: It is a two-dimensional array (actual and predicted) that gives information about the performance of machine learning classification model with four different combinations as follows:

1. True Positive (TP): The data instances that are true (normal data in IDS) in the dataset and are predicted correctly.
2. False Positive (FP): The data instances that are false (attack in IDS) in the dataset and are predicted correctly.
3. True Negative (TN): The data instances that are true in the dataset and are predicted wrongly.
4. False Negative (FN): The data instances that are false in the dataset and are predicted wrongly.

- Accuracy: It is the ratio of the total number of correct predicted instances to the total number of all instances. It is defined as follows:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (1)$$

- Precision: It is the ratio of correctly predicted instances to the all instances that are predicted as a true value. It is defined as follows:

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

- Recall: It is the ratio of correctly predicted instances to the total number of instances that are actually true. It is defined as follows:

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

- F-Score: It is a statistical measure to examine the accuracy of the model by considering both precision and recall. It is defined as follows:

$$F\text{-}Score = 2\left(\frac{Precision\ x\ Recall}{Precision + Recall}\right) \quad (4)$$

- False Negative Rate: It is the ratio of wrongly predicted instances to the all instances that are true. It is defined as follows:

$$False\ Negative\ Rate = \frac{FP}{FP + TN} \quad (5)$$

- True Negative Rate: It is the ratio of the instances that are correctly predicted as false to the total number of instances that are true. It is defined as follows:

$$True\ Negative\ Rate = \frac{TN}{TN + FP} \quad (6)$$

- Roc Curve: It is a graphical plot that gives information about classification performance at various threshold settings. It tells how much the model can distinguish between classes.

4.2. Benchmark Datasets for IDS

The experiments in any research of IDS domain require a network-based data representation. Benchmark datasets are a good choice for the evaluation and comparison between different IDS. The dataset contains a labelled data (for supervised learning) which can be classified to either an attack data or normal data. There are many representative datasets for the IDS. This section provides a literature survey of the existing IDS benchmark datasets that are used in the literature research papers in this survey with the properties for each one. The information is tabulated in Table 4 and 5. Table 5 gives the properties of each dataset and Table 6 provides the type of attacks that can be defined by each dataset.

Table 4. Benchmark datasets for IDS.

Dataset	Year	Data Label	Data Balance	Properties
ADFA-LD [46]	2013	Yes	No	Is a HIDS dataset. Contains information about the system-calls where each system-call has a unique number.
ADFA-WD [16]	2014	Yes	No	Is a HIDS dataset. Contains information about Windows-based vulnerability-oriented zero-day attacks.
BoT-IoT [25]	2018	Yes	No	Contains information about IoT network traffic features.
CICIDS2017 [48]	2017	Yes	NO	Contains information of network traffic in both packet-based and bidirectional data flow-based.
CSE-CIC-IDS2018 [9]	2018	Yes	No	Is an AIDS dataset. Contains scenarios for seven different attacks.
KDD-Cup 99 [49]	1998	Yes	NO	Contains information about TCP connections and number of failed logins. It is not a standard packet nor data flow-based. Contains large amount of redundancy.
NSL-KDD [60]	1998	Yes	NO	Enhances KDD-Cup 99 by removing duplicate data. Contains the same information about TCP and number of logins failed information.
UNSW-NB15 [36]	2015	Yes	NO	Contains information in packet-based format and in flow-based format.
WSN-DS [4]	2016	Yes	No	Contains information about different DoS attacks in the WSN environment.

Table 5. Attacks type for each dataset for IDS.

Dataset	Attack's type
ADFA-LD	Hydra-FTP, Hydra-SSH, Adduser, Java-Meterpreter, Meterpreter, Webshell
ADFA-WD	password brute-force, java-based meterpreter, add latest superuser, C100 Webshell and linux meterpreter payload
BoT-IoT	BENIGN, Service scanning, OS Fingerprinting, DDoS TCP, DDoS UDP, DDoS HTTP, DoS TCP, DoS UDP, DoS HTTP, Keylogging, Data theft
CICIDS2017	a botnet (Ares), cross-site-scripting, DoS (executed through Hulk, GoldenEye, Slowloris, and Slowhttptest), DDoS (executed through LOIC), heartbleed, infiltration, SSH brute force, SQL injection
CSE-CIC-IDS2018	Heartbleed, Brute-force, DoS attack, Web attack, Infiltration attack, Botnet attack, DDoS attack, and Heartleech
KDD-Cup 99	DoS, privilege escalation (remote-to-local and user-to-root), probing
NSL-KDD	DoS, privilege escalation (remote-to-local and user-to-root), probing
UNSW-NB15	backdoors, DoS, exploits, fuzzers, generic, port scans, reconnaissance, shellcode, spam, worms
WSN-DS	Four types of Denial of Service (DoS) attacks: Blackhole, Grayhole, Flooding, and Scheduling attacks

5. Deep Learning Methods for Intrusion Detection System

In this section, a set of recent related works that apply machine learning methods to the IDS are summarized and analysed. The literature review papers are collected for the years from 2018 to 2021 with a total of 30 research papers. Table 7 identifies each work by answering the following questions:

1. What are the machine learning methods used by each work to improve IDS?
2. Which datasets are used by each work to examine the performance and approve the results?
3. What are the metrics used for evaluation purposes?
4. What are the contributions of each proposed works?

The publisher's name and the publication year of each research paper are mentioned also in the table. Each research paper is then analysed and the advantages and disadvantages are listed in the next section. Finally, we identified the future scope of the intrusion detection system based on machine learning methods research by highlighting the challenges of the design of an efficient model in terms of accuracy, training time and security issues.

5.1. Strength and Weakness of the Proposed Literature Works for IDS

This section investigates the previous related works by listing the strength and weaknesses points of each work.

5.2. Discussion and Challenges

A. *Results*:

1. The use of state-of-the-art deep learning methods is more efficient than traditional machine learning methods and has led to better cyber security strategies that perform better in data analysis. The increase in the size of the dataset led to less accuracy in the multi-class classification attacks. Traditional machine learning methods become incompatible with high-dimensionality learning data. Deep learning methods are powerful due to its primary characteristics:
   - Hierarchical feature representations
   - Long-term dependency learning.

This result can be noticed from the related works that used deep learning methods and compared their performance with traditional machine learning methods [6, 26, 35].

2. IoT architecture consists of several layers. The network layer is responsible for transferring packet data between hosts. It is vulnerable to many security threats. Many security frameworks have been proposed in the literature to address security issues [7, 45]. Most of these frameworks require the consideration of storage as well as the computational power of IoT devices. A combination of IDS with deep learning algorithms can offer an intelligent solution to address security threats and prevent attacks in the IoT environments by keeping in mind the shortcoming of IoT devices.
3. New security solutions such as Blockchain technology can be integrated with deep learning methods and IDS in order to enhance security and

offer confidentiality, trust, integrity, privacy, etc. [45].

4. Feature selection technique can be used by deep learning methods to enhance the performance of IDS. The features are important for the prediction and their importance in the whole datasets are not equal. The complexity of training time can be reduced by using the feature selection technique and efficient work can be proposed with high accuracy at the same time [8, 15].
5. Data balancing is an important issue to be taken into consideration when dealing with datasets of intrusion detection. There are many powerful techniques for data sampling.
6. Testing the performance of IDS based machine learning algorithm is done by finding the outcome of different statistical metrics. The mostly used metrics for that are accuracy, precision, F1-score and recall [6, 10, 45, 59].
7. A good dataset plays a vital role in model training. The up-to-date dataset contains more information about new attacks. The problem of unbalancing in the dataset can be solved by oversampling techniques to improve the class distribution of the dataset. The GAN method is used in the literature that captures the real data distribution and then generate a specific type of data (attack) to reduce imbalance [63].
8. Ensemble learning aims to find the best set of classifiers and the best way to combine them to improve the overall performance of classification. It can be a good choice to deal with big data size then can be divided into small sets where each set can be trained by a single classifier.
9. The performance of ML and DL methods in IDS is the superior performance of other traditional methods. Most of the related works that used ML and DL methods in the IDS achieved a high accuracy rate and improve the generalization ability.
10. In general, the use of deep learning methods is more efficient than traditional machine learning methods, while the performance varies between them depending on the type of the model and the optimization techniques used to optimize it.

B. *Challenges*:

1. Designing a secure system based on the use of deep learning methods does not necessarily guarantee all the security issues like integrity, trust, transparency, confidence, etc. ML and DL methods have been used previously in several security applications [52]. The IDS aims to prevent cyber security from different attacks while deep learning methods play an important role in supporting IDS with solutions to successfully secure the system from known and unknown threats efficiently in terms of accuracy, training time, etc. Choosing the related aspect to be achieved in the security system depends on the domain application, quality of data, the method used, and the data engineer's experience [54].
2. Each model from the previous studies has its own strength and weakness, and has been evaluated over one or two datasets which make it suitable for a particular type of attack. The models are not generalizable due to outdated datasets.
3. A good dataset plays a vital role in model training. The IDS data obtained from a real environment regularly contains a huge amount of normal behavior with a minority of attacks behavior data. Thus, the number of attacks is imbalanced. The imbalanced dataset affects the model performance and will result in poor recognition of attacks as the model will pay attention to normal behaviors. Therefore, the imbalanced dataset of IDS became a major challenge. The general technique to increase minority in the dataset is oversampling.
4. Most of the previous research relies on the old dataset to evaluate the performance of the proposed system. The old datasets contain old traffic and do not represent a real and recent attack scenario. Therefore, using recent datasets to evaluate IDS would be more efficient.
5. An efficient, dynamic and lightweight model design is a challenge for the IDS of IoT environment where the memory storage and battery lifetime are big issues to be considered in the IoT devices.
6. The large volume of data represents a big challenge in the IDS design. The data are generated from different resources. Therefore, structured, unstructured, and semi-structured are included. This requires an efficient technique to analyze and manage various large quantities of data.
7. The datasets require passing through a set of pre-processing operations before providing it in any deep learning classifier model [53]. Changing the scale and distribution of input data may only be useful for the model that depends on the calculations of weighted sums, such as the neural network. The scale method may result in sensitive input data that can change the model results.
8. Tunning the neural Network Parameters is an (NP) problem that may require the run of several attempts in order to find the optimal value of each parameter that optimize the model performance [14]. There is no optimal method to be used for that. Most of the previous research depends on the trial-and-error method which is time-consuming and may exhaust resources.
9. Most of the literature research papers that are published in the ML and DL based IDS domain focused on the improvement of NIDS. Few types of research focused on the other types of IDS

(HIDS, SIDS, and AIDS).

10. Most of the dataset attributes are not clearly described in a way that can be easily understood by the researchers [1]. A well-described input and output attributes of the dataset are critical and helpful in the designing of IDS to achieve meaningful progress in performance.

c) IDS Based ML/DL Methods Framework

Based on the analysis of the previous literature research works, a framework for the application of ML/DL methods on the IDS is proposed. The framework shows the pipeline of the IDS works divided into two main phases: The data preparation phase and the model design phase. In the data preparation phase, the IDS dataset is chosen and pass through a set of pre-processing steps. In the model design phase, a ML/DL method is used to be applied in the classification task of IDS. The aim of using ML/DL method is to increase detection accuracy and reduce error rate. The details of the framework phases are as follows:

In the data preparation phase, cleaning, normalization, and transformation are the main steps that convert the dataset into a consistent form with no missing values. Normalization is an important step that converts data into a suitable range. The dataset is then split into training, testing, and validation sets.

In the model design phase, the type of ML/DL method to be used for the classification task is chosen. As summarized in the literature, there are many methods that can be used for this task. The choice of the best method depends on the application domain of IDS. The tuning of ML/DL model is essential to configure its setting to the best that guarantees the best results and accuracy. Figure 1. Shows the pipeline IDS phases.

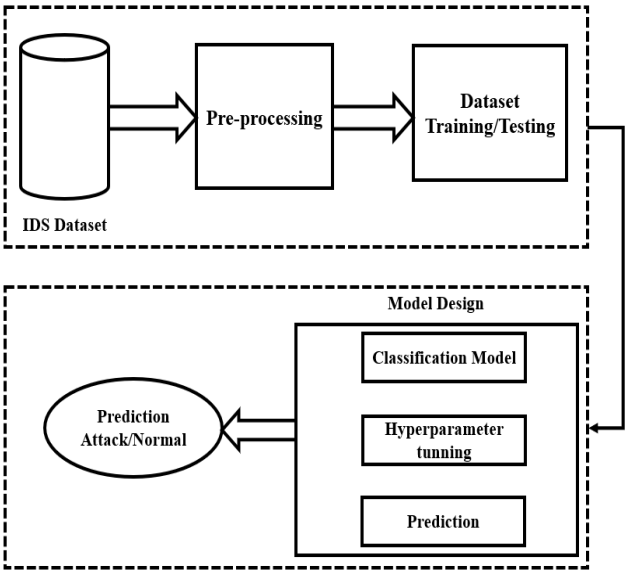

Figure 1. IDS based ML/DL methods framework.

6. Conclusions and Future Scope

This paper gives a comprehensive survey of the recent trends in the use of ML and DL methods to improve the performance of IDS. The recent typical studies which are published from 2018 to 2021 are summarized and analysed. Several machine learning and deep learning techniques have been used in the literature to improve the performance of IDS in terms of accuracy. The paper highlights the strength and weaknesses of each ML and DL method. The authors of selected articles in this survey evaluated the conducted results of their works over the use of different benchmark IDS datasets and different evaluation metrics. This detailed investigation was placed in the challenges that may face researchers in the future for the development of IDS based on the following aspects:

1. Benchmark's dataset.
2. ML and DL method.
3. IDS environment.

Based on the analysis of the previous studies, the future scope of the development of IDS based ML and DL methods can be summarized as follows:

- Efficient dataset for IDS can be either modified by using recent generation methods such as GAN technology or it can be developed by real-time monitoring of IDS in any network environment.
- DL methods improve the performance of detection attacks in IDS. More development in this area can be done by using the state-of-the-art DL methods or by developing a hybrid approach that combines different DL methods to enhance performance.
- More research is needed on the other IDS system such as SIDS, AIDS, and HIDS.
- A combination between DL method and recent security technology such as Blockchain can improve IDS in terms of accuracy and security issues. More research in this area are highly recommended.

Table 6. Summary of related work research papers.

Related Work (Citation)	Machine Learning Method	Dataset	Accuracy Metrics	Year	Publisher	Results
Alzahrani, and Alenazi [5]	DT, RF and XGBoost	NSL-KDD	Accuracy, Precision, Recall and F-Score	2021	MDPI	Accuracy of 95.95%
Zhong, *et al*. [69]	GRU, Text-CNN and MLP	KDD-Cup 99 and ADFA-LD	F-Score	2021	MDPI	The proposed method achieved higher F1-score than traditional methods
Mahbooba, *et al*. [32]	DT, KNN, RF, NB and LSTM, GRU,	WSN-DS and KDD-Cup 99	Accuracy, precision, recall, and F-Score	2021	Hindawi	The using of AI-solutions in IDS can enhance trust and accuracy
Khan [22]	CNN and RNN	CSE-CIC-IDS2018	Accuracy, TP, TN, FP, FN	2021	MDPI	The proposed model achieved high malicious attack detection rate accuracy of up to 97.75%
Yao, *et al*. [65]	LSTM and CNN	KDD-Cup 99 and NSL-KDD	Accuracy, Precision, DR, F-score and FPR	2021	MDPI	The experimental results demonstrated that the performance of the proposed model was superior to those of a single DL component and models proposed in previous studies.
Dutta, *et al*. [12]	Classical AutoEncoder and Deep Neural Network	UNSW-NB15	Precision, recall, accuracy, F-score, False Positive Rate (FPR), ROC curve	2020	Springer International Publishing	The proposed model increases accuracy and improves generalization ability.
Liang, *et al*. [28]	ANN	NSL-KDD	Accuracy, precision, recall and F-Score	2020	MDPI	The using of deep learning methods enhances IDS of IoT device.
Mebawondua, *et al*. [34]	MLP	UNSW-NB15	Accuracy and False Alarm Rate	2020	Elseveir	The proposed method is suitable for real-time IDS with accuracy of 76.96%
Liu and Zhang [29]	CNN	KDD-CUP 99 and NSL-KDD	Accuracy, Precision, Recall, F-Score and Error Rate	2020	Hindawi	The proposed model improves the accuracy and check rate, reduces the false positive rate.
Tang, *et al*. [58]	SAE and DNN	NSL-KDD	Accuracy, Precision, Recall and F-Score	2020	MDPI	Accuracy 87.74% and 82.14% (binary-classification and multi-classification)
SU, *et al*. [50]	LSTM and CNN	NSL-KDD	Accuracy, TPR and FPR	2020	IEEE	Accuracy of 84.25%
Sumaiya, *et al*. [51]	ANN	NSL-KDD and UNSW-NB15	Accuracy and Specificity	2020	WILEY	Accuracy of 97.49 and Specificity of 99.31for NSL-KDD Accuracy of 96.44 and Specificity of 98.4 for UNSW-NB
Kim, *et al*. [24]	CNN	KDD-CUP 99 and CSE-CIC-IDS2018	Accuracy, Precision, Recall and F1-score	2020	MDPI	Accuracy of 99% for KDD-CUP 99 and 91.5% for CIC-IDS2018
Susilo and Sari [57]	RF, SVM, CNN and MLP	BoT-IoT	Accuracy and Precision	2020	MDPI	RF and CNN increases accuracy.
ZHANG, *et al*. [67]	CWGAN and CSSAE	NSL-KDD and UNSW-NB15	Accuracy and F-Score	2020	IEEE	The proposed model improves the detection accuracy of minority attacks and unknown attacks
Kaplan and Alptekin [20]	BiGAN	KDD-CUP 99	Accuracy, Precision, Recall and F-Score	2020	Elseveir	The proposed approaches increased the performance of BiGAN on anomaly detection task.
Patil, *et al*. [41]	BiGAN	KDD-CUP 99	Accuracy, Precision, Recall and F1-score	2020	Wiley	An improvement in the performance and training time is achieved.
Shahriar, *et al*. [47]	GAN	NSL-KDD	Precision, Recall, F1-score and Confusion matrix	2020	IEEE	GAN improves performance by balancing the imbalanced dataset and proposed model improve accuracy
JAN, *et al*. [18]	SVM	Simulation Dataset of 100 normal samples and 100 intruded samples according to Poisson Distribution and CICIDS2017	Accuracy, TPR, TNR, FPR and FNR	2019	IEEE	The SVM-based IDS can perform satisfactorily in detection of attacks
Khan, *et al*. [21]	SAE	KDD-CUP 99 and UNSW-NB15	Accuracy, Precision, Recall, F-Score and FAR	2019	IEEE	Recognition rate of 99.996% for KDD-CUP 99 and 89.134% for UNSW-NB15
Hajimirzaei and Navimipour [17]	MLP, Heuristic Algorithm and Fuzzy Clustering Algorithm	NSL-KDD	MAE, RMSE, and the kappa statistic	2019	Elseveir	The proposed method shows a 2.23% improvement in correctly-classified instances and a decrease in incorrectly classified instances
Faker and Dogdu [13]	DNN, RF and GBT	UNSW-NB15 and CICIDS2017	Accuracy	2019	ACM	The results show a high accuracy with DNN for binary and multiclass classification.

Xiao and Xiao [64]	ResNets	NSL-KDD	Accuracy, recall and F-Score	2019	MDPI	The experimental results show that the IDS based on the S-ResNet achieves better Performance in terms of accuracy and recall compared to the existing IDSs.
Khater, *et al*. [23]	MLP	ADFA-LD and ADFA-WD	Accuracy, recall and F-Score	2019	MDPI	94% Accuracy, 95% Recall, and 92% F1-Measure in ADFA-LD and 74% Accuracy, 74% Recall, and 74% F1-Measure in ADFA-WD
Thamilarasu and Chawla [61]	DNN	dataset of 5 million network transactions from the six sensors distributed in a smart home network simulation	Precision, Recall, F - Score	2019	MDPI	The proposed intrusion-detection system can detect real-world intrusions effectively.
Peng, *et al*. [42]	RBM	KDD-CUP 99	Accuracy, FPR	2019	IEEE	The results show that the proposed method has a significant improvement over the traditional machine learning accuracy.
Ding and Zhai [11]	CNN	NSL-KDD	Accuracy, TPR and FPR	2018	ACM	The experimental results show that the performance of proposed IDS model is superior in multi-class classification to the performance of models based on traditional machine learning methods.
Pham, *et al*. [40]	Bagging and Boosting ensemble	NSL-KDD		2018	ACM	The bagging ensemble model produced the best performance in terms of both classification accuracy and FAR when working with the subset of 35 selected features.
Nguyen, *et al*. [38]	CNN	KDD Cup 99	Accuracy	2018	ACM	Accuracy of 99.87%
Li and Qin [27]	LSTM	NSL_KDD		2018	IEEE	Proposed model outperforms most of the standard classifier and solve anomaly detection

Table 7. Strength and weakness of each related works.

Related Work (Citation)	**Strength**	**Weakness**
Alzahrani, and Alenazi [5]	The proposed model is investigated over multi-class classification.	The proposed model used an older dataset for evaluation, more benchmark cyber security datasets can be used to achieve generalization. Traditional machine learning classification methods are used instead of state-of-the-art deep learning methods.
Zhong, *et al*. [69]	Deep learning methods (state-of-the-art) are used to design the model.	The structure of GRU is complex and computationally expensive. The integrity of the data was limited.
Mahbooba, *et al*. [32]	The proposed model investigated how to enhance the trust in IDS.	The performance-based comparison shows no superiority of one model (traditional machine learning and deep learning) among the chosen datasets.
Khan [22]	The problem of class imbalanced was handled.	The proposed model was tested on a single dataset.
Yao, *et al*. [65]	The proposed model guarantees AMI communication security	The detection effect of the U2R attack was not ideal
Dutta, *et al*. [12]	Feature engineering method was used to increase performance of IDS.	The proposed model did not address the problem of the classification of multiple attack families.
Liang, *et al*. [28]	Applied new technology, Blockchain and multi-agent for IDS.	Computational power problem was not considered in the system design. Testing the performance was done over an old dataset.
Mebawondua, *et al*. [34]	Using Gain ratio technique for feature selection and MLP for classification proposed a lightweight IDS.	The study fails to test the performance of the model using different number of attributes
Liu and Zhang [29]	Applied a multi-class classification.	Old datasets were used for experimental evaluations.
Tang, *et al*. [58]	The proposed model deals with high dimensionality data.	Old dataset was used for experimental evaluations.
SU, *et al*. [50]	The proposed model can capture features of network traffic more comprehensively.	Does not evaluate the performance in terms of time complexity.
Sumaiya, *et al*. [51]	The integration of CFS and ANN increases accuracy.	Time consumed is high.
Kim, *et al*. [24]	New types of data were used to train the model by generating a set of images from existing numerical samples in the datasets.	Increasing number of convolutional layers increases complexity of the training.
Susilo and Sari [57]	The authors investigated the model hyperparameters (number of epochs and batch size). Batch size speed up the calculation process.	An old dataset was used to evaluate the performance.
ZHANG, *et al*. [67]	The proposed model solves the imbalance problem in the dataset by using GAN technology.	An old dataset was used to evaluate the performance.
Kaplan and Alptekin [20]	The dependency between generators and discriminators is reduced to force generator to produce more reliable data and improve the performance.	The proposed approach only considers binary classification of attacks while anomaly detection requires multi-class classification.
Patil, *et al*. [41]	The authors investigated the importance of feature reduction in improving the overall performance.	An old dataset was used to evaluate the performance.

Shahriar, *et al*. [47]	The proposed model solves the imbalance problem in the dataset by using GAN technology.	The proposed model was time consuming.
JAN, *et al*. [18]	The lightweight Ness measures of proposed algorithm is proven in terms of CPU time execution.	One type of attacks is investigated in the proposed work.
Khan, *et al*. [21]	The proposed model learns the feature representation to avoid overfitting and increase accuracy. The imbalanced datasets were treated in the proposed work.	Less accuracy achieved for UNSW-NB15 dataset with complicated types of attack comparing with KDD-99 dataset.
Hajimirzaei and Navimipour [17]	Proposed new method for IDS in cloud environment that classifies instances correctly.	The addition of two algorithms to ANN was costly.
Faker and Dogdu [13]	The proposed model integrated big data technologies and deep learning techniques to improve IDS.	Better feature selection technique can be used.
Xiao and Xiao [64]	The simplified residual block prevents over-fitting and improves the generalization ability of the model. The imbalanced datasets were treated in the proposed work.	The performance of the proposed model in terms of training time is not mentioned in the work.
Khater, *et al*. [23]	Lightweight intrusion detection model with less computational complexity achieved via n-gram transformation for feature selection.	More efficient state-of-the-art learning algorithms can be used instead of Backpropagation.
Thamilarasu and Chawla [61]	No prior knowledge of captured network payload binaries, traffic signatures, or compromised node address are needed for the proposed approach.	Other types of attacks against the IoT including location dependent attacks are not investigated.
Peng, *et al*. [42]	Deep neural network increases detection rate.	An old dataset was used to evaluate the performance
Ding and Zhai [11]	Using multi-stage feature with CNN improves detection rate.	The FPR of Denial-of-Service attack was not satisfying.
Pham, *et al*. [40]	Ensemble learning improves classification accuracy in IDS.	An old dataset was used to evaluate the performance
Nguyen, *et al*. [38]	An investigation about normalization technique for data input was provided with a comparison between performance of each case.	The proposed model investigated one type of attacks.
Li and Qin [27]	The semantic representation of network data was used with DL LSTM method which improve classification accuracy.	An old dataset was used to evaluate the performance

References

[1] Abubakar A., Chiroma H., Muaz S., and Ila L., "A Review of the Advances in Cyber Security Benchmark Datasets for Evaluating Data-Driven based Intrusion Detection Systems," *in Proceedings of the International Conference on Soft Computing and Software Engineering*, California, pp. 221-227, 2015.

[2] Ahmad Z., Shahid Khan A., Wai Shiang C., Abdullah J., and Ahmad F., "Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, pp. 1-29, 2021.

[3] Ahmim A., Derdour M., and Ferrag M., "An Intrusion Detection System Based on Combining Probability Predictions of a Tree of Classifiers," *International Journal of Communication Systems*, vol. 31, no. 9, pp. 1-17, 2018.

[4] Almomani I., Al-Kasasbeh B., and AL-Akhras M., "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," *Journal of Sensors*, pp. 1-16, 2016.

[5] Alzahrani A. and Alenazi M., "Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks," *Future Internet*, vol. 13, no. 5, pp. 1-18, 2021.

[6] Anderson J., Computer Security Threat Monitoring and Surveillance, Technical Report, James P. Anderson Company, 1980.

[7] Chandola V., Banerjee A., and Kumar V., "Anomaly Detection: a Survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1-58, 2009.

[8] Chary S. and Rama B., "A Survey on Comparative Analysis of Decision Tree Algorithms in Data Mining," *International Journal of Advanced Scientific Technologies, Engineering and Management Sciences*, vol. 3, no. 1, pp. 91-95, 2017.

[9] CSE-CIC-IDS2018, https://www.unb.ca/cic/datasets/ids-2018.html Last Visited, 2022.

[10] Denning D., "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering*, no. 2, pp. 222-232, 1987.

[11] Ding Y. and Zhai Y., "Intrusion Detection System for NSL-KDD Dataset Using Convolutional Neural Networks," *in Proceedings of 2nd International Conference on Computer Science and Artificial Intelligence*, New York, pp. 81-85, 2018.

[12] Dutta V., Chora´s M., Kozik R., and Pawlicki M., "Hybrid Model for Improving the Classification Effectiveness of Network Intrusion Detection," *in Proceeding of the Computational Intelligence in Security for Information Systems Conference*, 2019.

[13] Faker O. and Dogdu E., "Intrusion Detection Using Big Data and Deep Learning Techniques," *in Proceedings of the ACM Southeast Conference*, New York, pp. 86-93, 2019.

[14] Fung P., Zaidan A., Surakhi O., Tarkoma S., Petäjä T., and Hussein T., "Data Imputation in Situ-Measured Particle Size Distributions by Means of Neural Networks," *Atmospheric Measurement Techniques*, vol. 14, no. 8, pp. 5535-5554, 2021.

[15] Garcia-Teodoro P., Diaz-Verdejo J., Maciá-Fernández G., and Vázquez E., "Anomaly-Based Network Intrusion Detection: Techniques Systems and Challenges," *Computers Security*, vol. 28, no. 1-2, pp. 18-28, 2009.

[16] Haider W., Creech G., Xie Y., and Hu J., "Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks," *Future Internet*, vol. 8, no. 3, pp. 1-8, 2016.

[17] Hajimirzaei B. and Navimipour N., "Intrusion Detection for Cloud Computing Using Neural Networks and Artificial Bee Colony Optimization Algorithm," *ICT Express*, vol. 5, no. 1, pp. 56-59, 2019.

[18] Jan S., Ahmed S., Shakhov V., and Koo I., "Toward a Lightweight Intrusion Detection System for the Internet of Things," IEEE Access, vol. 7, pp. 42450-42471, 2019.

[19] Kabiri P. and Ghorbani A. "Research on Intrusion Detection and Response: a Survey," *International Journal of Network Security*, vol. 1, no. 2, pp. 84-102, 2005.

[20] Kaplana M. and Alptekin S. "An Improved Bigan Based Approach for Anomaly Detection," *Procedia Computer Science*, vol. 176, pp. 185-194, 2020.

[21] Khan F., Gumaei A., Derhab A., and Hussain A., "A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection," *IEEE Access*, vol. 7, pp. 30373-30385, 2019.

[22] Khan M., "Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System," *Processes*, vol. 9, no. 5, pp. 1-14, 2021.

[23] Khater B., Abdul Wahab A., Idris M., Hussain M., and Ibrahim A., "A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing," *Applied Sciences*, vol. 9, no. 1, pp. 1-21, 2019.

[24] Kim J., Kim J., Kim H., Shim M., and Choi E., "CNN-Based Network Intrusion Detection against Denial-of-Service Attacks," *Electronics*, vol. 9, no. 6, pp. 1-21, 2020.

[25] Koroniotis N., Moustafa N., Sitnikova E., and Turnbull B., "Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-Iot Dataset," *Future Generation Computer Systems*, vol. 100, pp. 779-796, 2019.

[26] Li J., Qu Y., Chao F., Shum H., Ho E., and Yang L., "Machine Learning Algorithms For Network Intrusion Detection," *AI in Cybersecurity*, pp. 151-179, 2019.

[27] Li Z. and Qin Z., "A Semantic Parsing Based LSTM Model for Intrusion Detection," *in proceedings of International Conference on Neural Information Processing*, Cambodia, pp. 600-609, 2018.

[28] Liang C., Shanmugam B., Azam S., Karim A., Islam A., Zamani M., Kavianpour S., and Idris N., "Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems," *Electronics*, vol. 9, no. 7, pp. 1-27, 2020.

[29] Liu G. and Zhang J., "CNID: Research of Network Intrusion Detection Based on Convolutional Neural Network," *Discrete Dynamics in Nature and Society*, vol. 2020, pp. 1-11, 2020.

[30] Liu H. and Lang B., "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," *Applied Sciences*, vol. 9, no. 20, pp. 1-28, 2019.

[31] Ma W., "Analysis of Anomaly Detection Method for Internet of Things Based on Deep Learning," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, pp. 1-13, 2020.

[32] Mahbooba B., Sahal R, Alosaimi W., and Serrano M., "Trust in Intrusion Detection Systems: an Investigation of Performance Analysis for Machine Learning and Deep Learning Models," *Complexity*, 2021.

[33] Mahmood H., "Network Intrusion Detection System (NIDS) in Cloud Environment based on Hidden Naïve Bayes Multiclass Classifier," *Al-Mustansiriyah Journal of Science*, vol. 28, no. 2, pp. 134-142, 2017.

[34] Mebawondua J., Alowolodub O., Mebawondua J., and Adetunmbi A., "Network Intrusion Detection System Using Supervised Learning Paradigm," *Scientific African*, vol. 9, 2020.

[35] Michie D., Spiegelhalter D., and Taylor C., Machine Learning, Neurall and Statistical Classification, Citeseer, 1994.

[36] Moustafa N. and Slay J., "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," *in Proceedings of Military Communications and Information Systems Conference (MilCIS)*, Canberra, pp. 1-6, 2015.

[37] Mukkamala S., Janoski G., and Sung A., "Intrusion Detection Using Neural Networks and Support Vector Machines," *in Proceedings of the International Joint Conference on Neural Networks*, Honolulu, pp. 1702-1707, 2002.

[38] Nguyen S., Nguyen V., Choi J., and Kim K., "Design and Implementation of Intrusion Detection System using Convolutional Neural Network for DoS Detection," *in Proceedings of the International Conference on Machine Learning and Soft Computing*, Phu Quoc, pp. 34-38, 2018.

[39] Pandey N. and Savakis A., "Poly-GAN: Multi-Conditioned GAN for Fashion Synthesis," *Neurocomputing*, vol. 414, pp. 356-364, 2020.

[40] Pham N., Foo E., Suriadi S., Jeffery H., and Lahza H., "Improving Performance of Intrusion Detection System Using Ensemble Methods and

Feature Selection," *in Proceedings of the Australasian Computer Science Week Multiconference*, Brisbane, pp. 1-6, 2018.

[41] Patil R., Biradar R., Ravi V., Biradar P., and Ghosh U., "Network Traffic Anomaly Detection using PCA and BiGAN," *Internet Technology Letters*, vol. 5, no. 1, pp. 1-6, 2022.

[42] Peng W., Kong X., Peng G., Li X., and Wang Z., "Network Intrusion Detection Based on Deep Learning," *in Proceedings of International Conference on Communications, Information System and Computer Engineering (CISCE)*, Haikou, pp. 431-435, 2019.

[43] Pu Y., Gan Z., Henao R., Yuan X., Li C., Stevens A., and Carin L., "Variational Autoencoder for Deep Learning of Images, Labels and Captions," *in Proceedings of Advances in Neural Information Processing Systems*, Barcelona, 2016.

[44] Salameh A. and Surakhi O., "An Optimized Convolutional Neural Network for Handwritten Digital Recognition Classification," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 21, pp. 3494-3503, 2020.

[45] Saranya T., Sridevi S., Deisy C., Chung T., and Khan M., "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review," *Procedia Computer Science*, vol. 171, pp. 1251-1260, 2020.

[46] School of Engineering and Information Technology, UNSW, Australia. ADFA Linux data set (ADFA-LD) cyber security benchmark dataset, http://www.cybersecurity.unsw.adfa.edu.au/ADFA%20IDS%20Datasets, 2021.

[47] Shahriar M., Haque N., Rahman M., and Alonso M., "G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System," *in Proceedings of IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, Madrid, pp. 376-385, 2020.

[48] Sharafaldin I., Lashkari A., and Ghorbani A., "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *in Proceedings of 4th International Conference on Information Systems Security and Privacy (ICISSP)*, Madeira, pp. 108-116, 2018.

[49] Stolfo S, Fan W., Lee W., and Prodromidis A., http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, Last Visited, 2018.

[50] Su T., Sun H., Zhu J., Wang S., and Li Y., "BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset," *IEEE Access*, vol. 8, pp. 29575-29585, 2020.

[51] Sumaiya I., Saira Banu J., Lavanya K., Rukunuddin M., and Abhishek K., "An Integrated Intrusion Detection System Using Correlation-Based Attribute Selection and Artificial Neural Network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, pp. 1-15, 2021.

[52] Surakhi O. and AlKhanafseh M., "Review on the Application of Blockchain Technology to Compact COVID-19 Pandemic," *in Proceedings of IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, Amman, pp. 193-198, 2021.

[53] Surakhi O., Zaidan M., Fung P., Hossein Motlagh N., Serhan S., AlKhanafseh M., Ghoniem R., and Hussein T., "Time-Lag Selection for Time-Series Forecasting Using Neural Network and Heuristic Algorithm," *Electronics*, vol. 10, no. 20, pp. 1-22, 2021.

[54] Surakhi O., García A., Jamoos M., and Alkhanafseh M., "A Comprehensive Survey for Machine Learning and Deep Learning Applications for Detecting Intrusion Detection," *in 22nd International Arab Conference on Information Technology*, Muscat, pp. 1-13, 2021.

[55] Surakhi O., Serhan S., and Salah I., "On the Ensemble of Recurrent Neural Network for Air Pollution Forecasting: Issues and Challenges," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 2, pp. 512-526, 2020.

[56] Surakhi O., Zaidan M., Serhan S., Salah I., and Hussein T., "An Optimal Stacked Ensemble Deep Learning Model for Predicting Time-Series Data Using a Genetic Algorithm-An Application for Aerosol Particle Number Concentrations," *Computers*, vol. 9, no. 4, pp. 1-26, 2020.

[57] Susilo B. and Sari R., "Intrusion Detection in IoT Networks Using Deep Learning Algorithm," *Information*, vol. 11, no. 5, pp. 1-11, 2020.

[58] Tang C., Luktarhan N., and Zhao Y., "SAAE-DNN: Deep Learning Method on Intrusion Detection," *Symmetry*, vol. 12, no. 10, pp. 1-20, 2020.

[59] Tarter A., Community Policing-A European Perspective: Strategies, Best Practices and Guidelines, Springer, 2017.

[60] Tavallaee M., Bagheri E., Lu W., and Ghorbani A., "A Detailed Analysis of the KDD CUP 99 Data Set," *in Proceedings of IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, pp. 1-6, 2009.

[61] Thamilarasu G. and Chawla S., "Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things," *Sensors*, vol. 19, no. 9, pp. 1-19, 2019.

[62] Uddin M., Rahman A., Uddin N., Memon J., Alsaqour R., and Kazi S., "Signature-Based Multi-Layer Distributed Intrusion Detection System Using Mobile Agents," *International Journal of Network Security*, vol. 15, no. 2, pp. 79-87, 2013.

[63] Verwoerd T. and Hunt R., "Intrusion Detection Techniques and Approaches," *Computer*

Communications, vol. 25, no. 15, pp. 1356-1365, 2002.
[64] Xiao Y. and Xiao X., "An Intrusion Detection System Based on a Simplified Residual Network," *Information*, vol. 10, no. 11, pp. 1-17, 2019.
[65] Yao R., Wang N., Liu Z., Chen P., and Sheng X., "Intrusion Detection System in the Advanced Metering Infrastructure: A Cross-Layer Feature-Fusion CNN-LSTM-Based Approach," *Sensors*, vol. 21, no. 2, pp. 1-17, 2021.
[66] Zaidan M., Surakhi O., Fung P., and Hussein T., "Sensitivity Analysis for Predicting Sub-Micron Aerosol Concentrations Based on Meteorological Parameters," *Sensors*, vol. 20, no. 10, 2020.
[67] Zhang G., Wang X., Li R., Song Y., HEe J., and Lai J., "Network Intrusion Detection Based on Conditional Wasserstein Generative Adversarial Network and Cost-Sensitive Stacked Autoencoder," *IEEE Access*, vol. 8, pp. 190431-190447, 2020.
[68] Zhang Y., Cao G., Wang B., and Li X., "A Novel Ensemble Method Ffor K-Nearest Neighbor," *Pattern Recognition*, vol. 85, pp. 13-25, 2019.
[69] Zhong M., Zhou Y., and Chen G., "Sequential Model Based Intrusion Detection System for IoT Servers Using Deep Learning Methods," *Sensors*, vol. 21, no. 4, pp. 1-21, 2021.

Ola Surakhi is an Assistant Professor at Middle East University, Jordan.
Dr. Surakhi received her Ph.D. degree from the University of Jordan in the Computer Science field.
Her main areas of research are Big Data Analytics, Modeling, Computational Intelligence, Machine Learning and Optimization.
She has participated in several funded research projects and published a number of papers in top-rated international conferences and journals.

Antonio García received his PhD Degree in Computer Sciences from the University of Granada in 2009.
He is currently Associate Professor at the Signal Theory, Telematics and Communications Department also at the University of Granada, where he previously has worked as contracted researcher and substitute professor for 14 years. His working areas include bioinspired algorithms, and their applications to data analysis, network security, or videogames, among others. He has published more than 25 papers in indexed international journals and more than 100 papers in top-rated international conferences. He has an H-index of 25 in Google Scholar and 16 in Scopus.
He has been the main researcher in two National projects, one Regional project, and two within the Campus of International Excellence of the University of Granada. He has conducted 4 research stays (short visits), two in Spain as a guest researcher, one at the University of Napier (Scotland) and another at the University of L'Aquila (Italy).

Mohammed Jamoos is a PhD candidate in the Department of Signal Theory, Telematics and Communications at Granada University, Spain.
Mr. Jamoos received his BA and MA degrees from Al-Quds University, Palestine in the computer science field.
His current study is concerned with Computer security, Computational Intelligence, Machine Learning and Deep Learning.

Mohammad Alkhanafseh is an Assistant Professor at Birzeit University, Palestine.
Dr. Khanafseh received his Ph.D. degree from the University of Jordan in the Computer Science field.
His main areas of research are Computer Security, Digital Forensics, IoT Networking, Computational Intelligence and Optimization.
He has participated in several funded research projects and published a number of papers in top-rated international conferences and journals.