IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received April 19, 2021, accepted May 16, 2021, date of publication May 24, 2021, date of current version June 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3083060

Machine Learning for Anomaly Detection: A Systematic Review

ALI BOU NASSIF[1], (Member, IEEE), MANAR ABU TALIB[2], (Senior Member, IEEE), QASSIM NASIR[3], AND FATIMA MOHAMAD DAKALBAB[2]

[1]Department of Computer Engineering, University of Sharjah, Sharjah, United Arab Emirates
[2]Department of Computer Science, University of Sharjah, Sharjah, United Arab Emirates
[3]Department of Electrical Engineering, University of Sharjah, Sharjah, United Arab Emirates

Corresponding author: Ali Bou Nassif (anassif@sharjah.ac.ae)

This work was supported by the Open UAE research group, University of Sharjah.

ABSTRACT Anomaly detection has been used for decades to identify and extract anomalous components from data. Many techniques have been used to detect anomalies. One of the increasingly significant techniques is Machine Learning (ML), which plays an important role in this area. In this research paper, we conduct a Systematic Literature Review (SLR) which analyzes ML models that detect anomalies in their application. Our review analyzes the models from four perspectives; the applications of anomaly detection, ML techniques, performance metrics for ML models, and the classification of anomaly detection. In our review, we have identified 290 research articles, written from 2000-2020, that discuss ML techniques for anomaly detection. After analyzing the selected research articles, we present 43 different applications of anomaly detection found in the selected research articles. Moreover, we identify 29 distinct ML models used in the identification of anomalies. Finally, we present 22 different datasets that are applied in experiments on anomaly detection, as well as many other general datasets. In addition, we observe that unsupervised anomaly detection has been adopted by researchers more than other classification anomaly detection systems. Detection of anomalies using ML models is a promising area of research, and there are a lot of ML models that have been implemented by researchers. Therefore, we provide researchers with recommendations and guidelines based on this review.

INDEX TERMS Anomaly detection, machine learning, security and privacy protection.

I. INTRODUCTION

Detecting anomalies is a major issue that has been studied for centuries. Numerous distinct methods have been developed and used to detect anomalies for different applications. Anomaly detection refers to "the problem of finding patterns in data that do not conform to expected behavior" [1], [2]. The detection of anomalies is widely used in a broad variety of applications. Examples of these include fraud detection, loan application processing, and monitoring of medical conditions, An example of a medical application is heart rate monitors [3]. Other widely used applications of detecting anomalies include cyber security intrusion detection [4]–[6], fault detection for aviation safety study, streaming, and hyperspectral imagery, etc. The importance of detecting anomalies in various application domains concerns the risk that unprotected data may represent significant, critical, and actionable information. For instance, detecting an anomalous computer network traffic pattern may expose an attack from a hacked computer [7]. Another example would be the detection of anomalies in the transaction data of a credit card, which may indicate theft [8]. Besides, detecting an anomaly from an airplane sensor may result in the detection of a fault in some of the components of the aircraft.

Anomaly is defined at an abstract level as a pattern, not in line with the ordinary anticipated behavior. Anomalies are classified into three main categories [1], [9], [10]:

1. **Point Anomalies**: If a single data instance can be considered anomalous for the remainder of the data, the instance is called a point anomaly and is regarded as the simplest anomaly form.

2. **Contextual Anomalies**: If in a particular context a data instance is anomalous, but not in another context, it is called a contextual anomaly. There are two attributes of contextual

The associate editor coordinating the review of this manuscript and approving it for publication was Mehul S. Raval.

anomalies: contextual attributes and behavioral attributes. The first attribute is applied to determine an instance's context (or neighborhood). For example, the longitude and latitude of a location are contextual attributes in spatial datasets. Moreover, time is a contextual attribute in time series data that determines an instance's position on the entire sequence. The second attribute is considered as attributes of behavior where it defines an instance's noncontextual features. For example, the amount of rainfall that occurs at any location in a spatial dataset describing the world's average rainfall is a behavioral attribute.

The preference for using the technique of contextual anomaly detection is determined by the significance of the contextual abnormalities in the target area. The availability of qualitative attributes is another significant aspect. In some instances, it is easy to identify a context, and thus it makes sense to apply a contextual detection technique. In other instances, it is not possible to establish a sense such that certain methods are difficult to use.

3. **Collective anomalies**: If a set of associated data instances is anomalous for the entire dataset, it is called a collective anomaly.

Statistical anomaly detection techniques are some of the oldest algorithms used to detect anomalies [10]. Statistical methods build a statistical model for the ordinary behavior of the data provided. A statistical inference test may then be carried out to detect whether or not an instance belongs to this model. Several methods are used to conduct statistical anomaly detection [11]. This includes proximity based, parametric, non-parametric, and semi-parametric methods.

Machine learning (ML) techniques are increasingly being used as one of the approaches to detect anomalies. ML is the effort to "automate the process of knowledge acquisition from examples" [12]. The technique is used to build a model that distinguishes between ordinary and abnormal classes. Anomaly detection can therefore be split into three broad categories based on the training data function used to build the model. The three broad classes are [1], [13]:

- *Supervised anomaly detection*: In this class, both the normal and anomalous training datasets contain labeled instances. In this model, the approach is to build a predictive model for both anomaly and normal classes and then compare these two models. However, in this mode, two issues occur. First, the number of anomalies in the training set is much lower when compared with normal instances. Second, precise and representative labels are challenging to identify, particularly for the anomaly class.
- *Semi-supervised anomaly detection*: Training here includes only ordinary class cases. Therefore, anything that cannot be classified as ordinary is marked as anomalous. Semi-supervised techniques presume that training data have labeled instances for the normal class alone. Since they do not need anomaly class labels, they are more common than supervised methods.
- *Unsupervised anomaly detection*: In this case, training datasets are not required for the methods. Therefore, those methods imply that normal instances are much more common than anomalies in test datasets. However, if the assumption fails, it leads to a high false alarm rate for this technique.

Many semi-supervised techniques can be adapted to operate in an unsupervised mode by using unlabeled dataset samples as training data. Such adaptation assumes that there are very few anomalies in the test data and these few anomalies are robust to the model learning during training.

This study's primary objective is to conduct a systematic review that represents a comprehensive study of ML techniques for anomaly detection and their applications. Moreover, this review studies the accuracy of the ML models and the percentage of research papers that apply supervised, semi-supervised, or unsupervised anomaly detection classification. We believe that this review will enable researchers to have a better understanding of the different anomaly detection methods and guide them in reviewing the recent research done on this subject.

To the best of our knowledge, there are very few Systematic Literature Reviews (SLR) on detecting anomalies through machine learning techniques, which has motivated this work. Research articles were read thoughtfully and were selected, based on Kitchenham and Charter's methodology [14]., with regards to (i) the main prediction research work done in anomaly detection, (ii) the ML algorithms used in anomaly detection, (iii) the estimation and accuracy of ML models proposed, and (iv) the strength and weaknesses of the ML technique used.

The remainder of this paper is divided into six sections: Section 2 provides information on related work. Section 3 describes the methodology used in this research. Section 4 lists the results and discussions. Section 5 addresses the limitations of this review. Finally, Section 6 contains a discussion and suggestions for future work.

A. LITERATURE REVIEW

Detection of anomalies is an important issue that has been investigated in various fields of study and implementation. Many detection methods for anomalies have been created specifically for certain applications, while others are more generic. For example, Chandola *et al.* [1] provided an extensive survey of anomaly detection techniques and applications. A board review of different techniques of Machine learning as well as non-machine learning, such as statistical and spectral detection methods, was discussed in detail. Moreover, the survey presents several applications of anomaly detection. Examples include cyber intrusion detection, fraud detection, medical anomaly detection, industrial damage detection, image processing detection, textual anomaly detection, and sensor networks. The same authors introduced another survey [10] on the topic of anomaly detection for discrete sequence. The authors provided a comprehensive and structured overview of the existing research on the problem of detecting anomalies in discrete/symbolic sequences. In addition, Hodge and Austin [15] presented an overall

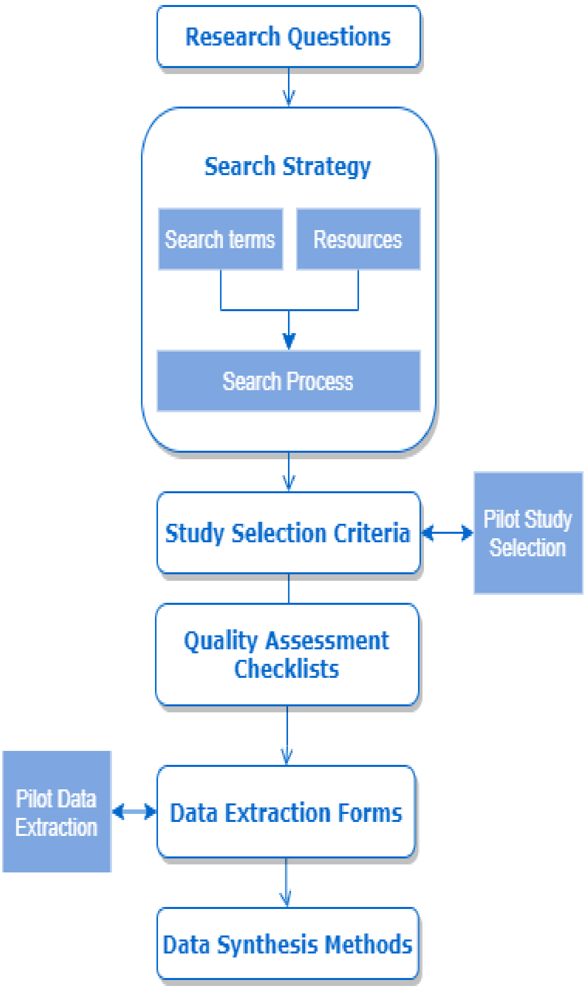


FIGURE 1. Research methodology.

TABLE 1. Inclusion & exclusion criteria.

Inclusion criteria	Exclusion criteria
Include only journals and conference papers.	Exclude papers with no clear publication information.
Include anomaly detection applications.	Exclude articles that include machine learning not related to anomaly detection.
Use machine learning techniques to identify anomalies.	Exclude all digital resources, which do not discuss anomaly detection techniques.
Include studies that compare machine learning techniques.	Exclude papers with predator journals
Consider articles published between 2000 and 2019.	

study of machine learning and statistical anomaly detection methodologies. Also, the authors discussed comparatively the advantages and disadvantages of each method. On the other hand, Agrawal and Agrawal [8] proposed a survey on anomaly detection using data mining techniques.

Several surveys were mainly focused on detecting anomalies in specific domains and applications, such as [16] where the authors presented an overall survey of wide clustering based fraud detection and also compared those techniques from several perspectives. In addition, Sodemann *et al.* [17] presented anomaly detection in automated surveillance, where they provided different models and classification algorithms. The authors examined research studies according to the problem domain, approach, and method. Moreover, Zuo [18], provided a survey of the three most widely used techniques of anomaly detection in the field of geochemical data processing; Fractal/multi-fractal models, compositional data analysis, and machine learning (ML), but the author focuses mainly on machine learning techniques. On the other hand, He *et al.* [19] surveyed the framework of log based anomaly detection. The authors reviewed six representative anomaly detection methods and evaluated each one. The authors also compared and contrasted the precision and effectiveness of two representative datasets of the production log. Furthermore, Ibidunmoye *et al.* [20] provided an overview of anomaly detection and bottleneck identification as they related to the performance of computing systems. The authors identified the fundamental elements of the problem and then classified the existing solutions.

Anomaly intrusion detection was the focus of many researchers. For instance, Yu [21] presented a comprehensive study on anomaly intrusion detection techniques such as statistical, machine learning, neural networks, and data mining detection techniques. Also, Tsai *et al.* [22] reviewed intrusion detection, but the authors focused on machine learning techniques. They provided an overview of machine learning techniques designed to solve intrusion detection problems written between 2000 and 2007. Moreover, the authors compared related work based on the types of classifier design, dataset, and other metrics. Similarly, Patcha and Park [23] presented an extensive study of anomaly detection and intrusion detection techniques, and Buczak and Guven [24] surveyed machine learning and data mining methods for cyber intrusion detection. They provided a description of each method and addressed the challenges of using machine learning and data mining in cyber security. Finally, Satpute *et al.* [25] presented a combination of various machine learning techniques with particle swarm optimization to improve the efficiency of detecting anomalies in network intrusion systems.

The detection of network anomalies has been an important area of research [26], [27] Therefore, many surveys focused on that topic. For example, Bhuyan *et al.* [11] presented a comprehensive study of network anomaly detection. They identified the kinds of attacks that are usually encountered by intrusion detection systems and then described and compared the effectiveness of different anomaly detection methods. In addition, the authors discussed network defenders' tools. Similarly, Gogoi *et al.* [7] surveyed an extensive study of well-known distance based, density based techniques as well as supervised and unsupervised learning in network anomaly detection. On the other hand, Kwon *et al.* [28] mainly focused on deep learning techniques, such as restricted Boltzmann machine based deep belief networks, deep recurrent neural networks, as well as machine learning methods appropriate to network anomaly detection. In addition, the authors presented experiments that demonstrated the practicality of using deep learning techniques in network traffic analysis.

Our systematic review is different from those described above, as we are presenting an extensive research study on detecting anomalies through machine learning techniques. Table 6 in Appendix A summarizes the related work and displays the differences between it and our work.

Our study differs from the related work in various aspects, such as:

1. Machine learning techniques are included, and the model types of techniques include supervised, semi-supervised, or unsupervised anomaly detection.
2. Precision comparison of each technique
3. A comprehensive approach is presented which includes the advantages and disadvantages of each technique.
4. Covers the period from 2000 to 2020, which is quite recent.

II. METHODOLOGY

In this study, we conducted a Systematic Literature Review (SLR) based on Kitchenham and Charters methodology [14]. The method includes the stages of planning and conducting research, and reporting. There are several phases in each stage. The planning phase is divided into six different stages. The first stage is to identify study questions that are based on the review's objectives. The second stage, in relation to specifying the proper search terms, is developing the search strategy, for collecting research papers related to the topic that fulfill the research questions. The third stage is to identify the study selection procedures, which include the exclusion and inclusion rules. In the fourth stage, rules are identified for quality assessment to be used to filter the collected study papers. The fifth stage involves detailing an extraction strategy to answer the research questions that were specified before. Finally, the sixth stage involves synthesizing the data obtained. We followed the review protocol, and this is demonstrated in the following subsections.

Error! Reference source not found. below illustrates this research methodology.

A. RESEARCH QUESTIONS

This SLR intends to summarize, clarify and examine the ML techniques and implementations that were applied in anomaly detection from 2000 through 2020

inclusive. The following four research questions (RQs) are raised for this purpose:

1.RQ1: What is the main prediction about research work done in anomaly detection?

RQ1 aims to identify the prediction research work that is done in anomaly detection, whether the prediction is an ML.

2.RQ2: What kinds of ML algorithms are being applied in anomaly detection?

RQ2 aims at specifying the ML methods that have been applied in the detection of anomalies.

3.RQ3: What is the overall estimation and accuracy of machine learning models?

RQ3 is concerned with ML model estimation. Estimation accuracy is the main performance metric for models of ML. This question focuses on the following three elements of estimation accuracy: dataset building, performance metric, and accuracy value.

4.RQ4: What is the percentage of papers that address unsupervised, semi-supervised, or supervised anomaly detection?

RQ4 aims to present the percentage of collected research papers that use unsupervised, semi- supervised, or supervised anomaly detection techniques.

B. SEARCH STRATEGY

We followed the following procedure to construct the search term:

1) Main search terms are identified from the research questions.
2) New terms were defined to replace main terms such as intrusion, outliers, and synonyms.
3) Boolean operators (ANDs and ORs) are used to limit the search results.
4) The search terms that are used in this review are related to anomaly detection and machine learning.

Below are the digital libraries that we used in this search (journals and conference papers):

- Google Scholar
- ACM Digital Library
- Springer
- Elsevier
- IEEE Explorer

According to our inclusion/exclusion criteria, 290 papers were used in this review. They include 95 journal papers and 195 conference papers.

C. STUDY SELECTION

In the beginning, we collected 350 papers based on the search terms mentioned earlier. Later, we filtered those papers to verify that only papers related to the topic were included in our review. The filtration process was discussed among the co-authors at planned periodic meetings. The filtration and selection processes are explained below:

Step 1: Remove all the duplicated articles that were collected from the different digital libraries.

Step 2: Apply inclusion and exclusion criteria to avoid any irrelevant papers.

Step 3: Remove review papers from the collected papers.

Step 4: Apply quality assessment rules to include only the qualified papers that ensure the best answer for our research questions.

Step 5: Search for additional related papers from references in the collected papers from step 4 and repeat step 4 on the new added articles.

TABLE 2. Selected papers' quality assessment results.

Result	No. of papers	Paper ID
3.5	1	A217 (Discarded)
4.75	1	A24 (Discarded)
5	6	A12, A43, A127, A163, A192 ,A208
5.25	1	A205
5.5	3	A141, A166, A201
5.75	4	A68, A147, A178, A195
6	6	A118, A173, A175, A183, A259, A278
6.25	8	A32, A134, A168, A187, A197, A28, A248, A282
6.5	7	A13, A25, A31, A33, A122, A174, A211
6.75	10	A11, A21, A22, A35, A36, A56, A57, A144, A186, A238
7	12	A3, A4, A30, A44, A62, A74, A77, A130, A140, A176, A200, A242
7.25	14	A26, A29, A58, A66, A67, A75, A101, A157, A224, A226, A227, A231, A266, A269
7.5	12	A20, A61, A72, A138, A142, A148, A153, A213, A244, A272, A280, A283
7.75	16	A1, A7, A19, A23, A41, A48, A53, A73, A135, A177, A181, A240, A261, A275, A281, A285
8	11	A27, A70, A92, A94, A105, A112, A164, A176, A185, A188, A268
8.25	16	A8, A16, A49, A76, A96, A149, A156, A169, A171, A182, A193, A207, A233, A267, A271, A286
8.5	23	A2, A9, A10, A18, A40, A42, A51, A52, A59, A60, A63, A64, A83, A124, A139, A143, A150, A161, A170, A184, A203, A243, A255
8.75	31	A103, A109, A123, A126, A136, A14, A146, A17, A189, A209, A212, A215, A225, A229, A234, A250, A260, A263, A279, A38, A39,A45, A46, A47, A5, A54, A71, A79, A82, A95, A99
9	32	A100, A106, A117, A120, A133, A137, A145, A15, 155, A159, A165, A180, A214, A219, A228, A230, A246, A251, A252, A265, A276, A284, A34 A37, A50, A55, A65, A86, A89, A91, A93, A98
9.25	23	A104, A107, A108, A113, A114, A115, A125, A128, A129, A160, A191, A198, A223, A239, A247, A249, A258, A6, A78, A80, A81, A84, A85
9.5	23	A110, A116, A131, A154, A158, A162, A190, A194, A204, A206, A216, A218, A220, A221, A222, A254, A262, A273, A69, A87, A90, A97, A287
9.75	20	A102, A111, A119, A121, A132, A167, A172, A196, A199, A202, A232, A235, A237, A241, A257, A264, A270, A274, A88, A289
10	10	A151, A152, A210, A236, A245, A253, A256, A277, A288, A290

TABLE 3. Anomaly detection applications among articles.

Application	Freq.	Application	Freq.
Intrusion Detection	68	Finance Domain	2
network anomaly detection	66	Road Anomaly	2
anomaly detection	29	temperature anomaly	2
data	11	water treatment system	2
video anomaly detection	10	Automotive CAN bus	1
Mobile ad-hoc networks	8	Power Quality Measurements	1
Cloud computing	7	anti forensic	1
Hyperspectral Imagery	7	Botnets	1
medical application	7	corpus anomaly detection	1
sensor network	6	digits	1
Time Series	6	Electrical Substation Circuits	1
smart environment	5	electroencephalography	1
System Log	5	evolving connectionist systems	1
Space Craft	4	Gas Turbine Combustor	1
Artificial immune system	3	Web Service	1
SCADA System	3	Internet of Things (IoT)	1
wireless network security	3	manufacturing process	2
Cyber Physical System	3	Maritime domain	1
Advanced Monitoring Systems	2	netflow records	1
Aviation	2	Online Anomaly Prediction	1
energy consumption	2	vessel tracks	1
Fault Diagnosis	2		

The applied inclusion and exclusion criteria in this review are discussed in Table 1. In the end, after conducting the filtration steps, 290 papers were observed for this review.

D. QUALITY ASSESSMENT RULES (QARs)

The QARs were the final step in the identification of the final list of papers to be included in this review. The QARs are essential to guaranteeing and assessing the quality of the

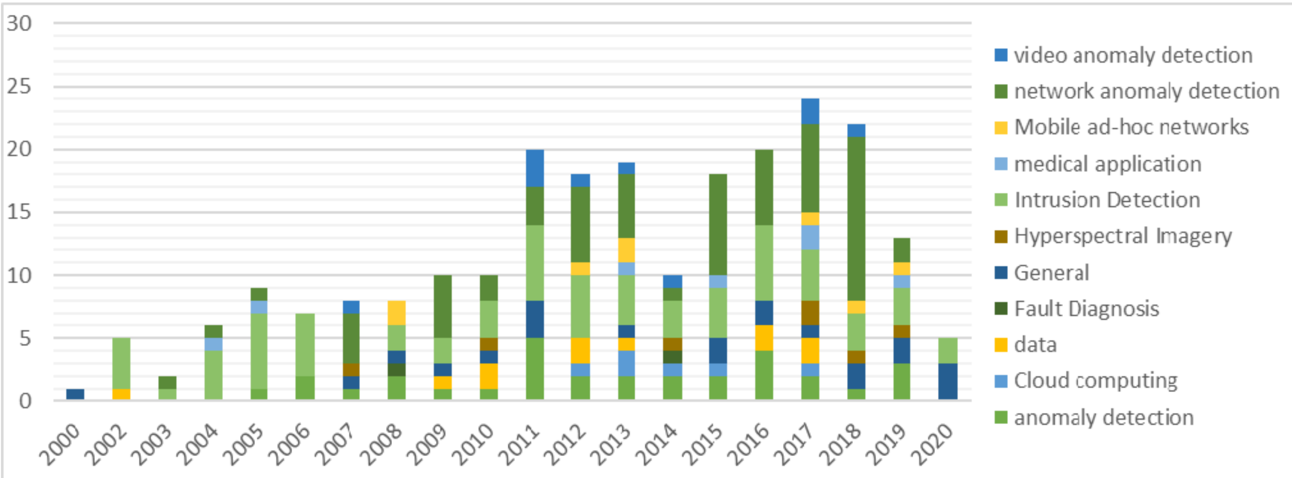


FIGURE 2. Anomaly detection applications iteration per year.

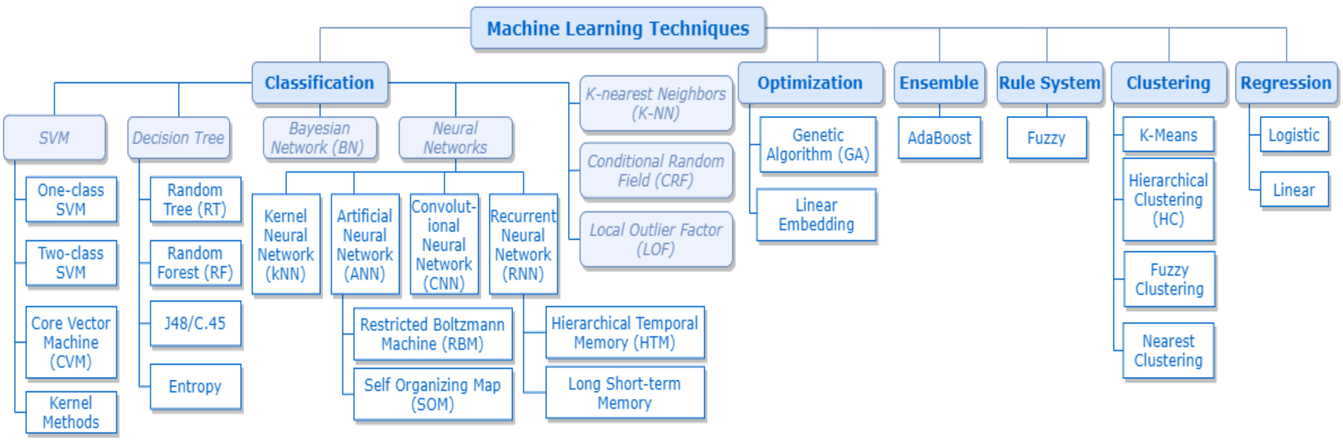


FIGURE 3. Machine learning techniques observed.

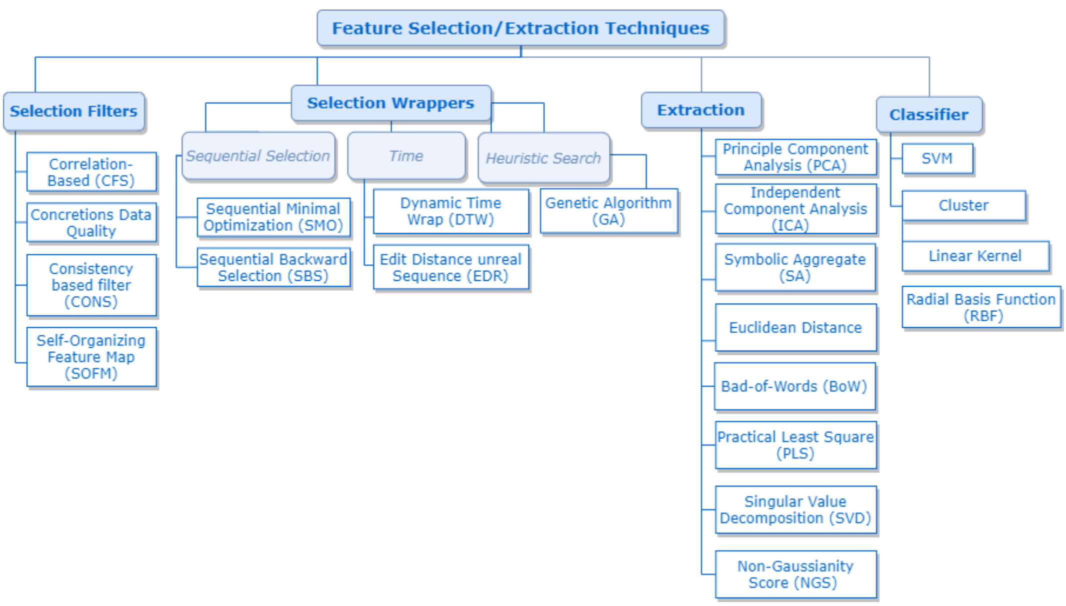


FIGURE 4. Feature selection/extraction techniques observed in the literature.

research papers. Therefore 10 QARs are identified and each is given a value of 1 mark out of 10. The score of each QAR is selected as follows: "fully answered" = 1, "above average" = 0.75, "average" = 0.5, "below average" = 0.25, "not

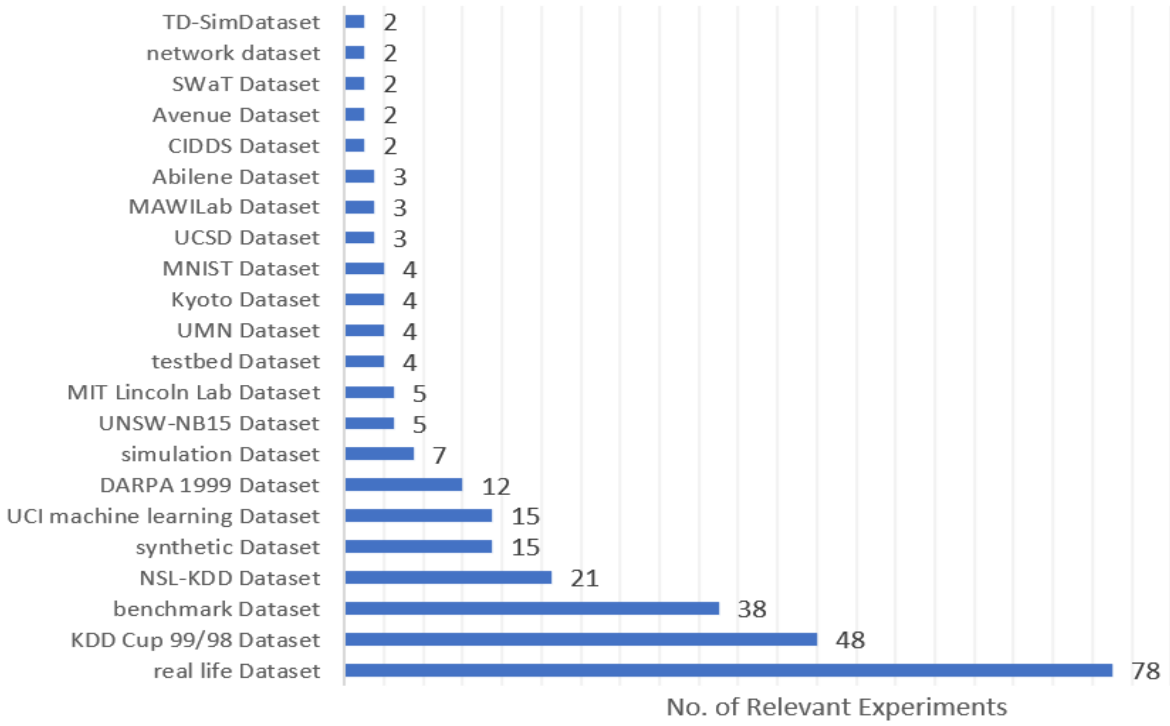


FIGURE 5. Utilized datasets in collected research articles.

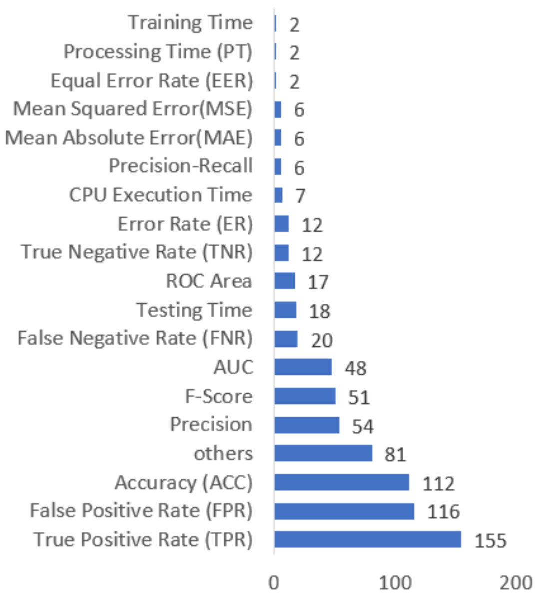


FIGURE 6. Percentage of anomaly detection type.

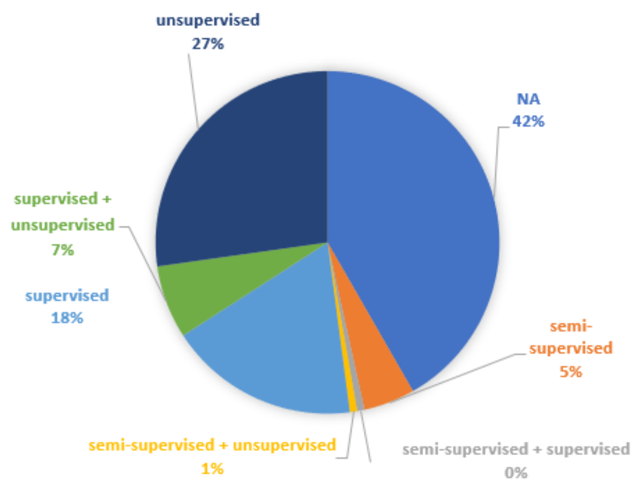


FIGURE 7. Frequency of performance metrics among.

answered'' = 0. The summation of the marks obtained for the 10 QARs is the score of the article. Moreover, if the result is 5 or higher, we consider the article; otherwise, we exclude it. Moreover, we choose the score 5 as it represents the middle point of the good quality articles and it answers our intended research questions.

QAR1: Are the study objectives clearly recognized?

QAR2: Are the anomaly detection techniques well defined and deliberated?

QAR3: Is the specific application of anomaly detection clearly defined?

QAR4: Does the paper cover practical experiments using the proposed technique?

QAR5: Are the experiments well designed and justifiable?

QAR6: Are the experiments applied on sufficient datasets?

QAR7: Are estimation accuracy criteria reported?

TABLE 4. Machine learning techniques among research articles.

Technique	Freq.	Technique2	Freq.2	Technique3	Freq.3
SVM	23	CNN + DBN + SAE + LSTM	1	LR + DT + SVM + PCA	1
Cluster	11	CNN + LSTM + DNN	1	LR + RF	1
NN	8	CPM	1	LSTM + NN	1
OCSVM	8	CSI + KNN	1	LSTM + RNN	1
AE	8	CVM	1	LSTM + RT	1
Naïve Bayes	6	DBN + RBM	1	multiple kernel	1
DT	5	DBN + SVM	1	naïve Bayes + adaboost	1
Ensemble	5	DBSCAN + Clustering	1	Naïve Bayes + DT	1
ELM	4	DCM	1	naïve Bayes + DT + J48	1
KNN	4	DCNN + LSTM	1	Naïve Bayes + K-Means Clustering	1
PCA	4	D-Markov + KNN	1	negative selection	1
RT	4	DNN	1	negative selection + C4.5 + naïve Bayes	1
DBN	3	DNN + RF + VAE	1	negative selection + MP	1
GAN	3	DRBM	1	negative selection + NN	1
HMM	3	DRBM + SVM	1	negative selection + SVM	1
LSTM	3	DT + K-Means Clustering	1	NN + SOM	1
n-gram	3	DT + NN	1	NN + SVM	1
RF	3	DT + RF + ANN	1	NOF	1
RNN	3	ensemble + clustering	1	OCSVM + LSTM	1
SVM + RBF	3	Ensemble + SVM	1	PCA + NN	1
BN	2	FFNN + LSTM	1	RBM + AE	1
ENN	2	Fuzzy + C-means	1	Regression	2
FRaC	2	fuzzy + GA	1	RF + DT + SVM + Naïve bayes + NN	1
fuzzy	2	fuzzy + SVM	1	RF + Entropy	1
GA	2	fuzzy K-Means Clustering + ANN	1	RF + LR	1
Gaussian model	2	GA + SOM + SVM	1	RF + RT	1
HTM	2	GA + SVM	1	RLS + ELM + NN	1
IF	2	GAN + LSTM + RNN	1	RNN + LSTM	1
kernel	2	Gaussian mixture + PCA	1	RVM + Bayesian Network	1
KNN + OCSVM	2	HMM + Naïve Bayes	1	SAE	1
Naïve Bayes + KNN	2	HMM + SVM	1	sequence algorithm	1
RLS	2	J48 / C4.5	1	single window	1
SOM	2	J48 + Naïve bayes	2	SOM + K-Means	1
SOM + J48/C4.5	2	J48 + Naïve Bayes + SMO	1	SVM + C4.5	1
SVM + Entropy	2	k-means and Skip-gram	1	SVM + Cluster	1
SVM + SOM	2	Kernel + PCA	1	SVM + DNN	1
TR	2	kernel + regression	1	SVM + DT	1
wrappers	2	K-mean + SMO network	1	SVM + ensemble	1
AE + ANN	1	k-Means + C4.6	1	SVM + entropy + Adaboost	1
AE + ensemble + SVM + RF	1	K-means + cluster	1	SVM + GA	1
AE + K-Means	1	K-means + DT	1	SVM + GA + KNN	1
ANN	1	K-means + SVM	1	SVM + Kernel	1
Bayesian network	1	K-means cluster	1	SVM + K-Medoids clusting	1
boosting	1	k-means + clustering	1	SVM + Random Forest	1
CESVM	1	KNN + SVM	1	SVM + RF	1
CFS	1	LE	1	SVM + SVR network	1
CNN	1	LOF	1	TCM-KNN	1
RF + KNN + DT	1	FCM + KNN	1	TD	1
OCSVM + LOF	1	DT + RF + KNN + Boosting DT	1	Sub-Space Clustering (SSC) and One Class Support Vector Machine (OCSVM)	1

QAR8: Is the proposed estimation method compared with other methods?

QAR9: Are the techniques of analyzing the outcomes suitable?

QAR10: Overall, does the study enrich the academic community or industry?

E. DATA EXTRACTION STRATEGY

In this step, our aim was to analyze the final list of papers to extract the required information for answering the four research questions. Consequently, we extracted the following information from each paper: paper number, title of the paper, publication year of the paper, publication type, anomaly

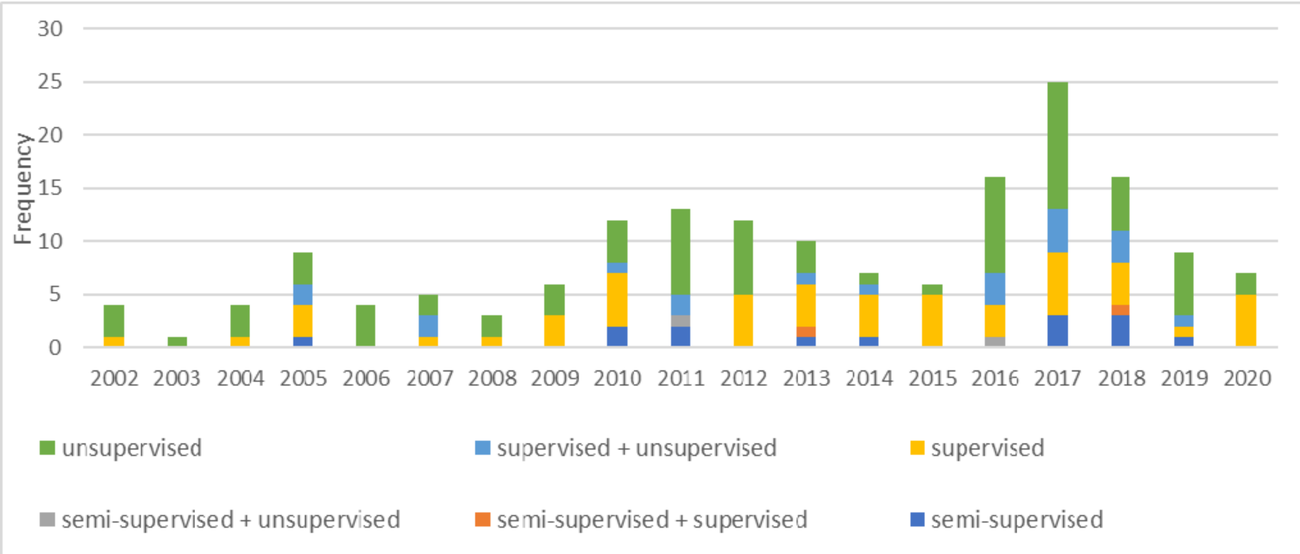


FIGURE 8. Anomaly detection classification type per year.

application type, RQ1, RQ2, RQ3, and RQ4. Due to the unstructured nature of information, extraction was challenging. For instance, for associated methods such as "J48" or "C4.5," researchers would use distinct terminologies. It is essential to note that the four research questions were not answered by all papers.

F. SYNTHESIS OF EXTRACTED DATA

In order to synthesize the information obtained from the chosen papers, we used various processes to aggregate evidence to answer the RQs. The following describes in detail the method of synthesis we followed: We used the technique of narrative synthesis to tabulate the information obtained in accordance with RQ1 and RQ2. We use binary outcomes to analyses the results for the information obtained (quantitative) in RQ3 and RQ4, which came from different papers with distinct accuracy calculation methods that are presented in a comparable way.

III. RESULTS AND DISCUSSIONS

In this section, we address the outcomes of this review. This subsection gives an overview of the selected papers of this review. The results of each research question are addressed in detail in the following five sections. A total of 290 studies were chosen which implemented machine learning for anomaly detection. These research articles were published between 2000 and 2020. The list of these papers is included in Table 7 in Appendix A. As explained earlier, a quality assessment criterion is used to stream the articles on the basis of the marks obtained. Research articles of grade 5 or higher (out of 10) have been taken into consideration. Moreover, the frequency of the QAR score of the selected paper is listed in Table 2.

A. ANOMALY DETECTION APPLICATIONS

In this section, we address RQ1 which aims to identify the prediction research work that has been done in anomaly detection.

Anomaly detection techniques are mainly divided into two classifications: machine learning based, and non-machine learning based. The non-machine learning based techniques can be classified into statistical and knowledge based. Regarding this review, there are 274 articles that discuss the detection of anomalies through machine learning techniques. On the other hand, there are 16 articles that focus on non-machine learning based techniques.

Detection of anomalies can be used in a wide variety of applications. In this review, we identified 43 different applications in the selected papers. The list of these applications appears in Table 3.

As shown in Table 3, the review indicates that intrusion detection, network anomaly detection, general anomaly detection, and data applications are the studies applied most often in the anomaly detection area. In addition, the table contains comprehensive information on the frequency with which anomaly detection application is used by the selected articles.

Moreover, the review shows that researchers began to adopt more applications of anomaly detection between 2011 and 2020. For further information on results, Figure 2 illustrates the distribution of anomaly detection application per year during the period considered.

B. TYPES OF MACHINE LEARNING TECHNIQUES

In this section, we address RQ2, which aims at specifying the machine learning techniques that have been used to detect anomalies between 2000 and 2020.

TABLE 5. Machine learning techniques strength and weakness.

ID	ML technique	Strength and Weakness
A1	SVM	Weakness: Soft margin SVM can't be used for novel attacks because it needs pre-acquired learning info One-class SVM is difficult to use in real world because of high false positive rate
A8	k-Means clustering + C4.5 decision tree	Weakness: Cascading the k-Means clustering method with C4.5 decision tree learning alleviates two problems in k-Means clustering: 1) the Forced Assignment problem and 2) the Class Dominance problem.
A9	SVM + decision trees (DT) + Simulated Annealing (SA)	Strength: SVM and SA can find the best selected features to elevate the accuracy of anomaly intrusion detection, and by analyzing the informatioon from using KDD'99 dataset DT, and SA can obtain rules for new attacks and can really improve accuraacy of classification
A87	Niche Clustering	Strength: UNC can handle noise
A88	Naïve Bayes with Adaboost	Strength: Low computation time
A90	Relevance Vector Machine (RVM) and Dynamic Bayesian Network	Strength: Their model is good for limit checking
A93	One class SVM (OCSVM)	Strength: No need for sample data with free anomalies
A94	SVM + DNN	Weakness: Difficulties in detecting gradual changes of sensor methods and detecting anomalous actuator behavior Strength: SVM takes approximatly 30 mins only to train
A97	Recursive Least Squares (RLS)	Weakness: Low True Positive Rate
A98	OneClassSVM + Local Outlier Factor LOF + Isolation forest + Elliptic Envelope	Weakness: Their model requires large aamount of data with good coverage Strength: Good performance and very effective in anomaly detecion
A105	SVM	Strength: SVM reduces computing complexity
A107	ERAD +CLAD	Weakness: ERAD assumes the training data are free of attacks Clad does not aim to generate a concise model and doesnt explain alerts well
A108	LR RF	Weakness: High detection accuracy Strength: Low categorizing accuracy
A111	centered hyperellipsoidal support vector machine CESVM	Strength: CESVM is flexible in terms of parameter selection
A116	one class SVM (OCSVM)	Strength: One-Class SVM achieves better accuracy rates than the conventional anomaly detectors.
A117	PCA	Strength: PCA substantially reduces the effectiveness of poisoning for a variety of scenarios and maintains a significantly better balance between false positives and false negatives than the original method when under attack
A119	Fuzzy Rough C-means	Strength: FRCM integrates the advantage of Fuzzy set theory and rough set theory that the improved algorithm to network intrusion detection
A121	Extreme learning machine (ELM)	Strength: ELM hidden layer parameters are assigned randomly
A122	random forest (RF)	Strength: In random forests algorithm, there is no need for crossvalidation or a test set to get an unbiased estimate of the test error. Since each tree is constructed using the bootstrap sample
A123	convolutional neural network (CNN) + long short-term memory (LSTM) + deep neural network (DNN)	Strength: The combination of CNN and+C14 LSTM can effectively extract features
A125	LibSVM	Strength: LibSVM is simple to use and high precision
A128	Extreme Learning Machine (ELM)	Strength: ELM for the single hidden layer feed forward neural networks.
A130	SVM and SVR	Strength: Their model can be used to avoid difficulties of using linear functions in the high dimensional feature space and optimization problem is transformed into dual convex quadratic programming
A131	Decision Tree (DT)	Strength: By tracking the nodes from the root of the tree based on the feature values of an example, we can get the predicted class of it.
A141	rule based decision tree (RBDT)	Weakness: Low complexity classification learning technique on present hardware speed and easy analysis is required to estimate the decision on classified patterns.
A148	SVM and SOM	Strength: - SOM discover the hidden structure or pattern in the training data - One-class SVM identifies outliers among positive examples and uses them as negative examples

As a fundamental point of this review, the most frequently used ML methods in anomaly detection are identified along with an evaluation of these methods. The evaluation of the methods considers all the phases of the method's experiment, such as the feature selection phase, extraction phase, etc.

TABLE 5. ***(Continued.)*** **Machine learning techniques strength and weakness.**

A155	naïve Bayesian classifier	Weakness: - false positive rate needs to be improved Strength: - One of the simplest and effective classifiers
A160	one class extreme learning machine Kernel (ELMk)	Strength: Fast learning and better generalization
A168	D-Markov machine with symbolic false nearest neighbors	Strength: The efficiency of numerical computation is significantly enhanced relative to what can be achieved by direct analysis of the original time series data
A170	correlational paraconsistent machine (CPM)	Weakness: Applications often face uncertainties and inconsistencies when required to characterize and analyze network traffic. Most of the time, the processed data may be incomplete or permeated with noise
A171	Negative selection + multilayer neural network (backprogagation) + evolutionary algorithm	Strength: Their model does not depend on any specific type of classification algorithm
A174	LERAD	Weakness: LERAD issues false alarms, because unusual events are not always hostile Strength: Can sometimes detect previously unknown attacks
A176	Adaboost + SVM + Entropy	Adaboost Weakness: Poor behavior on noisy data, the low level of noise in our data makes the learning conditions ideal Entropy strength: Much more robust to noise Overall Strength: Scalable algorithms that are guaranteed to converge with predictable performance
A180	SVM + GA with Neural Kernel	Strength: Efficient optimization of both features and parameters for detection models
A185	Stacked Autoencoder (SAE)	Strength: Their model self learns the features necessary to detect network anomalies and is able to perform attack classification accurately
A187	k-means clustering	Strength: K-means only requires pairwise distance of data, and the algorithm does not require the distance to be metric
A188	SOM + J.48 decision tree	Strength: Model is very robust, fast and simple.
A189	LSTM, NN	Strength: Their model adapts to new log paterns over time
A190	two-class SVM with a Radial Basis Function (RBF) kernel	perform in a continuous monitoring situation
A192	Bayesian estimation	Weakness: Model has high false alarm rate
A193	evolutionary neural networks	Strength: -Evolutionary approach can reduce the learning time as well as it has advantage that the near optimal network structure can be obtained. - ENN does not require trial and error cycles for designing the network structure and the near optimal structure can be obtained automatically
A194	3D convolutiona AutoEncoder	Strength: Highly effective in various computer vision tasks, as well as anomaly detection
A198	Auto encoder based on Artificial Neural networks	Strength: Efficiently reconstruct inputs that closely resemble normal network traffic but poorly reconstructs anomalous or attack inputs
A199	Random Forest algorithm and regression tree	Strength: Enhance the generalisation of the learning algorithm and can thereby produce better results than when using single classifiers
A202	swarm intelligence-based clustering	Strength: Model has increased detection accuracy and efficiency. As well as intersting properties such as flexibility, robustness, decentralization and self-organization
A204	Ensemble learning + AE+ SVR + RF	Strength: Reduced false alarm rate, and improved sensitivity
A209	Stochastic gradient boosting	Strength: Stochastic gradient boosting highly improve the quality of the top ranked items
A213	Recurrent Neural Networks (RNN)	Strength: RNN is capable of learning complex temporal sequence
A218	K-mean + SMO	Weakness: Takes more time than simple classification or clustering
A219	most relevant principal components + neural networks	Strength: adapt to the dynamics in a time window and at the same time consider the values of cloud performance metrics in previous windows
A225	Fuzzy Adaptive Resonance Theory + Evolving Fuzzy Neural Networks + SVM	Strength: can significantly reduce the false alarm rate while the attack detection rate remains high
A229	Conditional anomaly detection	Strength: takes into account the difference between the userspecified environmental and indicator attributes during the anomaly detection process "anomaly."
A231	Bayesian Networks	Strength: can learn cyclical baselines for gas concentrations, thus reducing false alarms usually caused by flatline thresholds
A232	Naive Bayes with adaboost	Strength: AdaBoost's computational complexity is generally lower than SOM, ANN and SVM.

TABLE 5. *(Continued.)* **Machine learning techniques strength and weakness.**

A233	Negative and positive selection + C4.5 and Naïve Bayes	Strength: the increased ability of classifiers in identifying both previously known and innovative anomalies, and the maximal degradation of overfitting phenomenon
A240	Deep Neural Network	Weakness: have an inherent problem linked to model visibility and interpretation
A253	fully convolutional neural network	Weakness: -Too slow for patch-based methods; thus, CNN is considered as being a time-consuming procedure. -Training a CNN is totally supervised learning; thus, the detection of anomalies in real-world videos suffers from a basic impossibility of training large sets of samples from non-existing classes of anomalies
A255	Neural networks	Strength: Neural networks are based on the concepts of statistical pattern recognition and have emerged as a practical technology
A259	Frequent itemset mining (FIM) + C5.0 + decision tree	Strength: conceptually simple and, therefore, easy to understand and configure by a network operator
A275	LSTM-RNN	Strength: ability to learn the behavior of a training set, and in this stage it acts like a time series anomaly detection model
A277	Ensemble learning	Strength: known to produce more robust results. For example, bootstrap aggregating (or bagging) tends to reduce problems related to overfitting to the training data

As shown in Figure 3, we identified 28 ML techniques that had been applied by researchers in the development of models to detect anomalies on their application. These techniques can be divided into six categories: classification, ensemble, optimization, rule system, clustering, and regression. Those ML techniques are used in two forms: standalone or hybrid models. Hybrid models are obtained by combining two or more ML techniques. Table 4 represents the frequency of ML techniques among the collected research articles. According to Table 4 in Appendix A, it can be seen that a lot of researchers used to combine more than one ML technique. This includes A2 (DBN with one class SVM), A23 (SVM with GA), and A14 (SVM with K-Medoids clustering). Moreover, SVM is the most used technique as either standalone or in hybrid models.

Feature selection/extraction has been discovered extensively in the literature and it is a significant move towards discarding irrelevant data, which helps to enhance and improve the precision and computational efficiency of the suggested models. Figure 4 demonstrates 21 different feature selec-

TABLE 6. **Related work summary.**

Ref.	Year	Summary	Differences between their review and ours
[15]	2004	This survey provides an overview of the techniques of outlier detection: classification-based, clustering based, nearest neighbour based, and statistical.	It covers outlier detection techniques, but it was published in 2004. Moreover, our work shows the estimation accuracy of ML models as well the type of anomaly detection.
[23]	2007	In this survey, the authors provide a comprehensive review of techniques and solutions in anomaly detection. They indicate methods for statistical identification of anomalies, anomaly detection based on machine learning, sequence analysis based on system call, etc.	It covers anomaly detection techniques before 2007. Ours covers work up to 2019.
[1]	2009	This survey is similar to [15]. The authors include several techniques of machine learning and non-machine learning. They also include anomaly detection applications.	This survey covered machine learning techniques before 2009. Our work includes additionally, an estimation of the accuracy of each ML model as well as the type of anomaly detection.
[22]	2009	In this survey, 55 associated studies on single, hybrid and ensemble classifiers are reviewed by the authors. Furthermore, a comparison is provided between the studies.	It covers anomaly intrusion techniques between 2000 and 2007.
[7]	2011	In this survey, the authors provide a comprehensive outlier detection method for network anomaly identification. They classified the methods into: Distance-based, density-based, and machine learning.	It covers distance-based, density-based and machine learning based techniques before 2011, while ours covers the period up to 2019.
[10]	2012	In this survey, the authors present a detailed overview of detecting anomalies in discrete/symbolic sequence. They reveal the strength and weaknesses of techniques discussed prior to 2012.	It covers anomaly detection for discrete sequence in particular. In contrast, our work is more general.
[21]	2012	The authors present anomaly intrusion detection methods in this survey and clarify its evolution. Machine learning methods, neural network, computer immunology, and data mining were included.	It covers anomaly intrusion techniques until 2012. Our study covers research up to 2019.
[17]	2012	In this survey, the authors provide anomaly detection techniques in automated surveillance. They provide different models and classification algorithms such as dynamic Bayesian network, Bayesian topic models, artificial neural network, clustering, decision tree, and fuzzy reasoning.	In specific, it includes anomaly detection methods in automated surveillance. Our work, on the other hand, is more general.

TABLE 6. ***(Continued.)*** **Related work summary.**

[11]	2013	In this survey, the authors addressed the causes and aspects of network anomalies. They add performance metrics and intrusion detection systems evaluation and provide a list of tools and research issues.	It covers network anomaly detection in particular. Our work differs in that it is more general, and includes an estimation of the accuracy of each ML model as well the type of anomaly detection used.
[25]	2013	In this survey, the authors present machine learning methods in network intrusion detection system with particle swarm optimization for anomaly detection. They provide intrusion detection system types and present each technique's advantages and disadvantages.	It covers machine learning and particle swarm optimization techniques up to 2013
[20]	2015	In this survey, the authors provide a comprehensive analysis of performance anomaly detection and identification of bottleneck. In computing systems, they identified various types of common anomalies and the techniques and strategies for detecting them.	It covers anomaly detection and performance of bottlenecks in particular. On the other hand, our work is more general, and includes the estimation accuracy of each ML model as well the type of anomaly detection used.
[16]	2015	In this survey, the authors review various clustering-based anomaly detection techniques and they provide comparison between the techniques.	It covers the techniques of fraud detection in particular. Our work is more general, and it includes an estimation of the accuracy of each ML model as well the type of anomaly detection used.
[8]	2015	Data mining methods are presented in this survey under four task classes: learning association rule, clustering, classification, and regression.	It includes various anomaly detection methods that focus on data mining methods.
[19]	2016	The authors provide six techniques for identification of anomalies in this survey. They compare their accuracy and effectiveness. They also published an open-source toolkit of the techniques used for identification of anomalies that were discussed in the survey.	It covers anomaly detection in system log analysis in particular. In contrast, our work is more general, and it includes an estimation of the accuracy of each ML model as well as the type of anomaly detection.
[24]	2016	This article includes an extensive overview of the techniques of machine learning and data mining for intrusion detection cyber analytics, discussions, difficulties and some recommendations.	It includes both machine learning and intrusion detection methods, but…our research…
[18]	2017	The authors present the methods of machine learning that define geochemical anomalies in this survey. In addition, the survey discusses techniques of analysis such as principle component analysis (PCA) and the analysis of the factor.	It covers geochemical Anomalies in particular. However, our work is more general, and focuses on ML techniques and their performance.

TABLE 6. ***(Continued.)*** **Related work summary.**

[28]	2017	The authors present an overview of methods of detection of anomalies and deep learning techniques in this survey. They also address the feasibility of using deep learning to detect network anomalies.	It includes deep learning methods for detecting anomalies in network intrusion systems, while our research…
[29]	2018	In this survey, the authors examine the most significant elements of anomaly detection in five areas: anomalies in network traffic, types of network data, and categories of intrusion detection technologies, techniques and systems detection, and open issues of unresolved problems.	It covers network anomaly detection in particular. Our work is more general and includes an estimation of the accuracy of each ML model as well the type of anomaly detection.
[30]	2018	In this survey, the authors present a comprehensive understanding of anomaly detection techniques to ensure both the cyber security and safety of connected vehicles. In addition, they researched 65 research articles and established a novel taxonomy, then classified the articles.	It includes the detection of anomalies for cyber security and safety of connected vehicles. On the other hand, our work is more general, including the accuracy of evaluation of each ML model, as well as the type of identification of anomalies.
[9]	2019	In this survey, the authors present an explanation of important contexts of real-time big data processing, detection of anomalies, and machine learning algorithms. They acknowledge the real-time big data processing research challenges in detecting anomalies.	It includes the detection of anomalies in the real-time processing of big data. In contrast, our work is more general, and it includes an estimation of the accuracy of each ML, model as well the type of anomaly detection.

tion/extraction techniques that are being applied. Moreover, we notice that PCA and CFS are the feature selection techniques being used most often in anomaly detection. Even though this step is very important, most of the research articles did not include it. While some research articles did apply this step, the techniques were not discussed.

Table 5 in Appendix A represents some of the research articles that mentioned the strength or weakness of their proposed machine learning model. Therefore, Table 5 shows the research article number, the machine learning technique, and the strength or weakness if mentioned.

C. OVERALL ESTIMATION AND ACCURACY OF ML MODELS

In this section, we address RQ3 which is concerned with the estimation of ML models. Estimation accuracy is the primary performance metric for machine learning models. This question focuses on the following four aspects of estimation

TABLE 7. Selected research article.

ID	TITLE	TYPE	YEAR	REFS.
A1	"A hybrid machine learning approach to network anomaly detection"	Jour.	2007	[31]
A2	"High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning"	Jour.	2016	[32]
A3	"Network anomaly detection with the restricted Boltzmann machine"	Conf.	2013	[13]
A4	"Multiple kernel learning for heterogeneous anomaly detection: algorithm and aviation safety case study"	Conf.	2010	[33]
A5	"Unsupervised Anomaly Detection with Generative Adversarial Networks to Guide Marker Discovery"	Conf.	2017	[3]
A6	"Enhancing one-class support vector machines for unsupervised anomaly detection"	Jour.	2013	[34]
A7	"The practice on using machine learning for network anomaly intrusion detection"	Conf.	2011	[35]
A8	"Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree algorithm"	Conf.	2012	[36]
A9	"An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection"	Jour.	2012	[37]
A10	"An analysis of supervised tree based classifiers for intrusion detection system"	Conf.	2013	[38]
A11	"A novel hybrid intrusion detection method integrating anomaly detection with misuse detection"	Jour.	2013	[39]
A12	"Performance Metric Selection for Autonomic Anomaly Detection on Cloud Computing Systems"	Conf.	2011	[40]
A13	"A novel unsupervised classification approach for network anomaly detection by k-Means clustering and ID3 decision tree learning methods"	Jour.	2009	[41]
A14	"Anomaly detection using Support Vector Machine classification with k-Medoids clustering"	Conf.	2012	[42]
A15	"A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection"	Conf.	2016	[43]
A16	"FRaC: a feature-modeling approach for semi-supervised and unsupervised anomaly detection"	Jour.	2011	[44]
A17	"AnyOut: Anytime Outlier Detection on Streaming Data"	Conf.	2012	[45]
A18	"Real-Time Anomaly Detection Framework for Many-Core Router through Machine-Learning Techniques"	Jour.	2016	[46]
A19	"Ensemble-learning Approaches for Network Security and Anomaly Detection"	Conf.	2017	[47]
A20	"Anomaly Detection Using an Ensemble of Feature Models"	Conf.	2011	[48]
A21	"Network intrusion detection with Fuzzy Genetic Algorithm for unknown attacks"	Conf.	2013	[49]
A22	"Intrusion detection in SCADA systems using machine learning techniques"	Conf.	2014	[50]
A23	"A machine learning framework for network anomaly detection using SVM and GA"	Conf.	2005	[51]
A24	"Anomaly-based network intrusion detection: Techniques, systems and challenges"	Jour.	2008	[52]
A25	"Evolutionary neural networks for anomaly detection based on the behavior of a program"	Conf.	2005	[53]
A26	"Anomaly detection in aircraft data using Recurrent Neural Networks (RNN)"	Conf.	2016	[54]
A27	"Centered Hyperspherical and Hyperellipsoidal One-Class Support Vector Machines for Anomaly Detection in Sensor Networks"	Conf.	2010	[55]
A28	"Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction"	Conf.	2014	[56]
A29	"Hybrid Approach for Detection of Anomaly Network Traffic using Data Mining Techniques"	Conf.	2012	[57]
A30	"Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach"	Conf.	2015	[58]
A31	"Flow-based anomaly detection in high-speed links using modified GSA-optimized neural network"	Jour.	2012	[59]
A32	"Anomaly detection in vessel tracks using Bayesian networks"	Jour.	2013	[60]
A33	"Opprentice: Towards Practical and Automatic Anomaly Detection Through Machine Learning"	Conf.	2015	[61]
A34	"Unsupervised Clustering Approach for Network Anomaly Detection"	Conf.	2012	[62]
A35	"Fuzzy logic-based anomaly detection for embedded network security cyber sensor"	Conf.	2011	[63]
A36	"Sequential anomaly detection based on temporal-difference learning: Principles, models and case studies"	Jour.	2009	[64]
A37	"Analysis of network traffic features for anomaly detection"	Jour.	2014	[65]
A38	"Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN"	Jour.	2015	[66]
A39	"A Hybrid Network Anomaly and Intrusion Detection Approach Based on Evolving Spiking Neural Network Classification"	Conf.	2014	[67]
A40	"Toward an Online Anomaly Intrusion Detection System Based on Deep Learning"	Conf.	2016	[68]

TABLE 7. *(Continued.)* Selected research article.

A41	"Unsupervised real-time anomaly detection for streaming data"	**Jour.**	**2017**	[69]
A42	"Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model"	**Jour.**	**2017**	[70]
A43	"MADAM: A Multi-level Anomaly Detector for Android Malware"	**Conf.**	**2012**	[71]
A44	"Anomaly Detection Through a Bayesian Support Vector Machine"	**Jour.**	**2010**	[72]
A45	"Sleep stage classification using unsupervised feature learning"	**Jour.**	**2012**	[73]
A46	"Toward a more practical unsupervised anomaly detection system"	**Jour.**	**2011**	[74]
A47	"A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks"	**Jour.**	**2017**	[75]
A48	"An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection"	**Jour.**	**2011**	[76]
A49	"Anomaly Detection in GPS Data Based on Visual Analytics"	**Conf.**	**2010**	[77]
A50	"A data mining approach for fault diagnosis: An application of anomaly detection algorithm"	**Jour.**	**2014**	[78]
A51	"Systematic construction of anomaly detection benchmarks from real data"	**Jour.**	**2013**	[79]
A52	"Anomaly detection in streaming environmental sensor data: A data-driven modeling approach"	**Jour.**	**2009**	[80]
A53	"Anomaly Detection in Medical Wireless Sensor Networks using Machine Learning Algorithms"	**Conf.**	**2015**	[81]
A54	"Anomaly intrusion detection based on PLS feature extraction and core vector machine"	**Jour.**	**2012**	[82]
A55	"Transferred Deep Learning for Anomaly Detection in Hyperspectral Imagery"	**Jour.**	**2017**	[83]
A56	"A close look on n-grams in intrusion detection: anomaly detection vs. classification"	**Conf.**	**2013**	[84]
A57	"Robust tensor subspace learning for anomaly detection"	**Jour.**	**2011**	[85]
A58	"Anomaly Detection with Robust Deep Autoencoders"	**Conf.**	**2017**	[86]
A59	"UBL: unsupervised behavior learning for predicting performance anomalies in virtualized cloud systems"	**Conf.**	**2012**	[87]
A60	"Direct Robust Matrix Factorizatoin for Anomaly Detection"	**Conf.**	**2011**	[88]
A61	"Anomaly Detection via Online Oversampling Principal Component Analysis"	**Jour.**	**2012**	[89]
A62	"Generic and Scalable Framework for Automated Time-series Anomaly Detection"	**Conf.**	**2015**	[90]
A63	"Sensor fault and patient anomaly detection and classification in medical wireless sensor networks"	**Conf.**	**2013**	[91]
A64	"Anomaly Detection for Hyperspectral Images Based on Robust Locally Linear Embedding"	**Jour.**	**2010**	[92]
A65	"A Robust Nonlinear Hyperspectral Anomaly Detection Approach"	**Jour.**	**2014**	[93]
A66	"Anomaly detection based on eccentricity analysis"	**Conf.**	**2014**	[94]
A67	"Data stream anomaly detection through principal subspace tracking"	**Jour.**	**2010**	[95]
A68	"A Neural Network Based Anomaly Intrusion Detection System"	**Conf.**	**2011**	[96]
A69	"Network anomaly detection through nonlinear analysis"	**Jour.**	**2010**	[97]
A70	"Frequency-based anomaly detection for the automotive CAN bus"	**Conf.**	**2015**	[98]
A71	"Context-Aware Activity Recognition and Anomaly Detection in Video"	**Conf.**	**2012**	[99]
A72	"An Anomaly Detection Framework for Autonomic Management of Compute Cloud Systems"	**Conf.**	**2010**	[100]
A73	"Anomaly detection on time series"	**Conf.**	**2010**	[101]
A74	"Self-adaptive and dynamic clustering for online anomaly detection"	**Jour.**	**2011**	[102]
A75	"An anomaly-based botnet detection approach for identifying stealthy botnets"	**Conf.**	**2011**	[103]
A76	"Anomaly detection in ECG time signals via deep long short-term memory networks"	**Conf.**	**2015**	[104]
A77	"Detecting anomalies in people's trajectories using spectral graph analysis"	**Jour.**	**2011**	[105]
A78	"Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective"	**Jour.**	**2019**	[106]
A79	"An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks"	**Jour.**	**2005**	[107]
A80	"Learning classifiers for misuse and anomaly detection using a bag of system calls representation"	**Conf.**	**2005**	[108]
A81	"Anomaly detection based on unsupervised niche clustering with application to network intrusion detection"	**Conf.**	**2004**	[109]
A82	"A Discriminative Framework for Anomaly Detection in Large Videos"	**Conf.**	**2016**	[110]
A83	"Anomaly Detection by Using CFS Subset and Neural Network with WEKA Tools"	**Conf.**	**2018**	[111]

TABLE 7. *(Continued.)* **Selected research article.**

A84	"Online Learning and Sequential Anomaly Detection in Trajectories"	Jour.	2013	[112]
A85	"Expected similarity estimation for large-scale batch and streaming anomaly detection"	Jour.	2016	[113]
A86	"Self-Taught Anomaly Detection With Hybrid Unsupervised/Supervised Machine Learning in Optical Networks"	Jour.	2019	[114]
A87	"Anomaly detection based on unsupervised niche clustering with application to network intrusion detection"	Conf.	2004	[109]
A88	"Two-tier network anomaly detection model: a machine learning approach"	Jour.	2015	[115]
A89	"Real-time network anomaly detection system using machine learning"	Conf.	2015	[116]
A90	"Telemetry-mining: a machine learning approach to anomaly detection and fault diagnosis for space systems"	Conf.	2006	[117]
A91	"Machine learning-based anomaly detection for post-silicon bug diagnosis"	Conf.	2013	[118]
A92	"Improving one-class SVM for anomaly detection"	Conf.	2003	[119]
A93	"Machine Learning Approach for IP-Flow Record Anomaly Detection"	Conf.	2011	[120]
A94	"Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning"	Conf.	2017	[121]
A95	"Network anomaly detection based on TCM-KNN algorithm"	Conf.	2007	[122]
A96	"Seeing the invisible: forensic uses of anomaly detection and machine learning"	Jour.	2008	[123]
A97	"Anomaly Detection in Sensor Systems Using Lightweight Machine Learning"	Conf.	2013	[124]
A98	"Anomaly Detection on Shuttle data using Unsupervised Learning Techniques"	Conf.	2019	[125]
A99	"Weighting technique on multi-timeline for machine learning-based anomaly detection system"	Conf.	2015	[126]
A100	"Anomaly Detection for Key Performance Indicators Through Machine Learning"	Conf.	2018	[127]
A101	"Unsupervised Anomaly Detection in Time Series Using LSTM-Based Autoencoders"	Conf.	2019	[128]
A102	"Research and application of One-class small hypersphere support vector machine for network anomaly detection"	Conf.	2011	[129]
A103	"Anomaly detection in network traffic using extreme learning machine"	Conf.	2016	[130]
A104	"Deep Learning for Network Anomalies Detection"	Conf.	2018	[131]
A105	"Using Immune Algorithm to Optimize Anomaly Detection Based on SVM"	Conf.	2006	[132]
A106	"Detecting Anomalies in Application Performance Management System with Machine Learning Algorihms"	Conf.	2019	[133]
A107	"Learning Rules and Clusters for Anomaly Detection in Network Traffic"	Jour.	2015	[134]
A108	"Machine Learning for Anomaly Detection and Categorization in Multi-Cloud Environments"	Conf.	2017	[135]
A109	"An Anomaly Detection Scheme Based on Machine Learning for WSN"	Conf.	2009	[136]
A110	"Enhanced Network Anomaly Detection Based on Deep Neural Networks"	Jour.	2018	[137]
A111	"CESVM: Centered Hyperellipsoidal Support Vector Machine Based Anomaly Detection"	Conf.	2008	[138]
A112	"Anomaly Detection in Electrical Substation Circuits via Unsupervised Machine Learning"	Conf.	2016	[139]
A113	"An anomaly intrusion detection method using the CSI-KNN algorithm"	Conf.	2008	[140]
A114	"K-Means+ID3: A Novel Method for Supervised Anomaly Detection by Cascading K-Means Clustering and ID3 Decision Tree Learning Methods"	Jour.	2007	[141]
A115	"Toward a reliable anomaly-based intrusion detection in real-world environments"	Jour.	2016	[142]
A116	"Anomaly intrusion detection using one class SVM"	Conf.	2004	[143]
A117	"ANTIDOTE: understanding and defending against poisoning of anomaly detectors"	Conf.	2009	[144]
A118	"Network traffic anomaly detection using clustering techniques and performance comparison"	Conf.	2013	[145]
A119	"Anomaly-Based Intrusion Detection using Fuzzy Rough Clustering"	Conf.	2006	[146]
A120	"The Anomaly Detection by Using DBSCAN Clustering with Multiple Parameters"	Conf.	2011	[147]
A121	"Anomaly detection in traffic using L1-norm minimization extreme learning machine"	Jour.	2015	[148]
A122	"Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection"	Conf.	2006	[149]
A123	"Web traffic anomaly detection using C-LSTM neural networks"	Jour.	2018	[150]
A124	"Android anomaly detection system using machine learning classification"	Conf.	2015	[148]
A125	"Anomaly Detection Using LibSVM Training Tools"	Conf.	2008	[151]
A126	"Unsupervised SVM Based on p-kernels for Anomaly Detection"	Conf.	2006	[152]
A127	"A Method for Anomaly Detection of User Behaviors Based on Machine Learning"	Jour.	2006	[153]

TABLE 7. *(Continued.)* **Selected research article.**

A128	"Anomaly-Based Intrusion Detection Using Extreme Learning Machine and Aggregation of Network Traffic Statistics in Probability Space"	**Jour.**	**2018**	[154]
A129	"Ramp loss one-class support vector machine; A robust and effective approach to anomaly detection problems"	**Jour.**	**2018**	[155]
A130	"Estimation of subsurface temperature anomaly in the Indian Ocean during recent global surface warming hiatus from satellite measurements: A support vector machine approach"	**Jour.**	**2015**	[156]
A131	"Anomaly Detection Model Based on Hadoop Platform and Weka Interface"	**Conf.**	**2016**	[157]
A132	"Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches"	**Jour.**	**2019**	[158]
A133	"Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic"	**Jour.**	**2018**	[159]
A134	"Anomaly Detection in Computer Security and an Application to File System Accesses"	**Conf.**	**2005**	[160]
A135	"Network traffic anomaly detection using machine learning approaches"	**Conf.**	**2012**	[161]
A136	"ManetSVM: Dynamic anomaly detection using one-class support vector machine in MANETs"	**Conf.**	**2013**	[162]
A137	"Semi-Supervised Anomaly Detection for EEG Waveforms Using Deep Belief Nets"	**Conf.**	**2010**	[163]
A138	"Using Machine Learning for Behavior-Based Access Control: Scalable Anomaly Detection on TCP Connections and HTTP Requests"	**Conf.**	**2013**	[164]
A139	"Applying machine learning classifiers to dynamic android malware detection at scale"	**Conf.**	**2013**	[165]
A140	"Big Data Analytics for User-Activity Analysis and User-Anomaly Detection in Mobile Wireless Network"	**Jour.**	**2017**	[166]
A141	"Anomaly detection using machine learning with a case study"	**Conf.**	**2014**	[167]
A142	"Octopus-IIDS: An anomaly based intelligent intrusion detection system"	**Conf.**	**2010**	[168]
A143	"A hybrid method based on genetic algorithm, self-organised feature map, and support vector machine for better network anomaly detection"	**Conf.**	**2013**	[169]
A144	"Anomaly Detection Support Vector Machine and Its Application to Fault Diagnosis"	**Conf.**	**2008**	[170]
A145	"Evaluation of Machine Learning-based Anomaly Detection Algorithms on an Industrial Modbus/TCP Data Set"	**Conf.**	**2018**	[171]
A146	"Network Anomaly Traffic Detection Method Based on Support Vector Machine"	**Conf.**	**2016**	[172]
A147	"Anomaly detection of spacecraft based on least squares support vector machine"	**Conf.**	**2011**	[173]
A148	"A Model Based on Hybrid Support Vector Machine and Self-Organizing Map for Anomaly Detection"	**Conf.**	**2010**	[174]
A149	"Anomaly detection in wide area network meshes using two machine learning algorithms"	**Jour.**	**2018**	[175]
A150	"Image Anomaly Detection with Generative Adversarial Networks"	**Conf.**	**2019**	[176]
A151	"Performance evaluation of BGP anomaly classifiers"	**Conf.**	**2015**	[177]
A152	"An uncertainty-managing batch relevance-based approach to network anomaly detection"	**Jour.**	**2015**	[178]
A153	"Energy Consumption Data Based Machine Anomaly Detection"	**Conf.**	**2014**	[167]
A154	"A Novel Algorithm for Network Anomaly Detection Using Adaptive Machine Learning"	**Conf.**	**2017**	[179]
A155	"Thermal anomaly prediction in data centers"	**Conf.**	**2010**	[180]
A156	"On the symbiosis of specification-based and anomaly-based detection"	**Jour.**	**2010**	[181]
A157	"A holistic smart home demonstrator for anomaly detection and response"	**Conf.**	**2015**	[182]
A158	"Online Anomaly Detection in Crowd Scenes via Structure Analysis"	**Jour.**	**2014**	[183]
A159	"Hierarchical Temporal Memory Based Machine Learning for Real-Time, Unsupervised Anomaly Detection in Smart Grid: WiP Abstract"	**Conf.**	**2020**	[184]
A160	"One-class extreme learning machines for gas turbine combustor anomaly detection"	**Conf.**	**2016**	[185]
A161	"Recurrent Neural Network Attention Mechanisms for Interpretable System Log Anomaly Detection"	**Conf.**	**2018**	[186]
A162	"Anomaly detection based on profile signature in network using machine learning technique"	**Conf.**	**2016**	[187]
A163	"Nonlinear structure of escape-times to falls for a passive dynamic walker on an irregular slope: Anomaly detection using multi-class support vector machine and latent state extraction by canonical correlation analysis"	**Conf.**	**2011**	[188]
A164	"A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks"	**Jour.**	**2018**	[189]
A165	"RoADS: A Road Pavement Monitoring System for Anomaly Detection Using Smart Phones"	**Conf.**	**2016**	[190]
A166	"Unitary Anomaly Detection for Ubiquitous Safety in Machine Health Monitoring"	**Conf.**	**2012**	[191]
A167	"An HMM-Based Anomaly Detection Approach for SCADA Systems"	**Conf.**	**2016**	[192]
A168	"Symbolic time series analysis for anomaly detection: A comparative evaluation"	**Jour.**	**2005**	[193]

TABLE 7. *(Continued.)* Selected research article.

A169	"Anomaly Detection Using Real-Valued Negative Selection"	Jour.	2003	[194]
A170	"Anomaly detection using the correlational paraconsistent machine with digital signatures of network segment"	Jour.	2017	[195]
A171	"Combining negative selection and classification techniques for anomaly detection"	Conf.	2002	[196]
A172	"A Geometric Framework for Unsupervised Anomaly Detection"	Jour.	2002	[197]
A173	"Monitoring Smartphones for Anomaly Detection"	Jour.	2008	[198]
A174	"Learning rules for anomaly detection of hostile network traffic"	Conf.	2003	[199]
A175	"System Anomaly Detection: Mining Firewall Logs"	Conf.	2006	[200]
A176	"Rule-Based Anomaly Detection on IP Flows"	Conf.	2009	[201]
A177	"Is negative selection appropriate for anomaly detection?"	Conf.	2005	[202]
A178	"Anomaly detection and classification in a laser powder bed additive manufacturing process using a trained computer vision algorithm"	Jour.	2018	[203]
A179	"Stealthy poisoning attacks on PCA-based anomaly detectors"	Jour.	2009	[204]
A180	"Fusions of GA and SVM for Anomaly Detection in Intrusion Detection System"	Conf.	2005	[205]
A181	"Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering"	Conf.	2016	[206]
A182	"An Anomaly Detection Method for Spacecraft Using Relevance Vector Learning"	Conf.	2005	[207]
A183	"ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks"	Conf.	2009	[208]
A184	"ADMIT: anomaly-based data mining for intrusions"	Conf.	2002	[209]
A185	"IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach"	Conf.	2017	[210]
A186	"Defying the gravity of learning curve: a characteristic of nearest neighbour anomaly detectors"	Jour.	2016	[211]
A187	"Detecting Anomaly in Videos from Trajectory Similarity Analysis"	Conf.	2007	[212]
A188	"An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks"	Jour.	2005	[107]
A189	"DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning"	Conf.	2017	[213]
A190	"Anomaly detection in earth dam and levee passive seismic data using support vector machines and automatic feature selection"	Jour.	2017	[214]
A191	"MS-LSTM: A multi-scale LSTM model for BGP anomaly detection"	Conf.	2016	[215]
A192	"SAD: web session anomaly detection based on parameter estimation"	Jour.	2004	[216]
A193	"Evolutionary Learning Program's Behavior in Neural Networks for Anomaly Detection"	Conf.	2004	[217]
A194	"Spatio-Temporal AutoEncoder for Video Anomaly Detection"	Conf.	2017	[218]
A195	"Robust feature selection and robust PCA for internet traffic anomaly detection"	Conf.	2012	[219]
A196	"Deep Anomaly Detection with Deviation Networks"	Conf.	2019	[220]
A197	"Machine learning and transport simulations for groundwater anomaly detection"	Jour.	2020	[221]
A198	"Unsupervised machine learning for network-centric anomaly detection in IoT"	Conf.	2019	[222]
A199	"Hybrid Machine Learning for Network Anomaly Intrusion Detection"	Conf.	2020	[223]
A200	"An anomaly prediction framework for financial IT systems using hybrid machine learning methods"	Jour.	2019	[224]
A201	"Kernel Eigenspace Separation Transform for Subspace Anomaly Detection in Hyperspectral Imagery"	Jour.	2007	[225]
A202	"An unsupervised anomaly intrusion detection algorithm based on swarm intelligence"	Conf.	2005	[226]
A203	"Maritime situation analysis framework: Vessel interaction classification and anomaly detection"	Conf.	2015	[227]
A204	"An ensemble learning framework for anomaly detection in building energy consumption"	Jour.	2017	[228]
A205	"Ensemble methods for anomaly detection and distributed intrusion detection in Mobile Ad-Hoc Networks"	Jour.	2008	[229]
A206	"Unsupervised Anomaly Intrusion Detection via Localized Bayesian Feature Selection"	Conf.	2011	[230]
A207	"McPAD: A multiple classifier system for accurate payload-based anomaly detection"	Jour.	2009	[231]
A208	"Detecting errors within a corpus using anomaly detection"	Conf.	2000	[232]
A209	"Efficient Top Rank Optimization with Gradient Boosting for Supervised Anomaly Detection"	Conf.	2017	[233]
A210	"Semi-supervised learning based big data-driven anomaly detection in mobile wireless networks"	Jour.	2018	[234]
A211	"Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis"	Jour.	2015	[235]

TABLE 7. *(Continued.)* **Selected research article.**

A212	"Spatial anomaly detection in sensor networks using neighborhood information"	**Jour.**	**2017**	[236]
A213	"Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks"	**Conf.**	**2017**	[237]
A214	"Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems"	**Jour.**	**2015**	[238]
A215	"A hybrid approach for efficient anomaly detection using metaheuristic methods"	**Jour.**	**2015**	[239]
A216	"Experience Report: System Log Analysis for Anomaly Detection"	**Conf.**	**2016**	[19]
A217	"Towards Learning Normality for Anomaly Detection in Industrial Control Networks"	**Conf.**	**2013**	[240]
A218	"Anomaly detection approach using hybrid algorithm of data mining technique"	**Conf.**	**2017**	[241]
A219	"Adaptive Anomaly Identification by Exploring Metric Subspace in Cloud Computing Infrastructures"	**Conf.**	**2013**	[242]
A220	"Towards reliable data feature retrieval and decision engine in host-based anomaly detection systems"	**Conf.**	**2015**	[243]
A221	"Using an Ensemble of One-Class SVM Classifiers to Harden Payload-based Anomaly Detection Systems"	**Conf.**	**2006**	[244]
A222	"An anomaly detection method to detect web attacks using Stacked Auto-Encoder"	**Conf.**	**2018**	[245]
A223	"Anomaly Detection Enhanced Classification in Computer Intrusion Detection"	**Conf.**	**2002**	[246]
A224	"Simple, state-based approaches to program-based anomaly detection"	**Jour.**	**2002**	[247]
A225	"Adaptive anomaly detection with evolving connectionist systems"	**Jour.**	**2007**	[248]
A226	"Enhancing Anomaly Detection Using Temporal Pattern Discovery"	**Jour.**	**2009**	[249]
A227	"Anomaly Detection in IPv4 and IPv6 networks using machine learning"	**Conf.**	**2015**	[250]
A228	"A training-resistant anomaly detection system"	**Jour.**	**2018**	[251]
A229	"Conditional Anomaly Detection"	**Jour.**	**2007**	[252]
A230	"An anomaly detection in smart cities modeled as wireless sensor network"	**Conf.**	**2016**	[253]
A231	"Spatiotemporal Anomaly Detection in Gas Monitoring Sensor Networks"	**Conf.**	**2008**	[254]
A232	"Using Naive Bayes with AdaBoost to Enhance Network Anomaly Intrusion Detection"	**Conf.**	**2010**	[255]
A233	"Applying both positive and negative selection to supervised learning for anomaly detection"	**Conf.**	**2005**	[256]
A234	"Real-time camera anomaly detection for real-world video surveillance"	**Conf.**	**2011**	[257]
A235	"Network Anomaly Detection with Stochastically Improved Autoencoder Based Models"	**Conf.**	**2017**	[258]
A236	"Learning deep event models for crowd anomaly detection"	**Jour.**	**2017**	[259]
A237	"GANomaly: Semi-supervised Anomaly Detection via Adversarial Training"	**Conf.**	**2018**	[260]
A238	"Mote-Based Online Anomaly Detection Using Echo State Networks"	**Conf.**	**2009**	[261]
A239	"Genetic algorithm with different feature selection techniques for anomaly detectors generation"	**Conf.**	**2013**	[262]
A240	"RawPower: Deep Learning based Anomaly Detection from Raw Network Traffic Measurements"	**Conf.**	**2018**	[263]
A241	"Network security and anomaly detection with Big-DAMA, a big data analytics framework"	**Conf.**	**2017**	[264]
A242	"An efficient hidden Markov model training scheme for anomaly intrusion detection of server applications based on system calls"	**Conf.**	**2004**	[265]
A243	"An anomaly detection framework for BGP"	**Conf.**	**2011**	[266]
A244	"Semantic anomaly detection in online data sources"	**Conf.**	**2002**	[267]
A245	"A framework for efficient network anomaly intrusion detection with features selection"	**Conf.**	**2018**	[268]
A246	"Cross-Layer Based Anomaly Detection in Wireless Mesh Networks"	**Conf.**	**2009**	[269]
A247	"Reducing calculation requirements in FPGA implementation of deep learning algorithms for online anomaly intrusion detection"	**Conf.**	**2017**	[270]
A248	"Anomaly detection in network traffic using K-mean clustering"	**Conf.**	**2016**	[271]
A249	"Stream-based Machine Learning for Network Security and Anomaly Detection"	**Conf.**	**2018**	[272]
A250	"Multivariate Online Anomaly Detection Using Kernel Recursive Least Squares"	**Conf.**	**2007**	[273]
A251	"A Hybrid Autoencoder and Density Estimation Model for Anomaly Detection"	**Conf.**	**2016**	[274]
A252	"Optimizing false positive in anomaly based intrusion detection using Genetic algorithm"	**Conf.**	**2016**	[275]
A253	"Deep-anomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes"	**Jour.**	**2018**	[276]
A254	"Group Anomaly Detection Using Deep Generative Models"	**Conf.**	**2019**	[277]

TABLE 7. *(Continued.)* **Selected research article.**

A255	"Anomaly Detection in IaaS Clouds"	**Conf.**	**2013**	[278]
A256	"An ensemble framework of anomaly detection using hybridized feature selection approach (HFSA)"	**Conf.**	**2015**	[279]
A257	"Anomaly detection combining one-class SVMs and particle swarm optimization algorithms"	**Jour.**	**2011**	[280]
A258	"Anomaly detection through on-line isolation Forest: An application to plasma etching"	**Conf.**	**2017**	[281]
A259	"Practical anomaly detection based on classifying frequent traffic patterns"	**Conf.**	**2012**	[282]
A260	"A hybrid model for anomaly-based intrusion detection in SCADA networks"	**Conf.**	**2018**	[283]
A261	"CH-SVM Based Network Anomaly Detection"	**Conf.**	**2007**	[284]
A262	"MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks"	**Conf.**	**2019**	[285]
A263	"Anomaly Detection from Network Logs Using Diffusion Maps"	**Conf.**	**2011**	[286]
A264	"A Deep Learning Approach for Network Anomaly Detection Based on AMF-LSTM"	**Conf.**	**2018**	[287]
A265	"Reducing Features of KDD CUP 1999 Dataset for Anomaly Detection Using Back Propagation Neural Network"	**Conf.**	**2015**	[288]
A266	"Online Anomaly Prediction for Robust Cluster Systems"	**Conf.**	**2009**	[289]
A267	"A study on anomaly detection ensembles"	**Jour.**	**2017**	[290]
A268	"Big data analytics for network anomaly detection from netflow data"	**Conf.**	**2017**	[291]
A269	"An anomaly-based network intrusion detection system using Deep learning"	**Conf.**	**2017**	[292]
A270	"An Empirical Evaluation of Deep Learning for Network Anomaly Detection"	**Conf.**	**2018**	[293]
A271	"Network Anomaly Detection Using Random Forests and Entropy of Traffic Features"	**Conf.**	**2013**	[294]
A272	"Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks"	**Conf.**	**2007**	[295]
A273	"Anomaly based intrusion detection using meta ensemble classifier"	**Conf.**	**2012**	[296]
A274	"Applying Machine Learning to Anomaly-Based Intrusion Detection Systems"	**Conf.**	**2019**	[297]
A275	"Collective Anomaly Detection Based on Long Short-Term Memory Recurrent Neural Networks"	**Conf.**	**2016**	[298]
A276	"AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning"	**Conf.**	**2019**	[299]
A277	"Less is More: Building Selective Anomaly Ensembles"	**Jour.**	**2016**	[300]
A278	"The best of both worlds: a framework for the synergistic operation of host and cloud anomaly-based IDS for smartphones"	**Conf.**	**2014**	[301]
A279	"A-GHSOM: An adaptive growing hierarchical self-organizing map for network anomaly detection"	**Jour.**	**2012**	[302]
A280	"Single-image splicing localization through autoencoder-based anomaly detection"	**Conf.**	**2017**	[303]
A281	"Efficacy of Hidden Markov Models Over Neural Networks in Anomaly Intrusion Detection"	**Conf.**	**2006**	[304]
A282	"An approach to spacecraft anomaly detection problem using kernel feature space"	**Conf.**	**2005**	[305]
A283	"Machine Learning in Anomaly Detection: Example of Colluded Applications Attack in Android Devices"	**Conf.**	**2019**	[306]
A284	"Optimal virtual machine selection for anomaly detection using a swarm intelligence approach"	**Jour.**	**2019**	[307]
A285	"Anomaly Detection in Power Quality Measurements Using Proximity-Based Unsupervised Machine Learning Techniques"	**Conf.**	**2019**	[308]
A286	"Network-Wide Traffic Anomaly Detection and Localization Based on Robust Multivariate Probabilistic Calibration Model"	**Jour.**	**2015**	[309]
A287	"Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities."	**Jour.**	**2020**	[310]
A288	"Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control. "	**Jour.**	**2020**	[311]
A289	"Anomaly detection in electronic invoice systems based on machine learning"	**Conf.**	**2020**	[312]
A290	"Anomaly detection in wireless sensor network using machine learning algorithm"	**Jour.**	**2020**	[313]
A291	"A Hybrid Unsupervised Clustering-Based Anomaly Detection Method"	**Jour.**	**2020**	[314]
A292	"Network traffic anomalies detection and identification with flow monitoring"	**Conf.**	**2008**	[315]
A293	"Network Traffic Anomaly Detection and Prevention, Concepts"	**Jour.**	**2017**	[316]
A294	"Network Traffic Anomaly Detection Based on Information Gain and Deep Learning"	**Conf.**	**2019**	[317]
A295	"Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation"	**Conf.**	**2005**	[318]
A296	"Network traffic anomalies detection and identification with flow monitoring"	**Conf.**	**2008**	[315]
A297	"Network Traffic Anomaly Detection and Prevention, Concepts"	**Jour.**	**2017**	[316]

TABLE 8. Performance metrics among selected papers.

ID	Type	ML Model	Performance Metrics	value	Dataset
A1	supervised and unsupervised	enhanced SVM	Detection Rate (DR)	87.74	MIT Lincoln Lab
			False Positive Rate (FPR)	10.2	
			False Negative Rate (FNR)	NA	
			Processing Time (PT)	27.27	
A2	unsupervised	DBN with 1SVM	Area Under Curve (AUC)	0.9863	six real life data set from UCI machine learning repository and two synthetic "Banana" and "Smiley"
			Accuracy (ACC)	0.0625	
			Testing Time	0.2093	
A3	semi-supervised	DRBM	Accuracy (ACC)	0.94	KDD99
A4	semi-supervised	multipule kernel	Statistics Discrete	19	Flight Data Recorders
			Statistics Continouss	94	
			Statistics Heterogneous	114	
A5	unsupervised	Generative Adversarial Network (GAN)	Precision	0.8834	real-life-datasets
			Recall	0.7277	
			Sensitivity	0.7279	
			Specificity	0.8928	
			Area Under Curve (AUC)	0.89	
A6	unsupervised	eta one-class SVM	Area Under Curve (AUC)	0.9972	UCI machine learning repository
			CPU execution	27.48±0.25 ms	
A7	supervised and unsupervised	J48	Accuracy (ACC)	(99.6298% - 99.9767%)	KDD99
A8	supervised	k-Means with C4.5	F-Score	94	KDD99
			True Positive Rate (TPR)	99.6	
			False Positive Rate (FPR)	0.1	
			Accuracy (ACC)	95.8	
			Precision	95.6	
A9	na	SVM + DT + SA	Accuracy (ACC)	99.96%	KDD99
A10	supervised	Random Tree	Mean Absolute Error (MAE)	0.0321	NSL-KDD 99
			Root Mean squared Error (RMSE)	0.0321	
			Kappa Statistics	0.8926	
			Error Measure	0.254	
			Recall	0.968	
			Precision	0.968	
			F-Score	0.968	
			False Alarm Rate(FAR)	0.074	
			Accuracy (ACC)	0.9974	
A11	na	one class SVM with C4.5	False Positive Rate (FPR)		NSL-KDD 99
			Testing Time	11.2	
A12	semi-supervised	decision tree	NA	NA	NA
A13	unsupervised	ID3 decision tree + k-Means clustering	Sensitivity	0.961538	real evaluation test bed network datasets
			Specificity	0.999747	
			Negative likelihood	0.038471	
			Positive Predictive Ratio	0.981567	
			Negative Predictive Ratio	0.999444	
A14	unsupervised	SVM + K-Medoids clustering	Accuracy (ACC)	99.79	Kyoto2006+ data set and KDD Cup 1999
			Detection Rate (DR)	99.87	
			False Alarm Rate(FAR)	0.99	
A15	supervised	SVM + Random Forest	Accuracy (ACC)	97.5	NSL-KDD99 dataset
			Sensitivity	93.49	
			Specificity	98.38	
			Precision	97.6	
			Recall	97.6	
A16	semi-supervised and unsupervised	FRaC	Area Under Curve (AUC)	1	UCI machine learning repository
A17	supervised	Cluster	Area Under Curve (AUC)	0.996	UCI machine learning repository
A18	supervised and unsupervised	SVM	Accuracy (ACC)	95% to 97%	"Golden Dataset" for Real-Time Anomaly Detection
			Precision	NA	
			Recall	NA	
A19	supervised	Super Learner ensemble learning model	Area Under Curve (AUC)	0.999	MAWILab dataset
			False Positive Rate (FPR)	5%	
			Detection Rate (DR)	97%	
A20	semi-supervised	FRaC	Area Under Curve (AUC)	0.9	UCI machine learning repository
A21	supervised	fuzzy genetic algorithm	Detection Rate (DR)	97.92	KDD99 dataset
			False Negative Rate (FNR)	4.10%	
			False Positive Rate (FPR)	1.13%	
A22	supervised	one-class SVM	Accuracy (ACC)	98.8796	network dataset

TABLE 8. *(Continued.)* **Performance metrics among selected papers.**

A23	supervised and unsupervised	SVM + GA	Correction Rate	94.7	MIT Lincoln Lab
			False Positive Rate (FPR)	5.23	
			False Negative Rate (FNR)	NA	
A24	supervised	NA	NA	NA	NA
A25	supervised	evolutionary neural networks	False Alarm Rate(FAR)	0.7	1999 DARPA IDEVAL dataset
			Detection Rate (DR)	100%	
A26	semi-supervised and unsupervised	Recurrent Neural Networks (RNN)	Precision	1	X-Plane simulation
			Recall	0.818	
			F-Score	0.89	
A27	NA	(CESVM) and (QSSVM)	Detection Rate (DR)	80%	UCI machine learning repository
			Area Under Curve (AUC)	0.9932	
A28	unsupervised	autoencoder	Area Under Curve (AUC)	0.9764	spacecrafts' telemetry data and generated data from Lorenz system
A29	NA	SVM + Entropy	Correctly Classification rate (CCR)	97.25%	MIT Lincoln (DARPA, 1999)
			Misclassified Rate (MR)	2.75%	
A30	NA	Neighborhood Outlier Factor (NOF)	Detection Rate (DR)	2400	KDD cup 99 dataset
			CPU Utilization	10%	
			Testing Time	95000 ms	
A31	supervised	modified gravitational search algorithm (MGSA)	Correctly Classification rate (CCR)	97.76	NA
			Misclassified Rate (MR)	2.48	
			False Alarm Rate(FAR)	0.21	
			Error Rate	2.24	
A32	unsupervised	Bayesian networks	Area Under Curve (AUC)	0.727	real world Automated Identification System
			False Positive Rate (FPR)	NA	
			True Positive Rate (TPR)	NA	
A33	supervised	random forest	Precision	0.89	KPI data
A34	unsupervised	Clustering algorithms	Accuracy (ACC)	80.15%	NSL-KDD
			False Positive Rate (FPR)	21.14%	
A35	unsupervised	Fuzzy Rule Based	Correctly Classification rate (CCR)	99.36%	set of network data recorded from an experimental test-bed mimicking the environment of a critical infrastructure control system.
			False Negative Rate (FNR)	0.90%	
			Testing Time	0.212 ms	
A36	supervised	TD	False Alarm Rate(FAR)	0.002951	real life time data
A37	supervised	filters and regerssion wrappers	Accuracy (ACC)	99.21±0.04	NSL-KDD
			Area Under Curve (AUC)	0.997±0.001	
			Recall	99.16±0.12	
			Precision	99.57±0.05	
A38	NA	Fuzzy Means clustering algorithm and Artificial Neural Network	Precision	99.94	DARPA's KDD cup dataset 1999
			Recall	97.2	
			F-Score	99.32	
			Detection Rate (DR)	99.96	
			False Alarm Rate(FAR)	0.2	
A39	supervised and unsupervised	evolving Spiking Neural Network	Accuracy (ACC)	99.90%	KDD Cup 1999 data
A40	unsupervised	deep belief network using Logistic Regression	Accuracy (ACC)	97.90%	DARPA KDDCUP'99 dataset
			True Positive Rate (TPR)	97.51%	
			True Negative Rate (TNR)	99.48%	
			False Positive Rate (FPR)	0.51%	
			False Negative Rate (FNR)	2.48%	
A41	unsupervised	Hierarchical Temporal Memory (HTM)	Preditición Error	NA	Benchmark dataset (NAB)
			CPU Utilization	NA	
A42	supervised and unsupervised		Accuracy (ACC)	99.9	NSL-KDD dataset
			True Positive Rate (TPR)	0.997	
			False Positive Rate (FPR)	0.003	
A43	NA	K-Nearest Neighbors	CPU Utilization	7%	NA
			False Positive Rate (FPR)	0.000171	
A44	supervised	CALCEsvm	Accuracy (ACC)	94%	NA
A45	unsupervised	DBN	Accuracy (ACC)	72.2±9.7	Benchmark Dataset and Home Sleep Dataset
A46	unsupervised	cluster + 1-SVM	Accuracy of normal data (ACC)	100%	real traffic data
			Accuracy of attack data (ACC)	79%	
			False Negative Rate (FNR)	0.10%	
			False Positive Rate (FPR)	20.50%	
A47	supervised	RNN	Detection Rate (DR)	97.09%	benchmark NSL-KDD dataset
			Accuracy (ACC)	81.29%	
			False Positive Rate (FPR)	0.07	
A48	unsupervised	SVM	Detection Rate (DR)	87.64	1998 DARPA
			False Alarm Rate(FAR)	6.73	

TABLE 8. *(Continued.)* Performance metrics among selected papers.

A49	supervised	conditional random field	Accuracy (ACC)	0.81	GPS data
			Query by Committee	0.9	
A50	supervised	SVM	Accuracy (ACC)	97%	NSF I/UCR Center
A51	NA	Isolation Forest model (IF)	Area Under Curve (AUC)	17	benchmark dataset
		Ensemble Gaussian Mixture Model (egmm)	Area Under Curve (AUC)	14	
A52	NA	NC + MLP + LC +AD	False Positive Rate (FPR)	5.18%	UCI machine learning repository
		NC + MLP + LC+ AD	False Negative Rate (FNR)	5.30%	
		NC + MLP + LC+ ADAM	False Positive Rate (FPR)	6.38%	
		NC + MLP + LC+ ADAM	False Negative Rate (FNR)	0.00%	
A53	NA	Random Forest (RF) + Linear Regression (LR)	Mean Absolute Error(MAE)	0.0145	real medical datasets
			Testing Time	1.43 s	
A54	NA	core Vector Machine	CPU Execution Time	2.72 s	KDD'99 dataset
			Support Vector	21	
			Detection Rate (DR)	99.74%	
			Accuracy (ACC)	99.87%	
A55	NA	convolutional neural network	Accuracy (ACC)	98.28	Airborne Visible/Infrared Imaging Spectrometer and AVIRIS sensor data
			Testing Time	483 s	
A56	NA	SVM	True Positive Rate (TPR)	81.50%	DARPA IDS evaluation dataset
			False Positive Rate (FPR)	0.01	
A57	NA	NA	similarity measurment	NA	two video sequence
A58	supervised and unsupervised	neural network	F-Score	0.64	MNIST dataset
			Recall	0.64	
			Precision	0.64	
A59	unsupervised	Self Organizing Map (SOM)	True Positive Rate (TPR)	98%	IBM Systems and MemLeak and NetHog dataset
			False Positive Rate (FPR)	1.70%	
A60	unsupervised	DRMF	Precision	0.805	simulation and real-world data set
			Testing Time	23.760 s	
A61	NA	PCA	Area Under Curve (AUC)	0.9987	KDD data set
			CPU Execution Time	2.697 s	
			True Positive Rate (TPR)	0.9133±0.0327	
			False Positive Rate (FPR)	0.0697±0.0188	
A62	unsupervised	Extensible Generic	Accuracy (ACC)	0.9	real and synthetic data
A63	NA	decision tree (DT) and linear regression (LR)	True Positive Rate (TPR)	100%	real patient datasets from Physionet database
			False Positive Rate (FPR)	7.40%	
A64	NA	Linear Embedding (LE)	Testing Time	29.1	data from Hyperion on the EO-1 satellite and HYDICE on an airborne platform
A65	unsupervised	kernel + regression	Area Under Curve (AUC)	0.89669	nonlinear synthetic data
A66	NA	NA	NA	NA	NA
A67	NA	NA	F-Score	0.86	Abilene datasets and ISP datasets
A68	NA	neural network	Detection Rate (DR)	90%	KDD'99
			Positive rate (PR)	3%	
A69	supervised	SVM	Correctly Classification rate (CCR)	98.24%	DARPA dataset
			Misclassified Rate (MR)	1.46%	
			Precision	0.985	
			Recall	1	
			Mean Absolute Error(MAE)	0.015	
			Kappa Statistics	0.646	
			Area Under Curve (AUC)	0.949	
A70	NA	one-class support vector	Area Under Curve (AUC)	0.9905	CAN bus data from a 2011 Ford Explorer
			Testing Time	0.4 s	
A71	NA	SVM	Area Under Curve (AUC)	(video clips) 79.8%	VIRATGroundDataset
			Area Under Curve (AUC)	(continuous videos) 68.5%	
A72	unsupervised	Bayesian Network + PCA	NA	NA	NA
A73	supervised	k-NN	False Alarm Rate(FAR)	0.225	UCR time series classification/clustering page
			Computational Cost	0.025	
A74	unsupervised	SOM + k-means	Detection Rate (DR)	0.966	KDD cup 99 dataset and Kyoto data set
			False Positive Rate (FPR)	0.13	
A75	NA	cluster	Detection Rate (DR)	100%	database produced by Domain-IP Mapping component
A76	NA	neural network	F-Score	0.9645	MIT-BIH Arrhythmia Database
			Precision	0.975	
			Recall	0.4647	
			False Positive Rate (FPR)	0.0119	
			True Positive Rate (TPR)	39.05	

TABLE 8. ***(Continued.)*** **Performance metrics among selected papers.**

A77	unsupervised	NA	NA	NA	Edinburgh Informatics Forum Pedestrian Database
A78	supervised	RBM and SVM	Detection Rate (DR)	99.04	real-time and benchmark datasets
			False Positive Rate (FPR)	1.31	
			Accuracy (ACC)	99.98	
			Precision	99.03	
			F-Score	99.5	
A79	supervised and unsupervised	SOM + J.48	Detection Rate (DR)	99.90%	KDD cup 99 dataset
			Correctly Classification rate (CCR)	99.84	
			False Positive Rate (FPR)	1.25	
A80	unsupervised	one class Naive Bayes algorithm and K-Means clustering	Accuracy (ACC)	99.28%	MIT Lincoln Labs and University of New Mexico (UNM)) system call sequences
			Detection Rate (DR)	100%	
			False Positive Rate (FPR)	1.29	
A81	unsupervised	clustering	Accuracy (ACC)	95.7	synthetic and real data sets (KDDCup'99 data set and Wisconsin Breast Cancer and Indian Diabetes)
			Detection Rate (DR)	96.32	
			False Positive Rate (FPR)	7.75	
A82	unsupervised	NA	Area Under Curve (AUC)	0.91	Avenue Dataset and Subway surveillance dataset and the Personal Vacation Dataset and the UMN Unusual Activity Dataset
A83	supervised and unsupervised	Neural network + CFS	CPU Utilization	13%	trained data of about two thousand connection records and test data includes five thousand connection records and a group of forty-one derived features received from every connection
			Detection Rate (DR)	83%	
			Testing Time	110000 ms	
A84	supervised and unsupervised	SHNN-CAD	Accuracy (ACC)	88.3	four different labeled trajectory datasets
			F-Score	0.75	
			Detection Delay	10.3	
A85	unsupervised	kernel methods (EXPoSE)	Area Under Curve (AUC)	1.85	smaller benchmark datasetswithknownanomalyclasse and KDD'99 cup and forest cover type
			Accuracy (ACC)	1.7	
A86	supervised and unsupervised	DCM and DCRM	False Negative Rate (FNR)	0.91	testbed
			False Positive Rate (FPR)	0.07	
			Freq. of validation	29.82	
A87	unsupervised	Niche Clustering	accuracy	96.99%	synthetic and real data set KDDCup'99
A88	NA	Naïve Bayes, KNN	Detection Rate (DR)	83.24	NSL-KDD
			False Alarm Rate(FAR)	4.83	
A89	NA	SVM	cross-validation	90.3	na
A90	NA	Relevance Vector Machine (RVM) and Dynamic Bayesian Network	Ratio of Thruster, Estimated Outputs of All Thrusters	na	Rendezvous Simulation
A91	NA	temporal relations	Anomaly mean	0.76	real data of raw sensor data and synthetic data of instances of a predefined set of activities
			Anomaly standard deviation	0.14	
			Anomaly threshold	0.99	
A92	NA	One-class SVM	Accuracy (ACC)	96%	1999 DARPA audit logs
A93	unsupervised	OCSVM	Accuracy (ACC)	93.8	Flame website dataset plus extending it with their own
			False Positive Rate (FPR)	0.1	
			True Negative Rate (TNR)	100	
A94	NA	SVM DNN	Precision	98.2	SWaT testbed
			Recall	69.9	
			F-Score	80.2	
A95	NA	TCM-KNN	True Positive Rate (TPR)	99.48	KSS Cup 1999
			True Negative Rate (TNR)	2.81	
A96	NA	na	Detection Rate (DR)	100	generated dataset
A97	NA	Recursive Least Squares (RLS)	True Positive Rate (TPR)	21	3 synthetic datasets and the real-world datase
			True Negative Rate (TNR)	4.9	
A98	unsupervised	OneClassSVM Local Outlier Factor LOF isolation forest Elliptic Envelope	Precision	99%	Shuttle dataset satellite dataset
			Recall	99%	
			F-Score	99%	
A99	NA	knearest neighbor, and one-class support vector machine	F-Score	na	real life time data
A100	NA	LSTM Gradient Boosting Regression Trees	Precision	92%	na
			Recall	63.94%	
			F-Score	89.37	

TABLE 8. *(Continued.)* **Performance metrics among selected papers.**

A101	unsupervised	OneClassSVM LSTM	Accuracy (ACC)	87%	DCASE
A102	NA	One-class small hypersphere support vector machine classifier (OCSHSVM)	Precision	98.17%	NSL-KDD
			Recall	97.16%	
A103	NA	ELM	Accuracy (ACC)	99.94%	NSL-KDD
A104	unsupervised	AE K-Means	Accuracy (ACC)	995	KDD99
			Precision	99%	
A105	NA	SVM	Detection Time	25.43s	na
			Accuracy (ACC)	96.57%	
A106	NA	xgboost	Precision	80.64%	real world dataset
			Recall	78.23%	
			F-Score	79%	
A107	NA	LERAD CLAD	na	na	DARPA 99
A108	supervised	LR + RF	Accuracy (ACC)	99%	UNSW
			categorizing Accuracy	93.60%	
A109	NA	Bayesian	False Positive Rate (FPR)	3%	DAPRA 1998
			Detection Rate (DR)	99%	
A110	NA	DCNN + LSTM	Accuracy (ACC)	89%	NSLKDD
A111	NA	centered hyperellipsoidal support vector machine CESVM	Detection Rate (DR)	80%	real world dataset
			False Positive Rate (FPR)	10%	
A112	unsupervised	na	Detection Rate (DR)	92.06%	RTDS
A113	NA	CSI-KNN	Detection Rate (DR)	94.60%	KDD99
			False Positive Rate (FPR)	3%	
			Accuracy (ACC)	95.10%	
A114	NA	K-means ID3 Decision Tree	Accuracy (ACC)	96.24%	NAD DED MSD
			False Positive Rate (FPR)	0.03%	
			True Positive Rate (TPR)	0.76%	
			F-Score	na	
			Precision	na	
A115	NA	Decision Tree	Accuracy (DT):	99.36%	DARPA1998
			FP (DT):	1.29%	
			FN (DT):	0.00%	
		Naïve Bayes	Accuracy (NB)	95.23%	
			FP (NB)	8.57%	
			FN (NB)	0.97%	
A116	unsupervised	once class SVM	Accuracy	95.50%	UNM dataset
			Detection rate	93.30%	
			False AIarm:	2.30%	
			Correlation:	0.85	
A117	NA	PCA	Detection Rate (DR)	na	Abilene (Internet2 backbone)
			False Negative Rate (FNR)	na	
			AUC	na	
A118	NA	Fuzzy c-means clustering (FCM) + K-means clustering and Gaussian mixture Model (GMM)	na	na	Netflow data
A119	unsupervised	Fuzzy Rough C-means	Accuracy (ACC)	82.46%	KDDCup'99
			Detection Rate (DR)	91.45%	
			False Alarm Rate(FAR)	24.80%	
			correlation	0.556	
A120	NA	DBSCAN Clustering	Detection Rate (DR)	0.961	KDD Cup 1999
			False Alarm Rate(FAR)	0.362	
A121	NA	Extreme learning machine	Recall	0.98897	synthetic datasets and three UCI datasets
			Accuracy (ACC)	0.9513	
A122	unsupervised	random forest	False Positive Rate (FPR)	na	KDD Cup 1999
			Detection Rate (DR)	na	
A123	NA	convolutional neural network (CNN), long short-term memory (LSTM), and deep neural network (DNN)	Accuracy (ACC)	98.60%	Yahoo S5 Webscope Dataset
			Recall	89.70%	
A124	NA	SVM	Accuracy (ACC)	85.60%	real life dataset
			True Positive Rate (TPR)	na	
			False Positive Rate (FPR)	na	
A125	unsupervised	LibSVM	Detection Rate (DR)	95%	KDD Cup 1999
			False Positive Rate (FPR)	7%	

TABLE 8. ***(Continued.)*** **Performance metrics among selected papers.**

A126	unsupervised	SVM and P-kernel	Detection Rate (DR)	98%	KDD Cup 1999
			False Positive Rate (FPR)	6%	
A127	NA	sequence-matching algorithm	False Positive Rate (FPR)	1.5	Purdue University dataset
			True Positive Rate (TPR)	92.8	
A128	supervised	Extreme Learning Machine (ELM)	Detection Rate (DR)	91%	ISCX-IDS 2012 dataset
			Misclassified Rate (MR)	9%	
A129	semisupervised	one-class support vector machine with ramp lose function	Accuracy (ACC)	98.59	NSL-KDD and UNSW-NB15 and UCI repository
			Detection Rate (DR)	98.25	
			False Alarm Rate(FAR)	1.25	
A130	supervised	SVM and SVR	Mean Absolute Error(MAE)	na	The Argo datasets
A131	NA	decision tree	Accuracy (ACC)	90%	KDD Cup 1999
			Precision	0.0973	
			Recall	0.9074	
			ROC Area	0.9073	
A132	NA	Decision Tree, Random Forest, and ANN	Accuracy (ACC)	99.40%	DS2OS traffic traces
			Precision	0.99	
			Recall	0.99	
			F-Score	0.99	
A133	NA	deep neural network (DNN), random forest (RF), variational autoencoder (VAE)	Accuracy (ACC)	99.99%	CIDDS-001
A134	unsupervised	Probabilistic Anomaly DQetection, File Wrapper	Detection Rate	95%	real life dataset
			False Positive Rate (FPR)	2%	
A135	supervised	naive Bayes and knearest neighbo	F-Score	na	real life dataset
			Precision	na	
			Recall	na	
			ROC Area	na	
A136	NA	one-class support vector machine (OCSVM)	Detection Rate (DR)	95.61%	real life dataset
			Falses Alarm Rate (FAR)	2.14%	
A137	semisupervised	Deep Belief Nets	F-Score	0.4752 ± 0.0044	real life dataset
			Recall	0.5514	
			Precision	0.4175	
A138	supervised	KMeans clustering and SVM SMO	True Positive Rate (TPR)	na	WHOIS data
			False Positive Rate (FPR)	na	
A139	NA	Bayes net	Detection Rate (DR)	81.25%	Google play dataset
			True Positive Rate (TPR)	97.30%	
			False Positive Rate (FPR)	31.03%	
A140	unsupervised	k-means clustering and hierarchical clustering	Mean Squared Error(MSE)	na	real life dataset
A141	supervised	rule based decision tree (RBDT)	False Positive Rate	0.13%	real life dataset
			Detection Rate (DR)	na	
A142	NA	Kohonen neural network (KNN) and support vector machine (SVM)	Detection Rate (DR)	83.90%	KDD Cup 1999
A143	supervised and unsupervised	Genetic Algorithm, Self-Organised Feature Map, and Support Vector Machine	Detection Rate (DR)	88.28	KDD Cup 1999
			False Positive rate (FPR)	9.17	
			False Negative Rate (FNR)	15.75	
A144	NA	SVM	Standard deviations	0.826	automobile dataset and UCI benchmark datasets
A145	supervised	Support Vector Machine	Accuracy (ACC)	0,999 701	synthetic data set
			F-Score	0,999 851	
		Random Forest	Accuracy (ACC)	0,999 936	
			F-Score	0,999 968	
A146	supervised	SVM+entropy	Detection Rate (DR)	na	KDD Cup 1999
			ROC Area	na	
A147	unsupervised	Least Squares Support Vector Machine	na	na	real life dataset
A148	unsupervised	Support Vector Machine and Self-Organizing Map	Detection Rate	92.30%	KDD Cup 1999
A149	supervised	Boosted Decision Tree, Neural Network	Accuracy (ACC)	0.928	Simulated Dataset and Real-world Dataset
			ROC Area	na	

TABLE 8. *(Continued.)* **Performance metrics among selected papers.**

A150	unsupervised	Generative Adversarial Networks	AUC	0.641	real life dataset
A151	NA	SVM-RBF	F-Score	0.88	Slammer, Nimda, Code Red I
			Matthews correlation coefficient	0.867	
			ROC Area	0.907	
			Precision-Recall	0.8	
A152	supervised	a batch relevance-based fuzzyfied learning algorithm	Accuracy (ACC)	0.941	NSL-KDD
			Sensitivity	0.893	
			Specificity	0.967	
			Precision	0.936	
			F-Score	0.914	
			correlation	0.87	
			ROC Area	0.93	
			Error Ratio	0.059	
A153	semisupervised	Artifical Neural Network and Mahalanobis distance based statistical approach	na	na	Real and synthesized energy consumption data
A154	semisupervised	Adaptive Network Anomaly Detection Algorithm	Detection Rate (DR)	0.9336	Kyoto University's 2006+
			Accuracy (ACC)	0.9666	
			False Alarm Rate(FAR)	0.0159	
			F-Score	0.9148	
A155	NA	naïve Bayesian classifier	ROC Area	na	real life dataset
			Total Events	252	
			True Positive Rate (TPR)	29 (17.7%)	
			Average Prediction Time	12.2s	
A156	supervised and unsupervised	SVM	Detection Rate (DT)	100%	synthetic dataset
			False Positive Rate (FPR)	8%	
A157	unsupervised	random forest, t distributed stochastic neighbor embedding (t-SNE)	Accuracy (ACC)	85%	real life dataset
A158	NA	structure analysis	AUC	0.9967	UMN Dataset
A159	unsupervised	Hierarchical Temporal Memory (HTM)	Accuracy (ACC) - standard	96%	µPMU Dataset
			Accuracy (ACC) - reward few false positive	96%	
			Accuracy (ACC) - reward few false negative	98%	
A160	unsupervised	one class extreme learning machine Kernel (ELMk)	AUC	0.9706±0.0029	real life dataset
A161	unsupervised	Recurrent Neural Network + LSTM	AUC - word	0.984	LANL Dataset
			AUC - character	0.977	
A162	NA	Genetic Algorithms + SVM	Accuracy (ACC)	98%	KDD Cup 1998
			True Positive Rate (TPR)	99.4987	
			False Positive Rate (FPR)	1.7806	
			True Negative Rate (TNR)	98.2194	
			False Negative Rate (FNR)	0.5013	
			Mean Squared Error(MSE)	0.0167	
A163	NA	Canonical Correlation Analysis (CCA) + Support Vector Machines (SVMs)	Mean Squared Error(MSE)	7.5	novel dataset
A164	supervised and unsupervised	Convolutional Neural Networks (CNN), Deep Belief Networks (DBN), Stacked AutoEncoders (SAE), Long Short-Term Memory Recurrent Networks (LSTM),	precision	0.95	CTU dataset and real life dataset
			Recall	0.38	
			F-Score	0.54	
A165	supervised	SVM	Accuracy (ACC)	90%	real life dataset
A166	NA	Gaussian models	na	na	na
A167	NA	Hidden Markov Model	Detection Rate (DR)	99.60%	real life dataset
A168	NA	D-Markov machine with symbolic false nearest neighbors	na	na	na

TABLE 8. ***(Continued.)*** **Performance metrics among selected papers.**

A169	unsupervised	real-value negative selection + multilayer perceptron	Detection Rate (DR)	na	MIT -Darpa 98, MIT- Darpa 99
			False Alarm Rate(FAR)	na	
A170	unsupervised	correlational paraconsistent machine (CPM)	True Positive Rate (TPR)	95%	real life dataset
			False Positive Rate (FPR)	4%	
			ROC Area	na	
A171	NA	Negative selection + multilayer neural network (backprogagation) + evolutionary algorithm	Detection Rate (DR)	100%	Iris dataset: Setosa, Virginica, Versicolor
			True Positive Rate (TPR)	100	
			False Positive Rate (FPR)	0	
			True Negative Rate (TNR)	50	
			False Negative Rate (FNR)	0	
A172	unsupervised	* Cluster-based Estimation * K-nearest neighbor * One Class SVM	Detection Rate	na	KDD CUP 1999, 1999 Lincoln Labs DARPA
			False Positive Rate	na	
			ROC Area	na	
A173	NA	na	Accuracy (ACC)	about 80%	real-time data from smartphone
A174	NA	LERAD	False Alarm Rate(FAR)	na	1999 DARPA/Lincoln and real-time dataset
A175	NA	Clustering	Correctly Classification rate (CCR)	99.92%	real life dataset
			Incorrectly classified instance	na	
			Kappa Statistics	na	
			Mean Absoulte Error	na	
A176	supervised	* Adaboost * SVM * Entropy	AUC, Average Precision	0.99	real life dataset
A177	supervised	negative selection SVM	detection rate, false alarm rate	V-detector 99.98 ocSVM100	Fisher Iris
A178	unsupervised	Cluster	confusion matrix	na	generated dataset
A179	unsupervised	Principal Components Analysis	ROC, FPR, TPR	na	real life dataset
A180	NA	SVM + GA with Neural Kernel	detection rate	99%	KDD Cup 1999
A181	unsupervised	AutoEncoder	mean squared error	na	real life dataset
A182	NA	relevance vector regression and autoregression	false alarms rate, detection rate	na	telemetry data obtained from an orbital rendezvous simulation
A183	NA	One class SVM	False alarm probability, Path loss exponent, Transmission ISR, Number of unauthorized transmitters	na	real life dataset
A184	unsupervised	clustering	detection rate	80.3%	nine UNIX users from Purdue University
			false positive rate	15.30%	
A185	supervised	a Stacked Auto-encoder	accuracy	98.67%	real life dataset
A186	unsupervised	Nearest neighbour	accuracy	na	CoverType, Mulcross, Smtp, U2R, etc..
A187	supervised	k-means clustering	na	na	real life dataset
A188	semi-supervisesd	SOM + J.48 decision tree	detection rate	99.90%	KDD Cup 99
			classification rate	99.84%	
			false positive rate	1.25%	
A189	semi-supervisesd	LSTM, NN	False Positive Rate (FPR)	833	real life dataset
			False Negative Rate (FNR)	619	
			F-Score	96%	
			detection rate (DR)	99.99%	
A190	unsupervised	two-class SVM with a Radial	Accuracy (ACC)	94%	experimental laboratory earth embankments
		Basis Function (RBF) kernel	F-Score	96%	
A191	NA	LSTM	accuarcy	99.50%	Code Red, Nimda, Slammer
A192	NA	Bayesian estimation	accuracy, false alarm, learning time	accuracy: 99%	real life dataset
A193	supervised	evolutionary neural networks	Detection rate, False Alarm rate	na	1999 DARPA
A194	unsupervised	3D convolutiona AutoEncoder	AUC	91.2	UCSD pedestrian dataset, . The UMN dataset
			EER	16.7	
A195	unsupervised	PCA	recall, FPR, Precision	na	real life dataset
A196	semi-supervised	Neural Network	AUC-ROC,	0.916±0.004	real-world dataset
			AUC-PR(Precision-Recall)	0.574±0.008	

TABLE 8. ***(Continued.)*** **Performance metrics among selected papers.**

A197	supervised	1-SVM	na	na	synthetic data and data in public domains such as: Colorado Water Watch
A198	unsupervised	Auto encoder based on Artificial Neural networks	Precision	0.996	benign IoT traffic
			recall	0.999	
			F-Score	0.997	
A199	supervised	Random Forest algorithm and regression tree	accuracy, false alarm rate, precision, recall, f1-measure	95.73	UNSW-NB15
			False Alarm Rate(FAR)	11.86	
			precision	78.65	
			recall	78.65	
			F-Score	78.65	
A200	NA	four single classifers (DT, RF, kNN and GBDT) and Linear Regression GBDT: gradient boosting Decision Tree	Precision	0.8803	System Log of server clusters in a financial company
			Recall	0.7017	
			F-Score	0.8376 Biz Business Type	
A201	NA	non linear Mercer kernel function	ROC curves	na	simulated data and real HYDICE images
A202	unsupervised	swarm intelligence-based clustering	Detection Rate (DR)	92%	KDD Cup 1999
			False Positive Rate (FPS)	10%	
A203	NA	Hidden Markov Model and Support Vector Machine	precision	86.16%	massive real-world datasets from AIS vessel tracking in coastal waters of North America
			recall	80.07%	
			F-Score	83.00%	
			accuarcy	96.70%	
A204	NA	Ensemble learning Autoencoder Support vector regression Random forest	True Positive Rate (TPR)	98.1	real-world data provided by Powersmiths
			False Positive Rate (FPR)	1.98	
			AUC	na	
A205	NA	ensemble + clustering	ROC	na	simulated MANET and real life dataset
A206	unsupervised	Bayesian mixture	Accuracy	85.2	KDD Cup 1999
			False Positive Rate (FPR)	7.3	
A207	unsupervised	ensemble of one class SVM	AUC, ROC	na	DARPA'99 , GATECH
A208	NA	Naive Bayes	Error Rate	44%	real life dataset
			System Error	202 out 4000	
			unsure	40 out of 4000	
			corpus error	158 out of 4000	
A209	supervised	Stochastic gradient boosting	AUC-ROC	0.8661 ± 0.0150	real life dataset
			Precision	0.8351 ± 0.0100	
A210	semi-supervised	Gaussian model	Accuracy (ACC)	92.79%	call detail records of real cellular network
			Error Rate (ER)	7.21%	
			F-Score	94.26%	
			False Positive Rate (FPR)	14.13%	
			Precision	92.34%	
			Recall	97.05%	
A211	supervised	n-gram	Detection Rate (DR)	99%	Channel 6 dataset
			False Positive Rate (FPR)	0.10%	
			ROC Area	na	
A212	unsupervised	recursive least squares (RLS) + online sequential extreme learning machin (OS-ELM) + single-layer feed-forward neural network (SLFN)	Precision, Recall, F-measure	na	real world dataset
A213	unsupervised	Recurrent Neural Networks	Cumulative Sum, false positive rate	na	Secure Water Treatment Testbed (SWaT)
A214	NA	Single-window classification	True Positive Rate (TPR)	93%	real life traffic dataset
			False Positive Rate (FPR)	0.86%	
A215	NA	negative selection-based	Accuracy (ACC)	96.10%	KDD Cup 1999

TABLE 8. ***(Continued.)*** **Performance metrics among selected papers.**

A216	supervised + unsupervised	Supervised: Logistic regression, Decision tree, and Support vector machine (SVM) Unsupervised: Log Clustering, PCA, Invariants Mining	Accuracy, Recall, Precision, F-measure	na	HDFS and BGL
A217	unsupervised	n-grams	efficiency, stability, scaling	na	na
A218	supervised	K-mean + SMO	Detection Rate (DR)	94.48%	NSL-KDD
			False Alarm Rate(FAR)	1.20%	
			Accuracy (ACC)	97.37%	
A219	NA	most relevant principal components + neural networks	True Positive Rate (TPR)	91.40%	real life dataset
			False Positive Rate (FPR)	3.70%	
A220	supervised	KNN	Detection Rate (DR)	78%	ADFA-LD
			False Alarm Rate(FAR)	21%	
A221	unsupervised	Ensemble of One-Class SVM	desired false positive rate (DFP), real false positive rate (RFP), DR, AUC	na	real life dataset
A222	unsupervised	Isolation Forest	Accuracy (ACC)	88.32	CSIC 2010 data set
			Detection Rate (DR)	88.34	
			Precision-Recall	80.79	
			F-Score	84.12	
A223	supervised	support vector machines with a radial basis kernel (SVM-RBF)	Detection Rate (DR)	90.30%	DARPA/KDD-99
			False Positive Rate (FPR)	0.50%	
A224	NA	program behavior traces	FP, Recall	na	1998/1999 Dataset
A225	unsupervised	Fuzzy Adaptive Resonance Theory	False Positive Rate (FPR)	3.73%	KDD Cup 1999
			Hit Rate	80.00%	
			Cost	0.424	
		Evolving Fuzzy Neural Networks	False Positive Rate (FPR)	2.61%	
			Hit Rate	76.00%	
			Cost	0.397	
		SVM	False Positive Rate (FPR)	15.70%	
			Hit Rate	80.00%	
			Cost	1.14	
A226	NA	Temporal relationships	Anomaly mean	0.76	real and synthetic dataset
			Anomaly standard deviation	0.14	
			Anomaly threshold	0.99	
A227	NA	Naive Bayes	Accuracy (ACC)	78.941	KDD dataset
		Decision table	Accuracy (ACC)	94.41	
		J48	Accuracy (ACC)	97.62	
		PART	Accuracy (ACC)	97.5179	
A228	NA	Stream clustering-based	detection rate	na	Digital Corpora, 2008, 2009, and real dataset
A229	unsupervised	conditional anomaly detection	Precision-Recall	0.72	KDD CUP 1999
A230	NA	neural network Neuro-fuzzy method	Accuracy (ACC)	86.72%	real time data collected by the city of Aarhus, Denmark
		Binary Support Vector Machines	Accuracy (ACC)	98.65%	
A231	unsupervised	Bayesian Networks	Prediction errors	na	real time data
A232	supervised	Naive Bayes with adaboost	False Positive Rate (FPR)	4.23%	KDD Cup 1999
			Detection Rate (DR)	84.32%	
A233	supervised	negative and positive selection + C4.5 and Naïve Bayes	True Positive Rate (TPR)	0.997	UCI data repository
			False Positive Rate (FPR)	0.028	
A234	NA	Online Kalman Filtering	Precision	96.55%	real time dataset
			Recall	98.25%	
			False Alarm Rate(FAR)	11.11%	
A235	NA	Auto Encoder	Accuracy (ACC)	88.65%	NSL-KDD
			Precision	96.48%	
			Recall	83.08%	
			F-Score	89.28%	
A236	unsupervised	deep Gaussian mixture model + PCANet	AUC	92.50%	UCSD Ped1 Dataset, Avenue Dataset
			Accuracy (ACC)	75.40%	
			Equal Error Rate (EER)	15.10%	
A237	semi-supervised	Generative Adversarial Networks	AUC	AUC: 0.882	CIFAR10 Dataset, MNIST Dataset

TABLE 8. ***(Continued.)*** **Performance metrics among selected papers.**

A238	supervised	Echo State Networks	False negative, false positive, Detection rate	na	real life dataset
A239	NA	Genetic algorithm (GA)	accuracy	accuracy: 85.38%	NSL-KDD
A240	NA	Deep Neural Network	Detection Rate (DR)	70%	real life dataset
			False Alarm Rate(FAR)	< 3%	
A241	supervised and unsupervised	CART Decision Trees (CART), Random Forest (RF), Support Vector Machines (SVM), Naive Bayes (NB) and Neural Networks (MLP)	ROC	ROC: 0.997	MAWILab
A242	NA	Hidden Markov Model	training time	na	"inetd" and "sride" dataset
A243	NA	SVM	classified, actual	na	real time dataset
A244	unsupervised	augmented Daikon and Mean. Daikon	TP, TN, FP, FN	na	stock quote data sources
A245	supervised and unsupervised	J48 + Naïve Bayes	accuracy, TP, TN, FP, FN	88%	UNSW-NB15
A246	NA	J48	Detection Rate (DR)	99.8	real time dataset
			False Alarm Rate(FAR)	0.1	
		BayseNet	Detection Rate (DR)	99.9	
			False Alarm Rate(FAR)	0	
		SMO	Detection Rate (DR)	98.6	
			False Alarm Rate(FAR)	2.9	
A247	semi-supervised	Deep Belief Network and Restricted Boltzmann Machine	Accuracy (ACC)	94%	MINIST
			Accuracy (ACC)	94.66%	NSL-KDD
			Accuracy (ACC)	95%	HTTP CSIC 2010
A248	unsupervised	K-means clustering	na	na	KDD cup 1999
A249	NA	K-NN	AUC Area	0.96	MAWILab
			Accuracy (ACC)	85.60%	
		Hoeffding Adaptive Trees (HAT)	AUC Area	0.79	
			Accuracy (ACC)	99.60%	
		Adaptive Random Forests (ARF)	AUC Area	0.99	
			Accuracy (ACC)	98.20%	
		Stochastic Gradient Descent (SGD)	AUC Area	0.99	
			Accuracy (ACC)	99.30%	
A250	supervised and unsupervised	Kernel Recursive Least Squares	Detected	25	network-wide traffic datasets
			Missed	9	
			FALSE	0	
A251	NA	Autoencoder + Kernel density estimation model (OCKDE)	AUC Area	0.987	NSL-KDD
		Autoencoder + Centroid (OCCEN)	AUC Area	0.986	
		Once class classifier Autoencoder (OCAE)	AUC Area	0.971	
A252	NA	Genetic algorithm (GA)	False Positive Rate (FPR)	1.2	KDD Cup 1999
			True Positive Rate (TPR)	96.49	
A253	supervised and unsupervised	fully convolutional neural network	AUC-EER-Exit	90.2/16	UCSD (Ucsd anomaly detection dataset, 2017) and Subway benchmarks (Adam et al., 2008)
			AUC-EER-Entrance	90.4/17	
A254	NA	Adversarial autoencoder (AAE)	Area Under Precision Recall Curve (AUPRC)	1	synthetic data, cifar-10, Pixabay,
		variational autoencoder (VAE)	Area Under Precision Recall Curve (AUPRC)	1	
A255	supervised	Neural networks	Detection Error Rate,	0,01375%	simulation dataset
A256	NA	ensemble	True Positive Rate (TPR)	98	NSL-KDD
			False Positive Rate (FPR)	0.021	
			F-Score	98	
			ROC Area	99.6	
A257	supervised and unsupervised	one class SVM + particle swarm optimization	AUC	0.952	UCI data set
A258	NA	Isolation Forest	Precision	92.50%	real life dataset
			Recall	82.84%	
A259	supervised	frequent item-set mining (FIM) + C5.0 + decision tree	Accuracy (ACC)	> 98%	real life dataset
			False Positive Rate (FPR)	< 1%	

TABLE 8. *(Continued.)* **Performance metrics among selected papers.**

A260	supervised	J48 classifier + Bayes Net	accuracy, precision, recall, F-value	99.50%	real life dataset
A261	NA	convex-hull SVM	ROC curve	na	KDD'99
A262	NA	GAN to train LSTM-RNNs	Precision	70	SWaT
			Recall	95.4	
			F-Score	0.81	
			Precision	53.75	WADI
			Recall	74.92	
			F-Score	0.62	
A263	NA	n-grams	Accuracy (ACC)	0.999	real life dataset
			Precision	0.998	
A264	NA	Attention-base Multi-Flow LSTM	Precision	0.98	CICIDS2017
			Recall	0.91	
			F-Score	0.94	
			Flows	348631	
A265	NA	Back Propagation Neural Network	Accuracy (ACC)	91%	KDD Cup 1999
			Precision	0.996699	
			Recall	0.90059	
			F-Score	0.94615	
A266	NA	Bayesian Learning + Markov models	true positive rate, false positive rate, accuracy	na	real life dataset
A267	unsupervised	greedy ensemble	AUC, True postive rate, false positive rate, ROC curve	AUC: 0.84	ALOI and synthetic data from MNIST and UCI datasets
A268	unsupervised	clustering-based	Accuarcy (ACC)	96%	public data
A269	unsupervised and supervised	Restricted Boltzmann Machines (RBM) and Autoencoder	na	na	KDD Cup 1999
A270	unsupervised	LSTM	Accuracy (ACC)	99%	NSL-KDD and Kyoto-Honeypot
			Precision	98.30%	
			Recall	99.60%	
			F-Score	99.00%	
A271	NA	Random Forests and Entropy	Precision	0.83	DARPA 1999 dataset
			Recall	0.85	
			F-Score	0.84	
A272	NA	one-class quarter sphere SVM	detection rate, false positive rate	na	real life dataset
A273	NA	ensemble	Accuracy (ACC)	na	UCI
A274	unsupervised	Random Forest Classifier	Precision	0.9992	NSL-KDD
			Recall	0.9969	
			F-Score	0.998	
A275	NA	LSTM-RNN	classification accuracy	na	KDD 1999 dataset
A276	NA	Random Forest	Accuracy (ACC)	99.34%	UNSW-NB15
			Precision	0.98	
			Recall	0.98	
			F-Score	0.98	
A277	unsupervised and supervised	ensemble	Accuracy (ACC)	na	UCI
A278	NA	Random Forest	Accuracy (ACC)	99.60%	SMS- real life dataset
			Accuracy (ACC)	99.10%	iDMA- real life dataset
			Accuracy (ACC)	99.20%	iTL- real life dataset
			Accuracy (ACC)	80.60%	Touchstroke- real life dataset
A279	unsupervised	growing hierarchical self organizing map	Accuracy (ACC)	97.12%	TD-Sim
			False Positive Rate (FPR)	2.60%	TD-Sim
			Accuracy (ACC)	99.63%	KDD Cup 1999
			False Positive Rate (FPR)	1.80%	KDD Cup 1999
A280	unsupervised	Autoencoder	true positive rate, false positive rate, F-measure	F-measure: 0.418 (basic)	synthetic dataset
A281	NA	Hidden Markov Models	normal Generalization	80	Computer Immune Systems benchmark data
			Intrusive Generaliztion	83	
			Overall Generaliztio	81.48	
			False Positive Rate	20	
			False Negative Rate	17	
A282	NA	Kernel PCA	Probability Density Function, Thruster Duty	na	telemetry data
A283	NA	LSTM	Accuracy (ACC)	96.41%	real life dataset
			F-Score	0.98	
		FFNN	Accuracy (ACC)	94.49%	
			F-Score	0.97	

TABLE 8. ***(Continued.)*** **Performance metrics among selected papers.**

A284	NA	Neural network, Analogous Particle swarm optimization	Precision	95.70%	real life dataset
			System Efficiency	5.60%	
			Error Rate	0.0403	
A285	unsupervised	Local Outlier Factor (LOF)	True Positive Rate	na	real life time series dataset
A286	supervised	Decision Forest	Precision	99.90%	real life dataset
			Recall	99.90%	
			F-score	0.9999	
		Decision Jungle	Precision	99.21%	
			Recall	99.21%	
			F-score	0.9921	
A287	supervised	autoencoder (AE)	Mean Absolute Error(MAE)	2.9	real life dataset
			Mean Squared Error(MSE)	15.8	
			AUC	0.9969	
			True Positive Rate (TPR)	98.6	
			False Positive Rate (FPR)	0.9	
A288	supervised	k-means and Skip-gram	accuracy	98	real life dataset
A289	na	Locally Weighted Projection Regression	Detection Rate (DR)	86%	real life dataset
			AUC	0.54	
			F1-score	0.86	
			Precision	0.85	
			Accuracy (ACC)	0.91	
			Error rate	16%	
A290	unsupervised	Sub-Space Clustering (SSC) and One Class Support Vector Machine (OCSVM)	Detection Rate (DR)	0.9	NSL-KDD dataset
			False Alarm Rate(FAR)	0.0905	

accuracy: performance metric, accuracy value, dataset for construction, and model validation methods.

Since building a ML model relies on the dataset, we reviewed the data source of ML models for anomaly detection utilized in the selected research articles. Moreover, we identified 22 different datasets that have been used in the experiments of related articles and many other general datasets. The datasets can be classified as synthetic data, real life data, and virtualized data. Figure 5 demonstrates the frequency of utilized datasets in the collected research articles. As shown in Figure 5, the most frequently used dataset in the selected research papers was real life dataset, according to anomaly detection application. In addition, 48 research papers utilized KDD Cup 1999 virtualized dataset and 38 research papers adopted benchmark datasets.

In addition to datasets, ML models should also be evaluated with performance metrics. We found 276 papers that clearly presented the performance metrics of their proposed models. Figure 6 shows that the performance metric used most was True Positive Rate (TPR), which is also known as detection date, sensitivity, and recall. It measures the anomalies that are correctly classified. Moreover, 116 papers used False Positive Rate (FPR) as a performance metric. This metric measures anomalies that are falsely classified, and it can be known as false alarm rate as well. Furthermore, Accuracy (Acc), precision, and were F-score applied often by researchers as a performance metric. Acc is the percentage of anomalies that were correctly classified. Adding more, AUC measures the whole two dimensional area under the entire ROC curve. ROC curve is one of the strongest metrics used to efficiently assess intrusion detection systems performance, and it is a graphical tool that illustrates accuracy across FPS. On the other hand, Precision is usually associated with F-score and recall, and it measures the ratio of anomalies that are correctly classified as an attack. In addition, we find that 64 of the 290 papers used only one performance metric, and most of those papers used only accuracy or AUC, which is not sufficient to determine the quality performance of the ML model. On the other hand, papers like A10 and A69 used 7 to 9 performance metrics to represent the performance of their ML models. Furthermore, a lot of papers present computational performance metrics in addition to performance metrics, such as CPU utilization, execution time, training time, testing time, and computational time. Table 8 in appendix A presents each paper ID and the proposed ML model along with the performance and computational metrics applied. Moreover, it presents anomaly detection types whether it is supervised, unsupervised, and semi-supervised. As well as the dataset used for that model.

D. PERCENTAGE OF UNSUPERVISED, SEMI-SUPERVISED OR SUPERVISED ANOMALY DETECTION TECHNIQUES

In this section, we address RQ4, which aims to present the percentage of collected research papers that use supervised, semi-supervised, or unsupervised anomaly detection methods.

As previously mentioned, anomaly detection can be divided into three broad classes depending on the feature of the training data that is applied to construct the model. The three broad classes are unsupervised anomaly detection, semi-supervised anomaly detection, and supervised anomaly detection. For this RQ we reviewed the classification type of anomaly detection techniques used in research articles. According to Figure 7, 27% of the selected papers applied unsupervised anomaly detection type, making it the most used technique among the research articles. On the other hand, 18% applied supervised anomaly detection, while 7% applied both supervised and unsupervised anomaly detection classification. In contrast, 5% of research articles adopted semi-supervised learning. Furthermore, 1% applied semi-supervised with unsupervised anomaly detection. Surprisingly, 42% of the research articles did not mention the classification type of the anomaly detection they applied.

According to Figure 8, the unsupervised anomaly detection type has been applied from 2002 until **2020**. As for supervised anomaly detection type, it was adopted by researchers in 2002 and has been used until the present time. Supervised and unsupervised anomaly detection types were utilized from 2005 to 2019. In contrast, supervised and semi-supervised anomaly detection types were adopted only in 2013 and 2018. Similarly, unsupervised and semi-supervised anomaly detection types have only been used twice, in 2011 and 2016. It can be seen then, that combining semi-supervised learning with either supervised or unsupervised learning was not adopted by many researchers compared to the supervised anomaly detection type or unsupervised anomaly detection type. For further information on results, Table 8 in Appendix A present the anomaly detection type of each research article.

IV. LIMITATION OF THIS REVIEW

This systematic literature review is limited to journal and conference papers related to ML in the field of anomaly detection. We excluded several non-relevant research papers by implementing our search approach in the first stages of the review. This ensured that the research papers chosen met the research requirements. However, we believe that this review would have been further enhanced by drawing on additional sources. Moreover, the same concept applies to quality assessment since we applied a strict QAR.

V. CONCLUSION

This systematic literature review studied anomaly detection through machine learning techniques (ML). It reviewed ML models from four perspectives: the application of anomaly detection type, the type of ML technique, the ML model accuracy estimation, and the type of anomaly detection (supervised, semi-supervised, and unsupervised). The review investigated the relevant studies that were published from 2000-2020. We queried 290 research articles that answered the four research questions (RQs) raised in this review.

The findings of RQ1 were that we identified 43 different applications of anomaly detection in the selected papers. We observed that intrusion detection, network anomaly detection, general anomaly detection, and data applications are the studies most often applied in the anomaly detection area. Furthermore, between 2011 and 2019 researchers started to adopt more applications for anomaly detection. As for RQ2, we demonstrated 29 different ML models that have been applied by researchers, with the most commonly used being SVM. Moreover, we noted an interest in building hybrid models. In addition, we identified that PCA and CFS are the most commonly used among 21 feature selection/extraction techniques. In RQ3 we presented the performance metrics applied by each research paper, and we found that 64 of the 290 papers used accuracy or AUC as their main performance metric, which is not efficient enough. Furthermore, we identified 22 different datasets that have been used in the experiments of related articles as well as many other general datasets, and most of the experiments used real life dataset as training or testing datasets for their models. Lastly, in RQ4 we counted the classification type of anomaly detection used in selected research articles. We found that 27% of the selected papers applied unsupervised anomaly detection type, making it the most used approach among the research articles. The next most utilized approach was applied supervised anomaly detection, at 18%, followed by 7% of the papers which applied both supervised and unsupervised anomaly detection classification.

Based on this review, we recommend that researchers conduct more research on ML studies of anomaly detection to gain more evidence on ML model performance and efficiency. Moreover, researchers are also encouraged to create a general structure for introducing experiments on ML models. Moreover, since we found research papers that did not mention feature selection/extraction type, this field is important for improvement. Furthermore, some of the research papers reported their results using one performance metric, such as accuracy, which needs more improvement and more consideration. We also noticed that several researchers used old databases in conducting their research. We recommend researchers use more recent datasets.

APPENDIX

See Tables 4–8.

ACKNOWLEDGMENT

The authors would like to thank the University of Sharjah and OpenUAE Research and Development Group for funding this research study. They are also grateful to their research assistants who helped in collecting, summarizing, and analyzing the research articles for this SLR study.

"**Conflict of Interest:** The authors declare that they have no competing interests".

"**Informed consent:** This study does not involve any experiments on animals or humans".

REFERENCES

[1] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 71–97, 2009, doi: 10.1145/1541880.1541882.

[2] M. Injadat, F. Salo, A. B. Nassif, A. Essex, and A. Shami, "Bayesian optimization with machine learning algorithms towards anomaly detection," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6, doi: 10.1109/GLOCOM.2018.8647714.

[3] T. Schlegl, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, *Unsupervised Anomaly Detection With Generative Adversarial Networks to Guide Marker Discovery*, vol. 10265, no. 2. Cham, Switzerland: Springer, 2017.
[4] F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: A systematic literature review," *IEEE Access*, vol. 6, pp. 56046–56058, 2018, doi: 10.1109/ACCESS.2018.2872784.
[5] F. Salo, M. N. Injadat, A. Moubayed, A. B. Nassif, and A. Essex, "Clustering enabled classification using ensemble feature selection for intrusion detection," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, 2019, pp. 276–281, doi: 10.1109/ICCNC.2019.8685636.
[6] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," *Comput. Netw.*, vol. 148, pp. 164–175, Jan. 2019, doi: 10.1016/J.COMNET.2018.11.010.
[7] P. Gogoi, D. K. Bhattacharyya, B. Borah, and J. K. Kalita, "A survey of outlier detection methods in network anomaly identification," *Comput. J.*, vol. 54, no. 4, pp. 570–588, Apr. 2011, doi: 10.1093/comjnl/bxr026.
[8] S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques," *Procedia Comput. Sci.*, vol. 60, no. 1, pp. 708–713, 2015, doi: 10.1016/j.procs.2015.08.220.
[9] R. A. A. Habeeb, F. Nasaruddin, A. Gani, I. A. T. Hashem, E. Ahmed, and M. Imran, "Real-time big data processing for anomaly detection: A survey," *Int. J. Inf. Manage.*, vol. 45, pp. 289–307, Apr. 2019, doi: 10.1016/j.ijinfomgt.2018.08.006.
[10] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 5, pp. 823–839, Nov. 2012.
[11] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 303–336, 1st Quart., 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6524462/
[12] I. Bose and R. K. Mahapatra, "Business data mining—A machine learning perspective," *Inf. Manage.*, vol. 39, no. 3, pp. 211–225, 2001, doi: 10.1016/S0378-7206(01)00091-X.
[13] U. Fiore, F. Palmieri, A. Castiglione, and A. De Santis, "Network anomaly detection with the restricted Boltzmann machine," *Neurocomputing*, vol. 122, pp. 13–23, Dec. 2013, doi: 10.1016/j.neucom.2012.11.050.
[14] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering version 2.3," *Engineering*, vol. 45, no. 4, p. 1051, 2007, doi: 10.1145/1134285.1134500.
[15] V. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artif. Intell. Rev.*, vol. 22, no. 2, pp. 85–126, Oct. 2004, doi: 10.1023/b:aire.0000045502.10941.a9.
[16] M. Ahmed, A. N. Mahmood, and M. R. Islam, "A survey of anomaly detection techniques in financial domain," *Future Gener. Comput. Syst.*, vol. 55, pp. 278–288, Feb. 2016, doi: 10.1016/j.future.2015.01.001.
[17] A. A. Sodemann, M. P. Ross, and B. J. Borghetti, "A review of anomaly detection in automated surveillance," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 6, pp. 1257–1272, Nov. 2012, doi: 10.1109/TSMCC.2012.2215319.
[18] R. Zuo, "Machine learning of mineralization-related geochemical anomalies: A review of potential methods," *Natural Resour. Res.*, vol. 26, no. 4, pp. 457–464, Oct. 2017, doi: 10.1007/s11053-017-9345-4.
[19] S. He, J. Zhu, P. He, and M. R. Lyu, "Experience report: System log analysis for anomaly detection," in *Proc. IEEE 27th Int. Symp. Softw. Rel. Eng. (ISSRE)*, Oct. 2016, pp. 207–218, doi: 10.1109/ISSRE.2016.21.
[20] O. Ibidunmoye, F. Hernández-Rodriguez, and E. Elmroth, "Performance anomaly detection and bottleneck identification," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 1–35, Sep. 2015, doi: 10.1145/2791120.
[21] Y. Yu, "A survey of anomaly intrusion detection techniques," *J. Comput. Sci. Coll.*, vol. 28, no. 1, pp. 9–17, 2012. [Online]. Available: http://dl.acm.org/citation.cfm?id=2379707
[22] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," *Expert Syst. Appl.*, vol. 36, no. 10, pp. 11994–12000, Dec. 2009, doi: 10.1016/j.eswa.2009.05.029.
[23] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Comput. Netw.*, vol. 51, no. 12, pp. 3448–3470, Aug. 2007, doi: 10.1016/j.comnet.2007.02.001.
[24] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016, doi: 10.1109/COMST.2015.2494502.
[25] K. Satpute, S. Agrawal, J. Agrawal, and S. Sharma, "A survey on anomaly detection in network intrusion detection system using swarm optimization based machine learning techniques," in *Proc. Int. Conf. Frontiers Intell. Comput.*, vol. 199, 2013, pp. 441–452, doi: 10.1007/978-3-642-35314-7.
[26] V. Sharma, R. Kumar, W.-H. Cheng, M. Atiquzzaman, K. Srinivasan, and A. Zomaya, "NHAD: Neuro-fuzzy based horizontal anomaly detection in online social networks," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 11, pp. 2171–2184, Nov. 2018, doi: 10.1109/TKDE.2018.2818163.
[27] P. Zhao, Y. Zhang, M. Wu, S. C. H. Hoi, M. Tan, and J. Huang, "Adaptive cost-sensitive online classification," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 2, pp. 214–228, Feb. 2019, doi: 10.1109/TKDE.2018.2826011.
[28] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Comput.*, vol. 22, pp. 1–13, Sep. 2017, doi: 10.1007/s10586-017-1117-8.
[29] G. Fernandes, J. J. P. C. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi, and M. L. Proença, "A comprehensive survey on network anomaly detection," *Telecommun. Syst.*, vol. 70, no. 3, pp. 447–489, Mar. 2019, doi: 10.1007/s11235-018-0475-8.
[30] G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, "A survey of anomaly detection for connected vehicle cybersecurity and safety," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 421–426, doi: 10.1109/IVS.2018.8500383.
[31] T. Shon and J. Moon, "A hybrid machine learning approach to network anomaly detection," *Inf. Sci.*, vol. 177, no. 18, pp. 3799–3821, Sep. 2007, doi: 10.1016/j.ins.2007.03.025.
[32] S. M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, "High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning," *Pattern Recognit.*, vol. 58, pp. 121–134, Oct. 2016, doi: 10.1016/j.patcog.2016.03.028.
[33] M. Field, S. Das Bryanlmatthewsnasagov, N. C. Oza, B. L. Matthews, and A. N. Srivastava, "Multiple kernel learning for heterogeneous anomaly detection: Algorithm and aviation safety case study categories and subject descriptors," in *Proc. Comput.*, Jul. 2010, pp. 47–56.
[34] M. Amer, M. Goldstein, and S. Abdennadher, "Enhancing one-class support vector machines for unsupervised anomaly detection," in *Proc. ACM SIGKDD Workshop Outlier Detection Description (ODD)*, 2013, pp. 8–15, doi: 10.1145/2500853.2500857.
[35] Y.-X. Meng, "The practice on using machine learning for network anomaly intrusion detection," in *Proc. Int. Conf. Mach. Learn. Cybern.*, Jul. 2011, pp. 576–581, doi: 10.1109/ICMLC.2011.6016798.
[36] A. P. Muniyandi, R. Rajeswari, and R. Rajaram, "Network anomaly detection by cascading K-means clustering and C4.5 decision tree algorithm," *Procedia Eng.*, vol. 30, pp. 174–182, Jan. 2012, doi: 10.1016/j.proeng.2012.01.849.
[37] S.-W. Lin, K.-C. Ying, C.-Y. Lee, and Z.-J. Lee, "An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection," *Appl. Soft Comput.*, vol. 12, no. 10, pp. 3285–3290, Oct. 2012, doi: 10.1016/j.asoc.2012.05.004.
[38] S. Thaseen and C. A. Kumar, "An analysis of supervised tree based classifiers for intrusion detection system," in *Proc. Int. Conf. Pattern Recognit., Informat. Mobile Eng. (PRIME)*, Feb. 2013, pp. 294–299, doi: 10.1109/ICPRIME.2013.6496489.
[39] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Syst. Appl.*, vol. 41, no. 4, pp. 1690–1700, Mar. 2014, doi: 10.1016/j.eswa.2013.08.066.
[40] S. Fu, "Performance metric selection for autonomic anomaly detection on cloud computing systems," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–5, doi: 10.1109/GLOCOM.2011.6134532.
[41] Y. Yasami and S. P. Mozaffari, "A novel unsupervised classification approach for network anomaly detection by k-means clustering and ID3 decision tree learning methods," *J. Supercomput.*, vol. 53, no. 1, pp. 231–245, Jul. 2010, doi: 10.1007/s11227-009-0338-x.
[42] R. Chitrakar and H. Chuanhe, "Anomaly detection using support vector machine classification with k-medoids clustering," in *Proc. 3rd Asian Himalayas Int. Conf. Internet*, Nov. 2012, pp. 1–5, doi: 10.1109/AHICI.2012.6408446.

[43] N. Chand, P. Mishra, C. R. Krishna, E. S. Pilli, and M. C. Govil, "A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection," in *Proc. Int. Conf. Adv. Comput., Commun., Automat. (ICACCA)*, Apr. 2016, pp. 1–6, doi: 10.1109/ICACCA.2016.7578859.

[44] K. Noto, C. Brodley, and D. Slonim, "FRaC: A feature-modeling approach for semi-supervised and unsupervised anomaly detection," *Data Mining Knowl. Discovery*, vol. 25, no. 1, pp. 109–133, Jul. 2012, doi: 10.1007/s10618-011-0234-x.

[45] I. Assent, P. Kranen, C. Baldauf, and T. Seidl, "AnyOut: Anytime outlier detection on streaming data," in *Proc. Int. Conf. Database Syst. Adv. Appl.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 7238, 2012, pp. 228–242, doi: 10.1007/978-3-642-29038-1_18.

[46] A. Kulkarni, Y. Pino, M. French, and T. Mohsenin, "Real-time anomaly detection framework for many-core router through machine-learning techniques," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, pp. 1–22, Dec. 2016, doi: 10.1145/2827699.

[47] J. Vanerio and P. Casas, "Ensemble-learning approaches for network security and anomaly detection," in *Proc. Workshop Big Data Anal. Mach. Learn. Data Commun. Netw.*, Aug. 2017, pp. 1–6, doi: 10.1145/3098593.3098594.

[48] K. Noto, C. Brodley, and D. Slonim, "Anomaly detection using an ensemble of feature models," in *Proc. IEEE Int. Conf. Data Mining (ICDM)*, Dec. 2010, pp. 953–958, doi: 10.1109/ICDM.2010.140.

[49] P. Jongsuebsuk, N. Wattanapongsakorn, and C. Charnsripinyo, "Network intrusion detection with fuzzy genetic algorithm for unknown attacks," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2013, pp. 1–5, doi: 10.1109/ICOIN.2013.6496342.

[50] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," in *Proc. Sci. Inf. Conf. SAI*, Aug. 2014, pp. 626–631, doi: 10.1109/SAI.2014.6918252.

[51] T. Shon, Y. Kim, C. Lee, and J. Moon, "A machine learning framework for network anomaly detection using SVM and GA," in *Proc. 6th Annu. IEEE SMC Inf. Assurance Workshop*, Jun. 2005, pp. 176–183, doi: 10.1109/IAW.2005.1495950.

[52] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, nos. 1–2, pp. 18–28, Feb. 2009, doi: 10.1016/j.cose.2008.08.003.

[53] S.-J. Han and S.-B. Cho, "Evolutionary neural networks for anomaly detection based on the behavior of a program," *IEEE Trans. Syst. Man, Cybern. B, Cybern.*, vol. 36, no. 3, pp. 559–570, Jun. 2006, doi: 10.1109/tsmcb.2005.860136.

[54] A. Nanduri and L. Sherry, "Anomaly detection in aircraft data using recurrent neural networks (RNN)," in *Proc. Integr. Commun. Navigat. Surveill. (ICNS)*, Apr. 2016, pp. 1–8, doi: 10.1109/ICNSURV.2016.7486356.

[55] S. Rajasegarar, C. Leckie, J. C. Bezdek, and M. Palaniswami, "Centered hyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 518–533, Sep. 2010, doi: 10.1109/TIFS.2010.2051543.

[56] *Distribution Restriction Statement Approved for Public Release*, USACE, Washington, DC, USA, 1994, vol. 2.

[57] B. Agarwal and N. Mittal, "Hybrid approach for detection of anomaly network traffic using data mining techniques," *Procedia Technol.*, vol. 6, pp. 996–1003, Jan. 2012, doi: 10.1016/j.protcy.2012.10.121.

[58] J. Jabez and B. Muthukumar, "Intrusion detection system (IDS): Anomaly detection using outlier detection approach," *Procedia Comput. Sci.*, vol. 48, pp. 338–346, Jan. 2015, doi: 10.1016/j.procs.2015.04.191.

[59] M. Sheikhan and Z. Jadidi, "Flow-based anomaly detection in high-speed links using modified GSA-optimized neural network," *Neural Comput. Appl.*, vol. 24, nos. 3–4, pp. 599–611, Mar. 2014, doi: 10.1007/s00521-012-1263-0.

[60] S. Mascaro, A. E. Nicholso, and K. B. Korb, "Anomaly detection in vessel tracks using Bayesian networks," *Int. J. Approx. Reasoning*, vol. 55, no. 1, pp. 84–98, Jan. 2014, doi: 10.1016/j.ijar.2013.03.012.

[61] D. Liu, Y. Zhao, H. Xu, Y. Sun, D. Pei, J. Luo, X. Jing, and M. Feng, "Opprentice: Towards practical and automatic anomaly detection through machine learning," in *Proc. Internet Meas. Conf.*, Oct. 2015, pp. 51–78, doi: 10.1145/2815675.2815679.

[62] I. Syarif, A. Prugel-Bennett, and G. Wills, "Unsupervised clustering approach for network anomaly detection," in *Proc. Int. Conf. Netw. Digit. Technol.*, 2012, pp. 135–145.

[63] O. Linda, M. Manic, T. Vollmer, and J. Wright, "Fuzzy logic based anomaly detection for embedded network security cyber sensor," in *Proc. IEEE Symp. Comput. Intell. Cyber Secur. (CICS)*, Apr. 2011, pp. 202–209, doi: 10.1109/CICYBS.2011.5949392.

[64] X. Xu, "Sequential anomaly detection based on temporal-difference learning: Principles, models and case studies," *Appl. Soft Comput.*, vol. 10, no. 3, pp. 859–867, Jun. 2010, doi: 10.1016/j.asoc.2009.10.003.

[65] F. Iglesias and T. Zseby, "Analysis of network traffic features for anomaly detection," *Mach. Learn.*, vol. 101, nos. 1–3, pp. 59–84, Oct. 2015, doi: 10.1007/s10994-014-5473-9.

[66] N. Pandeeswari and G. Kumar, "Anomaly detection system in cloud environment using fuzzy clustering based ANN," *Mobile Netw. Appl.*, vol. 21, no. 3, pp. 494–505, Jun. 2016, doi: 10.1007/s11036-015-0644-x.

[67] K. Demertzis and I. Lazaros, "A hybrid network anomaly and intrusion detection approach based on evolving spiking neural network classification," in *Proc. Int. Conf. E-Democracy*, vol. 441, Dec. 2014, pp. 11–23, doi: 10.1007/978-3-319-11710-2.

[68] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in *Proc. 15th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2016, pp. 195–200, doi: 10.1109/ICMLA.2016.0040.

[69] S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, "Unsupervised real-time anomaly detection for streaming data," *Neurocomputing*, vol. 262, pp. 134–147, Nov. 2017, doi: 10.1016/j.neucom.2017.04.070.

[70] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *J. Comput. Sci.*, vol. 25, pp. 152–160, Mar. 2018, doi: 10.1016/j.jocs.2017.03.006.

[71] G. Dini, F. Martinelli, A. Saracino, and D. Sgandurra, "MADAM: A multi-level anomaly detector for Android malware," in *Proc. Int. Conf. Math. Methods, Models, Archit. Comput. Netw. Secur.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 7531, 2012, pp. 240–253, doi: 10.1007/978-3-642-33704-8_21.

[72] V. A. Sotiris, P. W. Tse, and M. G. Pecht, "Anomaly detection through a Bayesian support vector machine," *IEEE Trans. Rel.*, vol. 59, no. 2, pp. 277–286, Jun. 2010.

[73] M. Längkvist, L. Karlsson, and A. Loutfi, "Sleep stage classification using unsupervised feature learning," *Adv. Artif. Neural Syst.*, vol. 2012, pp. 1–9, Jul. 2012, doi: 10.1155/2012/107046.

[74] J. Song, H. Takakura, Y. Okabe, and K. Nakao, "Toward a more practical unsupervised anomaly detection system," *Inf. Sci.*, vol. 231, pp. 4–14, May 2013, doi: 10.1016/j.ins.2011.08.011.

[75] 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, doi: 10.1109/ACCESS.2017.2762418.

[76] C. A. Catania, F. Bromberg, and C. G. Garino, "An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection," *Expert Syst. Appl.*, vol. 39, no. 2, pp. 1822–1829, Feb. 2012, doi: 10.1016/j.eswa.2011.08.068.

[77] Z. Liao, Y. Yu, and B. Chen, "Anomaly detection in GPS data based on visual analytics," in *Proc. IEEE Symp. Vis. Analytics Sci. Technol.*, Oct. 2010, pp. 51–58, doi: 10.1109/VAST.2010.5652467.

[78] A. Purarjomandlangrudi, A. H. Ghapanchi, and M. Esmalifalak, "A data mining approach for fault diagnosis: An application of anomaly detection algorithm," *Measurement*, vol. 55, pp. 343–352, Sep. 2014, doi: 10.1016/j.measurement.2014.05.029.

[79] A. F. Emmott, S. Das, T. Dietterich, A. Fern, and W.-K. Wong, "Systematic construction of anomaly detection benchmarks from real data," in *Proc. ACM SIGKDD Workshop Outlier Detection Description (ODD)*, 2013, pp. 16–21, doi: 10.1145/2500853.2500858.

[80] D. J. Hill and B. S. Minsker, "Anomaly detection in streaming environmental sensor data: A data-driven modeling approach," *Environ. Model. Softw.*, vol. 25, no. 9, pp. 1014–1022, Sep. 2010, doi: 10.1016/j.envsoft.2009.08.010.

[81] G. Pachauri and S. Sharma, "Anomaly detection in medical wireless sensor networks using machine learning algorithms," *Procedia Comput. Sci.*, vol. 70, pp. 325–333, Jan. 2015, doi: 10.1016/j.procs.2015.10.026.

[82] X.-S. Gan, J.-S. Duanmu, J.-F. Wang, and W. Cong, "Anomaly intrusion detection based on PLS feature extraction and core vector machine," *Knowl.-Based Syst.*, vol. 40, pp. 1–6, Mar. 2013, doi: 10.1016/j.knosys.2012.09.004.

[83] W. Li, G. Wu, and Q. Du, "Transferred deep learning for anomaly detection in hyperspectral imagery," *IEEE Geosci. Remote Sens. Lett.*, vol. 14, no. 5, pp. 597–601, May 2017, doi: 10.1109/LGRS.2017.2657818.

[84] C. Wressnegger, G. Schwenk, D. Arp, and K. Rieck, "A close look on n -grams in intrusion detection," in *Proc. ACM Workshop Artif. Intell. Secur. (AISec)*, Nov. 2013, pp. 67–76, doi: 10.1145/2517312.2517316.

[85] J. Li, G. Han, J. Wen, and X. Gao, "Robust tensor subspace learning for anomaly detection," *Int. J. Mach. Learn. Cybern.*, vol. 2, no. 2, pp. 89–98, Jun. 2011, doi: 10.1007/s13042-011-0017-0.

[86] C. Zhou and R. C. Paffenroth, "Anomaly detection with robust deep autoencoders," in *Proc. 23rd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2017, pp. 665–674, doi: 10.1145/3097983.3098052.

[87] D. J. Dean, H. Nguyen, and X. Gu, "UBL: Unsupervised behavior learning for predicting performance anomalies in virtualized cloud systems," in *Proc. 9th Int. Conf. Auton. Comput. (ICAC)*, 2012, pp. 191–200, doi: 10.1145/2371536.2371572.

[88] L. Xiong, X. Chen, and J. Schneider, "Direct robust matrix factorizatoin for anomaly detection," in *Proc. IEEE 11th Int. Conf. Data Mining (ICDM)*, Dec. 2011, pp. 844–853, doi: 10.1109/ICDM.2011.52.

[89] Y.-J. Lee, Y.-R. Yeh, and Y.-C.-F. Wang, "Anomaly detection via online oversampling principal component analysis," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 7, pp. 1460–1470, Jul. 2013, doi: 10.1109/TKDE.2012.99.

[90] N. Laptev, S. Amizadeh, and I. Flint, "Generic and scalable framework for automated time-series anomaly detection," in *Proc. 21th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2015, pp. 1939–1947, doi: 10.1145/2783258.2788611.

[91] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, and B. Furht, "Sensor fault and patient anomaly detection and classification in medical wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, vol. 7, no. 4, pp. 272–284, doi: 10.1109/icc.2013.6655254.

[92] L. Ma, M. M. Crawford, and J. Tian, "Anomaly detection for hyperspectral images based on robust locally linear embedding," *J. Infr., Millim., THz Waves*, vol. 31, no. 6, pp. 753–762, Mar. 2010, doi: 10.1007/s10762-010-9630-3.

[93] R. Zhao, B. Du, and L. Zhang, "A robust nonlinear hyperspectral anomaly detection approach," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 7, no. 4, pp. 1227–1234, Apr. 2014, doi: 10.1109/JSTARS.2014.2311995.

[94] P. Angelov, "Anomaly detection based on eccentricity analysis," in *Proc. IEEE Symp. Evolving Auton. Learn. Syst. (EALS)*, Dec. 2014, pp. 1–8, doi: 10.1109/EALS.2014.7009497.

[95] P. H. dos Santos Teixeira and R. L. Milidiú, "Data stream anomaly detection through principal subspace tracking," in *Proc. ACM Symp. Appl. Comput.*, 2010, p. 1609, doi: 10.1145/1774088.1774434.

[96] S. T. F. Al-Janabi and H. A. Saeed, "A neural network based anomaly intrusion detection system," in *Proc. Develop. E-Syst. Eng. (DeSE)*, Dec. 2011, pp. 221–226, doi: 10.1109/DeSE.2011.19.

[97] F. Palmieri and U. Fiore, "Network anomaly detection through nonlinear analysis," *Comput. Secur.*, vol. 29, no. 7, pp. 737–755, Oct. 2010, doi: 10.1016/j.cose.2010.05.002.

[98] A. Taylor, N. Japkowicz, and S. Leblanc, "Frequency-based anomaly detection for the automotive CAN bus," in *Proc. World Congr. Ind. Control Syst. Secur. (WCICSS)*, Dec. 2015, pp. 45–49, doi: 10.1109/WCICSS.2015.7420322.

[99] Y. Zhu, N. M. Nayak, and A. K. Roy-Chowdhury, "Context-aware activity recognition and anomaly detection in video," *IEEE J. Sel. Topics Signal Process.*, vol. 7, no. 1, pp. 91–101, Feb. 2013, doi: 10.1109/JSTSP.2012.2234722.

[100] D. Smith, Q. Guan, and S. Fu, "An anomaly detection framework for autonomic management of compute cloud systems," in *Proc. IEEE 34th Annu. Comput. Softw. Appl. Conf. Workshops*, Jul. 2010, pp. 376–381, doi: 10.1109/COMPSACW.2010.72.

[101] M. Teng, "Anomaly detection on time series," in *Proc. IEEE Int. Conf. Prog. Informat. Comput.*, Dec. 2010, pp. 603–608. [Online]. Available: http://arxiv.org/abs/1708.02975.

[102] S. Lee, G. Kim, and S. Kim, "Self-adaptive and dynamic clustering for online anomaly detection," *Expert Syst. Appl.*, vol. 38, no. 12, pp. 14891–14898, Nov. 2011, doi: 10.1016/j.eswa.2011.05.058.

[103] S. Arshad, M. Abbaspour, M. Kharrazi, and H. Sanatkar, "An anomaly-based botnet detection approach for identifying stealthy botnets," in *Proc. IEEE Int. Conf. Comput. Appl. Ind. Electron. (ICCAIE)*, Dec. 2011, pp. 564–569, doi: 10.1109/ICCAIE.2011.6162198.

[104] S. Chauhan and L. Vig, "Anomaly detection in ECG time signals via deep long short-term memory networks," in *Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA)*, Oct. 2015, pp. 1–7, doi: 10.1109/DSAA.2015.7344872.

[105] S. Calderara, U. Heinemann, A. Prati, R. Cucchiara, and N. Tishby, "Detecting anomalies in people's trajectories using spectral graph analysis," *Comput. Vis. Image Understand.*, vol. 115, no. 8, pp. 1099–1111, Aug. 2011, doi: 10.1016/j.cviu.2011.03.003.

[106] S. Garg, K. Kaur, N. Kumar, and J. J. P. C. Rodrigues, "Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 566–578, Mar. 2019, doi: 10.1109/TMM.2019.2893549.

[107] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," *Expert Syst. Appl.*, vol. 29, no. 4, pp. 713–722, Nov. 2005, doi: 10.1016/j.eswa.2005.05.002.

[108] D. Kang, D. Fuller, and V. Honavar, "Learning classifiers for misuse detection using a bag of system calls representation," in *Proc. Int. Conf. Intell. Secur. Inform.*, 2005, pp. 511–516.

[109] E. Leon, O. Nasraoui, and J. Gomez, "Anomaly detection based on unsupervised niche clustering with application to network intrusion detection," in *Proc. Congr. Evol. Comput.*, 2004, pp. 502–508, doi: 10.1109/cec.2004.1330898.

[110] A. Del Giorno, J. A. Bagnell, and M. Hebert, "A discriminative framework for anomaly detection in large videos," in *Computer Vision—ECCV*, vol. 9905. Cham, Switzerland: Springer, 2016, pp. 334–349, doi: 10.1007/978-3-319-46454-1_21.

[111] J. Jabez, S. Gowri, S. Vigneshwari, J. A. Mayan, and S. Srinivasulu, "Anomaly detection by using CFS subset and neural network with WEKA tools," in *Information and Communication Technology for Intelligent Systems*, vol. 106. 2019, pp. 675–682, doi: 10.1007/978-981-13-1742-2.

[112] R. Laxhammar and G. Falkman, "Online learning and sequential anomaly detection in trajectories," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 36, no. 6, pp. 1158–1173, Jun. 2014, doi: 10.1109/TPAMI.2013.172.

[113] M. Schneider, W. Ertel, and F. Ramos, "Expected similarity estimation for large-scale batch and streaming anomaly detection," *Mach. Learn.*, vol. 105, no. 3, pp. 305–333, Dec. 2016, doi: 10.1007/s10994-016-5567-7.

[114] X. Chen, B. Li, R. Proietti, Z. Zhu, and S. J. B. Yoo, "Self-taught anomaly detection with hybrid unsupervised/supervised machine learning in optical networks," *J. Lightw. Technol.*, vol. 37, no. 7, pp. 1742–1749, Apr. 1, 2019.

[115] H. H. Pajouh, G. Dastghaibyfard, and S. Hashemi, "Two-tier network anomaly detection model: A machine learning approach," *J. Intell. Inf. Syst.*, vol. 48, no. 1, pp. 61–74, Feb. 2017, doi: 10.1007/s10844-015-0388-x.

[116] S. Zhao, M. Chandrashekar, Y. Lee, and D. Medhi, "Real-time network anomaly detection system using machine learning," in *Proc. 11th Int. Conf. Design Reliable Commun. Netw. (DRCN)*, Mar. 2015, pp. 267–270.

[117] Y. K. Takehisa Yairi, "Telemetry-mining: A machine learning approach to anomaly detection and fault diagnosis for space systems," in *Proc. 2nd IEEE Int. Conf. Space Mission Challenges Inf. Technol. (SMC-IT)*, Jul. 2006, pp. 466–473, doi: 10.1109/SMC-IT.2006.79.

[118] A. DeOrio, Q. Li, M. Burgess, and V. Bertacco, "Machine learning-based anomaly detection for post-silicon bug diagnosis," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, 2013, pp. 491–496.

[119] K.-L. Li, H.-K. Huang, S.-F. Tian, and W. Xu, "Improving one-class SVM for anomaly detection," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 5, 2003, pp. 3077–3081, doi: 10.1109/icmlc.2003.1260106.

[120] C. Wagner, J. François, R. State, and T. Engel, "Machine learning approach for IP-flow record anomaly detection," in *Proc. Int. Conf. Res. Netw.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 6640, 2011, pp. 28–39, doi: 10.1007/978-3-642-20757-0_3.

[121] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, "Anomaly detection for a water treatment system using unsupervised machine learning," in *Proc. IEEE Int. Conf. Data Mining Workshops (ICDMW)*, Nov. 2017, pp. 1058–1065.

[122] Y. Li, B. Fang, L. Guo, and Y. Chen, "Network anomaly detection based on TCM-KNN algorithm," in *Proc. 2nd ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*, 2007, pp. 13–19, doi: 10.1145/1229285.1229292.
[123] F. Maggi, S. Zanero, and V. Iozzo, "Seeing the invisible: Forensic uses of anomaly detection and machine learning," *ACM SIGOPS Oper. Syst. Rev.*, vol. 42, no. 3, pp. 51–58, Apr. 2008, doi: 10.1145/1368506.1368514.
[124] H. H. W. J. Bosman, A. Liotta, G. Iacca, and H. J. Wortche, "Anomaly detection in sensor systems using lightweight machine learning," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2013, pp. 7–13, doi: 10.1109/SMC.2013.9.
[125] S. Shriram and E. Sivasankar, "Anomaly detection on shuttle data using unsupervised learning techniques," in *Proc. Int. Conf. Comput. Intell. Knowl. Economy (ICCIKE)*, Dec. 2019, pp. 221–225, doi: 10.1109/ICCIKE47802.2019.9004325.
[126] K. Limthong, K. Fukuda, Y. Ji, and S. Yamada, "Weighting technique on multi-timeline for machine learning-based anomaly detection system," in *Proc. Int. Conf. Comput., Commun. Secur. (ICCCS)*, Dec. 2015, pp. 1–6, doi: 10.1109/CCCS.2015.7374168.
[127] J. Shi, G. He, and X. Liu, "Anomaly detection for key performance indicators through machine learning," in *Proc. Int. Conf. Netw. Infrastruct. Digit. Content (IC-NIDC)*, Aug. 2018, pp. 1–5, doi: 10.1109/ICNIDC.2018.8525714.
[128] O. I. Provotar, Y. M. Linder, and M. M. Veres, "Unsupervised anomaly detection in time series using LSTM-based autoencoders," in *Proc. IEEE Int. Conf. Adv. Trends Inf. Theory (ATIT)*, Dec. 2019, pp. 513–517, doi: 10.1109/ATIT49449.2019.9030505.
[129] S. Kumar, S. Nandi, and S. Biswas, "Research and application of one-class small hypersphere support vector machine for network anomaly detection," in *Proc. 3rd Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2011, pp. 1–4, doi: 10.1109/COMSNETS.2011.5716425.
[130] Y. Imamverdiyev and L. Sukhostat, "Anomaly detection in network traffic using extreme learning machine," in *Proc. IEEE 10th Int. Conf. Appl. Inf. Commun. Technol. (AICT)*, Oct. 2016, pp. 1–4, doi: 10.1109/ICAICT.2016.7991732.
[131] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning for network anomalies detection," in *Proc. Int. Conf. Mach. Learn. Data Eng. (iCMLDE)*, Dec. 2018, pp. 117–120, doi: 10.1109/iCMLDE.2018.00035.
[132] H.-G. Zhou and C.-D. Yang, "Using immune algorithm to optimize anomaly detection based on SVM," in *Proc. Int. Conf. Mach. Learn. Cybern.*, 2006, pp. 4257–4261, doi: 10.1109/ICMLC.2006.259008.
[133] Y. Shi and K. Miao, "Detecting anomalies in application performance management system with machine learning algorihms," in *Proc. 3rd Int. Conf. Electron. Inf. Technol. Comput. Eng. (EITCE)*, Oct. 2019, pp. 1797–1800, doi: 10.1109/EITCE47263.2019.9094916.
[134] P. K. Chan, M. V. Mahoney, and M. H. Arshad, "Learning rules and clusters for anomaly detection in network traffic," in *Managing Cyber Threats*. Boston, MA, USA: Springer-Verlag, 2005, pp. 81–99.
[135] T. Salman, D. Bhamare, A. Erbad, R. Jain, and M. Samaka, "Machine learning for anomaly detection and categorization in multi-cloud environments," in *Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud), 3rd IEEE Int. Conf. Scalable Smart Cloud (SSC)*, Jun. 2017, pp. 97–103, doi: 10.1109/CSCloud.2017.15.
[136] Z. Xiao, C. Liu, and C. Chen, "An anomaly detection scheme based on machine learning for WSN," in *Proc. 1st Int. Conf. Inf. Sci. Eng. (ICISE)*, 2009, pp. 3959–3962, doi: 10.1109/ICISE.2009.235.
[137] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, pp. 48231–48246, 2018, doi: 10.1109/ACCESS.2018.2863036.
[138] S. Rajasegarar, C. Leckie, and M. Palaniswami, "CESVM: Centered hyperellipsoidal support vector machine based anomaly detection," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 1610–1614, doi: 10.1109/ICC.2008.311.
[139] A. Valdes, R. Macwan, and M. Backes, "Anomaly detection in electrical substation circuits via unsupervised machine learning," in *Proc. IEEE 17th Int. Conf. Inf. Reuse Integr. (IRI)*, Jul. 2016, pp. 500–505, doi: 10.1109/IRI.2016.74.
[140] L. Kuang and M. Zulkernine, "An anomaly intrusion detection method using the CSI-KNN algorithm," in *Proc. ACM Symp. Appl. Comput. (SAC)*, 2008, pp. 921–926, doi: 10.1145/1363686.1363897.
[141] S. R. Gaddam, V. V. Phoha, and K. S. Balagani, "K-means+ID3: A novel method for supervised anomaly detection by cascading K-means clustering and ID3 decision tree learning methods," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 3, pp. 345–354, Mar. 2007, doi: 10.1109/TKDE.2007.44.
[142] E. K. Viegas, A. O. Santin, and L. S. Oliveira, "Toward a reliable anomaly-based intrusion detection in real-world environments," *Comput. Netw.*, vol. 127, pp. 200–216, Nov. 2017, doi: 10.1016/j.comnet.2017.08.013.
[143] Y. Wang, J. Wong, and A. Miner, "Anomaly intrusion detection using one class SVM," in *Proc. 5th Annu. IEEE Syst., Man Cybern. Inf. Assurance Workshop (SMC)*, Jun. 2004, pp. 358–364, doi: 10.1109/iaw.2004.1437839.
[144] B. I. P. Rubinstein, B. Nelson, L. Huang, A. D. Joseph, S.-H. Lau, S. Rao, N. Taft, and J. D. Tygar, "ANTIDOTE: Understanding and defending against poisoning of anomaly detectors," in *Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf. (IMC)*, 2009, pp. 1–14, doi: 10.1145/1644893.1644895.
[145] D. Liu, C.-H. Lung, I. Lambadaris, and N. Seddigh, "Network traffic anomaly detection using clustering techniques and performance comparison," in *Proc. 26th IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2013, pp. 1–4, doi: 10.1109/CCECE.2013.6567739.
[146] W. Chimphlee, A. H. Abdullah, M. N. M. Sap, S. Srinoy, and S. Chimphlee, "Anomaly-based intrusion detection using fuzzy rough clustering," in *Proc. Int. Conf. Hybrid Inf. Technol.*, Nov. 2006, pp. 329–334.
[147] T. M. Thang and J. Kim, "The anomaly detection by using DBSCAN clustering with multiple parameters," in *Proc. Int. Conf. Inf. Sci. Appl.*, Apr. 2011, pp. 1–5, doi: 10.1109/ICISA.2011.5772437.
[148] Y. Wang, D. Li, Y. Du, and Z. Pan, "Anomaly detection in traffic using L1-norm minimization extreme learning machine," *Neurocomputing*, vol. 149, pp. 415–425, Feb. 2015, doi: 10.1016/j.neucom.2014.04.073.
[149] J. Zhang and M. Zulkernine, "Anomaly based network intrusion detection with unsupervised outlier detection," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2006, pp. 2388–2393.
[150] T.-Y. Kim and S.-B. Cho, "Web traffic anomaly detection using C-LSTM neural networks," *Expert Syst. Appl.*, vol. 106, pp. 66–76, Sep. 2018, doi: 10.1016/j.eswa.2018.04.004.
[151] C.-H. Lin, J.-C. Liu, and C.-H. Ho, "Anomaly detection using LibSVM training tools," in *Proc. Int. Conf. Inf. Secur. Assurance (ISA)*, Apr. 2008, pp. 166–171, doi: 10.1109/ISA.2008.12.
[152] K. Li and G. Teng, "Unsupervised SVM based on p-kernels for anomaly detection," in *Proc. 1st Int. Conf. Innov. Comput., Inf. Control (ICICIC)*, 2006, pp. 59–62, doi: 10.1109/icicic.2006.371.
[153] X. G. Tian, L. Z. Gao, C. L. Sun, M. Y. Duan, and E. Y. Zhang, "A method for anomaly detection of user behaviors based on machine learning," *J. China Univ. Posts Telecommun.*, vol. 13, no. 2, pp. 61–78, 2006, doi: 10.1016/S1005-8885(07)60105-8.
[154] B. G. Atli, Y. Miche, A. Kalliola, I. Oliver, S. Holtmanns, and A. Lendasse, "Anomaly-based intrusion detection using extreme learning machine and aggregation of network traffic statistics in probability space," *Cognit. Comput.*, vol. 10, no. 5, pp. 848–863, Oct. 2018, doi: 10.1007/s12559-018-9564-y.
[155] Y. Tian, M. Mirzabagheri, S. M. H. Bamakan, H. Wang, and Q. Qu, "Ramp loss one-class support vector machine; a robust and effective approach to anomaly detection problems," *Neurocomputing*, vol. 310, pp. 223–235, Oct. 2018, doi: 10.1016/j.neucom.2018.05.027.
[156] H. Su, X. Wu, X.-H. Yan, and A. Kidwell, "Estimation of subsurface temperature anomaly in the indian ocean during recent global surface warming hiatus from satellite measurements: A support vector machine approach," *Remote Sens. Environ.*, vol. 160, pp. 63–71, Apr. 2015, doi: 10.1016/j.rse.2015.01.001.
[157] B. Cui and S. He, "Anomaly detection model based on Hadoop platform and weka interface," in *Proc. 10th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2016, pp. 84–89, doi: 10.1109/IMIS.2016.50.
[158] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100059, doi: 10.1016/j.iot.2019.100059.
[159] R. Abdulhammed, M. Faezipour, A. Abuzneid, and A. AbuMallouh, "Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic," *IEEE Sensors Lett.*, vol. 3, no. 1, pp. 1–4, Jan. 2019, doi: 10.1109/LSENS.2018.2879990.

[160] S. J. Stolfo, S. Hershkop, L. H. Bui, R. Ferster, and K. Wang, "Anomaly detection in computer security and an application to file system accesses," in *Proc. Int. Symp. Methodol. Intell. Syst.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 3488, 2005, pp. 14–28, doi: 10.1007/11425274_2.

[161] K. Limthong and T. Tawsook, "Network traffic anomaly detection using machine learning approaches," in *Proc. IEEE Netw. Oper. Manage. Symp.*, Apr. 2012, pp. 542–545, doi: 10.1109/NOMS.2012.6211951.

[162] F. Barani and S. Gerami, "ManetSVM: Dynamic anomaly detection using one-class support vector machine in MANETs," in *Proc. 10th Int. ISC Conf. Inf. Secur. Cryptol. (ISCISC)*, Aug. 2013, pp. 1–6, doi: 10.1109/ISCISC.2013.6767325.

[163] D. Wulsin, J. Blanco, R. Mani, and B. Litt, "Semi-supervised anomaly detection for EEG waveforms using deep belief nets," in *Proc. 9th Int. Conf. Mach. Learn. Appl.*, Dec. 2010, pp. 436–441, doi: 10.1109/ICMLA.2010.71.

[164] A. Adler, M. J. Mayhew, J. Cleveland, M. Atighetchi, and R. Greenstadt, "Using machine learning for behavior-based access control: Scalable anomaly detection on TCP connections and HTTP requests," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2013, pp. 1880–1887.

[165] B. Amos, H. Turner, and J. White, "Applying machine learning classifiers to dynamic Android malware detection at scale," in *Proc. 9th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jul. 2013, pp. 1666–1671, doi: 10.1109/IWCMC.2013.6583806.

[166] M. S. Parwez, D. B. Rawat, and M. Garuba, "Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 2058–2065, Aug. 2017, doi: 10.1109/TII.2017.2650206.

[167] G. Shah and A. Tiwari, "Anomaly detection in IIoT: A case study using machine learning," in *Proc. ACM India Joint Int. Conf. Data Sci. Manage. Data*, Jan. 2018, pp. 295–300, doi: 10.1145/3152494.3156816.

[168] P. M. Mafra, V. Moll, J. da Silva Fraga, and A. O. Santin, "Octopus-IIDS: An anomaly based intelligent intrusion detection system," in *Proc. IEEE Symp. Comput. Commun.*, Jun. 2010, pp. 405–410, doi: 10.1109/ISCC.2010.5546735.

[169] S. Anil and R. Remya, "A hybrid method based on genetic algorithm, self-organised feature map, and support vector machine for better network anomaly detection," in *Proc. 4th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2013, pp. 1–5, doi: 10.1109/ICCCNT.2013.6726604.

[170] R. Fujimaki, "Anomaly detection support vector machine and its application to fault diagnosis," in *Proc. 8th IEEE Int. Conf. Data Mining (ICDM)*, Dec. 2008, pp. 797–802, doi: 10.1109/ICDM.2008.69.

[171] S. D. Anton, S. Kanoor, D. Fraunholz, and H. D. Schotten, "Evaluation of machine learning-based anomaly detection algorithms on an industrial modbus/TCP data set," in *Proc.13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, vol. 41, no. 9, pp. 1–41, doi: 10.1145/3230833.3232818.

[172] G. Yan, "Network anomaly traffic detection method based on support vector machine," in *Proc. Int. Conf. Smart City Syst. Eng. (ICSCSE)*, Nov. 2016, pp. 3–6, doi: 10.1109/ICSCSE.2016.0011.

[173] L. Xiong, H.-D. Ma, H.-Z. Fang, K.-X. Zou, and D.-W. Yi, "Anomaly detection of spacecraft based on least squares support vector machine," in *Proc. Prognostics Syst. Health Managment Conf.*, May 2011, pp. 1–6, doi: 10.1109/PHM.2011.5939470.

[174] F. Wang, Y. Qian, Y. Dai, and Z. Wang, "A model based on hybrid support vector machine and self-organizing map for anomaly detection," in *Proc. Int. Conf. Commun. Mobile Comput. (CMC)*, Apr. 2010, pp. 97–101, doi: 10.1109/CMC.2010.9.

[175] J. Zhang, R. Gardner, and I. Vukotic, "Anomaly detection in wide area network meshes using two machine learning algorithms," *Future Gener. Comput. Syst.*, vol. 93, pp. 418–426, Apr. 2019, doi: 10.1016/j.future.2018.07.023.

[176] L. Deecke, R. Vandermeulen, L. Ruff, S. Mandt, and M. Kloft, "Image anomaly detection with generative adversarial networks," in *Proc. Joint Eur. Conf. Mach. Learn. Knowl. Discovery Databases*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 11051, 2019, pp. 3–17, doi: 10.1007/978-3-030-10925-7_1.

[177] M. Cosovic, S. Obradovic, and L. Trajkovic, "Performance evaluation of BGP anomaly classifiers," in *Proc. 3rd Int. Conf. Digit. Inf., Netw., Wireless Commun. (DINWC)*, Feb. 2015, pp. 115–120.

[178] G. D'angelo, F. Palmieri, M. Ficco, and S. Rampone, "An uncertainty-managing batch relevance-based approach to network anomaly detection," *Appl. Soft Comput.*, vol. 36, pp. 408–418, Nov. 2015, doi: 10.1016/j.asoc.2015.07.029.

[179] D. A. Kumar and S. R. Venugopalan, "A novel algorithm for network anomaly detection using adaptive machine learning," in *Progress in Advanced Computing and Intelligent Engineering* (Advances in Intelligent Systems and Computing), vol. 564. 2018, pp. 59–69, doi: 10.1007/978-981-10-6875-1_7.

[180] M. Marwah, R. Sharma, and C. Bash, "Thermal anomaly prediction in data centers," in *Proc. 12th IEEE Intersoc. Conf. Thermal Thermomechanical Phenomena Electron. Syst.*, Jun. 2010, pp. 1–7, doi: 10.1109/ITHERM.2010.5501330.

[181] N. Stakhanova, S. Basu, and J. Wong, "On the symbiosis of specification-based and anomaly-based detection," *Comput. Secur.*, vol. 29, no. 2, pp. 253–268, Mar. 2010, doi: 10.1016/j.cose.2009.08.007.

[182] J. Lundstrom, W. O. De Morais, and M. Cooney, "A holistic smart home demonstrator for anomaly detection and response," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2015, pp. 330–335, doi: 10.1109/PERCOMW.2015.7134058.

[183] Y. Yuan, J. Fang, and Q. Wang, "Online anomaly detection in crowd scenes via structure analysis," *IEEE Trans. Cybern.*, vol. 45, no. 3, pp. 548–561, Mar. 2015, doi: 10.1109/TCYB.2014.2330853.

[184] A. Barua, D. Muthirayan, P. P. Khargonekar, and M. A. Al Faruque, "Hierarchical temporal memory based machine learning for real-time, unsupervised anomaly detection in smart grid: WiP abstract," in *Proc. ACM/IEEE 11th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2020, pp. 188–189, doi: 10.1109/ICCPS48487.2020.00027.

[185] W. Yan, "One-class extreme learning machines for gas turbine combustor anomaly detection," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2016, pp. 2909–2914, doi: 10.1109/IJCNN.2016.7727567.

[186] A. Brown, A. Tuor, B. Hutchinson, and N. Nichols, "Recurrent neural network attention mechanisms for interpretable system log anomaly detection," in *Proc. 1st Workshop Mach. Learn. Comput. Syst.*, Jun. 2018, pp. 1–8, doi: 10.1145/3217871.3217872.

[187] K. Atefi, S. Yahya, A. Rezaei, and S. H. B. M. Hashim, "Anomaly detection based on profile signature in network using machine learning technique," in *Proc. IEEE Region Symp. (TENSYMP)*, May 2016, pp. 71–76, doi: 10.1109/TENCONSpring.2016.7519380.

[188] H. Suetani, A. M. Ideta, and J. Morimoto, "Nonlinear structure of escape-times to falls for a passive dynamic walker on an irregular slope: Anomaly detection using multi-class support vector machine and latent state extraction by canonical correlation analysis," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, Sep. 2011, pp. 2715–2722, doi: 10.1109/IROS.2011.6048434.

[189] L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez, "A self-adaptive deep learning-based system for anomaly detection in 5G networks," *IEEE Access*, vol. 6, pp. 7700–7712, 2018, doi: 10.1109/ACCESS.2018.2803446.

[190] F. Seraj, J. Van Der Zwaag, P. Havinga, A. Dilo, and T. Luarasi, "RoADS: A road pavement monitoring system for anomaly detection using smart phones," in *Proc. Int. Workshop Mach. Learn. Urban Sensor Data*, vol. 9546. Cham, Switzerland: Springer, 2016, pp. 128–146, doi: 10.1007/978-3-319-29009-6_7.

[191] M. Amar, I. Gondal, and C. Wilson, "Unitary anomaly detection for ubiquitous safety in machine health monitoring," in *Proc. Int. Conf. Neural Inf. Process.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 7667, 2012, pp. 361–368, doi: 10.1007/978-3-642-34500-5_43.

[192] K. Stefanidis and A. G. Voyiatzis, "An HMM-based anomaly detection approach for SCADA systems," in *Proc. IFIP Int. Conf. Inf. Secur. Theory Pract.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 9895, 2016, pp. 85–99, doi: 10.1007/978-3-319-45931-8_6.

[193] S. C. Chin, A. Ray, and V. Rajagopalan, "Symbolic time series analysis for anomaly detection: A comparative evaluation," *Signal Process.*, vol. 85, no. 9, pp. 1859–1868, Sep. 2005, doi: 10.1016/j.sigpro.2005.03.014.

[194] F. A. González and D. Dasgupta, "Anomaly detection using real-valued negative selection," *Genet. Program. Evolvable Mach.*, vol. 4, no. 4, pp. 383–403, 2003, doi: 10.1023/A:1026195112518.

[195] E. H. M. Pena, L. F. Carvalho, S. Barbon, Jr., J. J. P. C. Rodrigues, and M. L. Proença, Jr., "Anomaly detection using the correlational paraconsistent machine with digital signatures of network segment," *Inf. Sci.*, vol. 420, pp. 313–328, Dec. 2017, doi: 10.1016/j.ins.2017.08.074.
[196] F. Gonzalez, D. Dasgupta, and R. Kozma, "Combining negative selection and classification techniques for anomaly detection," in *Proc. Congr. Evol. Comput. (CEC)*, vol. 1, 2002, pp. 705–710, doi: 10.1109/CEC.2002.1007012.
[197] E. Eskin, A. Arnold, M. Prerau, L. Portnoy, and S. Stolfo, "A geometric framework for unsupervised anomaly detection," in *Applications of Data Mining in Computer Security*. Springer, 2002, pp. 77–101.
[198] A.-D. Schmidt, F. Peters, F. Lamour, C. Scheel, S. A. Çamtepe, and Ş. Albayrak, "Monitoring smartphones for anomaly detection," *Mobile Netw. Appl.*, vol. 14, no. 1, pp. 92–106, Feb. 2009, doi: 10.1007/s11036-008-0113-x.
[199] M. V. Mahoney and P. K. Chan, "Learning rules for anomaly detection of hostile network traffic," in *Proc. 3rd IEEE Int. Conf. Data Mining (ICDM)*, Nov. 2003, pp. 601–604, doi: 10.1109/icdm.2003.1250987.
[200] R. Winding, T. Wright, and M. Chapple, "System anomaly detection: Mining firewall logs," in *Proc. Securecomm Workshops*, Aug. 2006, pp. 1–5, doi: 10.1109/SECCOMW.2006.359572.
[201] N. Duffield, P. Haffner, B. Krishnamurthy, and H. Ringberg, "Rule-based anomaly detection on IP flows," in *Proc. IEEE 28th Conf. Comput. Commun. (INFOCOM)*, Apr. 2009, pp. 424–432, doi: 10.1109/INFCOM.2009.5061947.
[202] T. Stibor, P. Mohr, J. Timmis, and C. Eckert, "Is negative selection appropriate for anomaly detection?" in *Proc. Conf. Genet. Evol. Comput. (GECCO)*, 2005, pp. 321–328, doi: 10.1145/1068009.1068061.
[203] L. Scime and J. Beuth, "Anomaly detection and classification in a laser powder bed additive manufacturing process using a trained computer vision algorithm," *Additive Manuf.*, vol. 19, pp. 114–126, Jan. 2018, doi: 10.1016/j.addma.2017.11.009.
[204] B. I. P. Rubinstein, B. Nelson, L. Huang, A. D. Joseph, S.-H. Lau, S. Rao, N. Taft, and J. D. Tygar, "Stealthy poisoning attacks on PCA-based anomaly detectors," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 37, no. 2, pp. 73–74, Oct. 2009, doi: 10.1145/1639562.1639592.
[205] D. S. Kim, H.-N. Nguyen, S.-Y. Ohn, and J. S. Park, "Fusions of GA and SVM for anomaly detection in intrusion detection system," in *Proc. Int. Symp. Neural Netw.*, in Lecture Notes in Computer Science, 2005, vol. 3498, no. 3, pp. 415–420, doi: 10.1007/11427469_67.
[206] E. L. Paula, M. Ladeira, R. N. Carvalho, and T. Marzagão, "Deep learning anomaly detection as support fraud investigation in Brazilian exports and anti-money laundering," in *Proc. 15th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2016, pp. 954–960, doi: 10.1109/ICMLA.2016.0172.
[207] R. Fujimaki, T. Yairi, and K. Machida, "An anomaly detection method for spacecraft using relevance vector learning," in *Proc. Pacific-Asia Conf. Knowl. Discovery Data Mining*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 3518, 2005, pp. 785–790, doi: 10.1007/11430919_92.
[208] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "ALDO: An anomaly detection framework for dynamic spectrum access networks," in *Proc. IEEE 28th Conf. Comput. Commun. (INFOCOM)*, Apr. 2009, pp. 675–683.
[209] K. Sequeira and M. Zaki, "ADMIT: Anomaly-based data mining for intrusions," in *Proc. 8th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2002, pp. 386–395.
[210] V. L. L. Thing, "IEEE 802.11 network anomaly detection and attack classification: A deep learning approach," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6, doi: 10.1109/WCNC.2017.7925567.
[211] K. M. Ting, T. Washio, J. R. Wells, and S. Aryal, "Defying the gravity of learning curve: A characteristic of nearest neighbour anomaly detectors," *Mach. Learn.*, vol. 106, no. 1, pp. 55–91, Jan. 2017, doi: 10.1007/s10994-016-5586-4.
[212] Y. Zhou, S. Yan, and T. S. Huang, "Detecting anomaly in videos from trajectory similarity analysis," in *Proc. IEEE Multimedia Expo Int. Conf.*, Jul. 2007, pp. 1087–1090.
[213] M. Du, F. Li, G. Zheng, and V. Srikumar, "DeepLog: Anomaly detection and diagnosis from system logs through deep learning," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1285–1298, doi: 10.1145/3133956.3134015.
[214] W. D. Fisher, T. K. Camp, and V. V. Krzhizhanovskaya, "Anomaly detection in earth dam and levee passive seismic data using support vector machines and automatic feature selection," *J. Comput. Sci.*, vol. 20, pp. 143–153, May 2017, doi: 10.1016/j.jocs.2016.11.016.
[215] M. Cheng, Q. Li, J. Lv, W. Liu, and J. Wang, "Multi-scale LSTM model for BGP anomaly classification," *IEEE Trans. Services Comput.*, early access, Apr. 10, 2018, doi: 10.1109/TSC.2018.2824809.
[216] S. Cho and S. Cha, "SAD: Web session anomaly detection based on parameter estimation," *Comput. Secur.*, vol. 23, no. 4, pp. 312–319, Jun. 2004, doi: 10.1016/j.cose.2004.01.006.
[217] S. J. Han, K. J. Kim, and S. B. Cho, "Evolutionary learning program's behavior in neural networks for anomaly detection," in *Proc. Int. Conf. Neural Inf. Process.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 3316, 2004, pp. 236–241, doi: 10.1007/978-3-540-30499-9_35.
[218] Y. Zhao, B. Deng, C. Shen, Y. Liu, H. Lu, and X.-S. Hua, "Spatio-temporal AutoEncoder for video anomaly detection," in *Proc. 25th ACM Int. Conf. Multimedia*, Oct. 2017, pp. 1933–1941, doi: 10.1145/3123266.3123451.
[219] C. Pascoal, M. R. de Oliveira, R. Valadas, P. Filzmoser, P. Salvador, and A. Pacheco, "Robust feature selection and robust PCA for Internet traffic anomaly detection," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1755–1763.
[220] G. Pang, C. Shen, and A. van den Hengel, "Deep anomaly detection with deviation networks," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Jul. 2019, pp. 353–362, doi: 10.1145/3292500.3330871.
[221] J. Liu, J. Gu, H. Li, and K. H. Carlson, "Machine learning and transport simulations for groundwater anomaly detection," *J. Comput. Appl. Math.*, vol. 380, Dec. 2020, Art. no. 112982, doi: 10.1016/j.cam.2020.112982.
[222] R. Bhatia, S. Benno, J. Esteban, T. V. Lakshman, and J. Grogan, "Unsupervised machine learning for network-centric anomaly detection in IoT," in *Proc. 3rd ACM CoNEXT Workshop Big DAta, Mach. Learn. Artif. Intell. Data Commun. Netw. (Big-DAMA)*, 2019, pp. 42–48, doi: 10.1145/3359992.3366641.
[223] Z. Chkirbene, S. Eltanbouly, M. Bashendy, N. AlNaimi, and A. Erbad, "Hybrid machine learning for network anomaly intrusion detection," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 163–170, doi: 10.1109/ICIoT48696.2020.9089575.
[224] J. Wang, J. Liu, J. Pu, Q. Yang, Z. Miao, J. Gao, and Y. Song, "An anomaly prediction framework for financial IT systems using hybrid machine learning methods," *J. Ambient Intell. Humanized Comput.*, vol. 2019, Dec. 2019, doi: 10.1007/s12652-019-01645-z.
[225] H. Goldberg, H. Kwon, and N. M. Nasrabadi, "Kernel eigenspace separation transform for subspace anomaly detection in hyperspectral imagery," *IEEE Geosci. Remote Sens. Lett.*, vol. 4, no. 4, pp. 581–585, Oct. 2007, doi: 10.1109/LGRS.2007.903083.
[226] Y. Feng, Z.-F. Wu, K.-G. Wu, Z.-Y. Xiong, and Y. Zhou, "An unsupervised anomaly intrusion detection algorithm based on swarm intelligence," in *Proc. Int. Conf. Mach. Learn. Cybern. (ICMLC)*, 2005, pp. 3965–3969, doi: 10.1109/icmlc.2005.1527630.
[227] H. Y. Shahir, U. Glasser, A. Y. Shahir, and H. Wehn, "Maritime situation analysis framework: Vessel interaction classification and anomaly detection," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Oct. 2015, pp. 1279–1289, doi: 10.1109/BigData.2015.7363883.
[228] D. B. Araya, K. Grolinger, H. F. ElYamany, M. A. M. Capretz, and G. Bitsuamlak, "An ensemble learning framework for anomaly detection in building energy consumption," *Energy Buildings*, vol. 144, pp. 191–206, Jun. 2017, doi: 10.1016/j.enbuild.2017.02.058.
[229] J. B. D. Cabrera, C. Gutiérrez, and R. K. Mehra, "Ensemble methods for anomaly detection and distributed intrusion detection in mobile ad-hoc networks," *Inf. Fusion*, vol. 9, no. 1, pp. 96–119, Jan. 2008, doi: 10.1016/j.inffus.2007.03.001.
[230] W. Fan, N. Bouguila, and D. Ziou, "Unsupervised anomaly intrusion detection via localized Bayesian feature selection," in *Proc. IEEE 11th Int. Conf. Data Mining (ICDM)*, Dec. 2011, pp. 1032–1037, doi: 10.1109/ICDM.2011.152.
[231] R. Perdisci, D. Ariu, P. Fogla, G. Giacinto, and W. Lee, "McPAD: A multiple classifier system for accurate payload-based anomaly detection," *Comput. Netw.*, vol. 53, no. 6, pp. 864–881, Apr. 2009.
[232] E. Eskin, "Detecting errors within a corpus using anomaly detection," in *Proc. 1st Meeting North Amer. Chapter Assoc. Comput. Linguistics*, 2000, pp. 1–6.

[233] J. Frery, A. Habrard, M. Sebban, O. Caelen, and L. He-Guelton, "Efficient top rank optimization with gradient boosting for supervised anomaly detection," in *Proc. Joint Eur. Conf. Mach. Learn. Knowl. Discovery Databases*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 10534, 2017, pp. 20–35, doi: 10.1007/978-3-319-71249-9_2.
[234] B. Hussain, Q. Du, and P. Ren, "Semi-supervised learning based big data-driven anomaly detection in mobile wireless networks," *China Commun.*, vol. 15, no. 4, pp. 41–57, Apr. 2018, doi: 10.1109/CC.2018.8357700.
[235] H. Alipour, Y. B. Al-Nashif, P. Satam, and S. Hariri, "Wireless anomaly detection based on IEEE 802.11 behavior analysis," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2158–2170, Oct. 2015, doi: 10.1109/TIFS.2015.2433898.
[236] H. H. Bosman, G. Iacca, A. Tejada, H. J. Wörtche, and A. Liotta, "Spatial anomaly detection in sensor networks using neighborhood information," *Inf. Fusion*, vol. 33, pp. 41–56, Jan. 2017, doi: 10.1016/j.inffus.2016.04.007.
[237] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, Jan. 2017, pp. 140–145, doi: 10.1109/HASE.2017.36.
[238] N. Erez and A. Wool, "Control variable classification, modeling and anomaly detection in modbus/TCP SCADA systems," *Int. J. Crit. Infrastruct. Protection*, vol. 10, pp. 59–70, Sep. 2015, doi: 10.1016/j.ijcip.2015.05.001.
[239] T. F. Ghanem, W. S. Elkilani, and H. M. Abdul-Kader, "A hybrid approach for efficient anomaly detection using metaheuristic methods," *J. Adv. Res.*, vol. 6, no. 4, pp. 609–619, Jul. 2015, doi: 10.1016/j.jare.2014.02.009.
[240] F. Schuster, A. Paul, and H. König, "Towards learning normality for anomaly detection in industrial control networks," in *Proc. IFIP Int. Conf. Auton. Infrastruct., Manage. Secur.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 7943, 2013, pp. 61–72, doi: 10.1007/978-3-642-38998-6_8.
[241] S. M. A. M. Gadal and R. A. Mokhtar, "Anomaly detection approach using hybrid algorithm of data mining technique," in *Proc. Int. Conf. Commun., Control, Comput. Electron. Eng. (ICCCCEE)*, Jan. 2017, pp. 1–6, doi: 10.1109/ICCCCEE.2017.7867661.
[242] Q. Guan and S. Fu, "Adaptive anomaly identification by exploring metric subspace in cloud computing infrastructures," in *Proc. IEEE 32nd Int. Symp. Reliable Distrib. Syst.*, Sep. 2013, pp. 205–214, doi: 10.1109/SRDS.2013.29.
[243] W. Haider, J. Hu, and M. Xie, "Towards reliable data feature retrieval and decision engine in host-based anomaly detection systems," in *Proc. IEEE 10th Conf. Ind. Electron. Appl. (ICIEA)*, Jun. 2015, pp. 513–517, doi: 10.1109/ICIEA.2015.7334166.
[244] R. Perdisci, G. Gu, and W. Lee, "Using an ensemble of one-class SVM classifiers to harden payload-based anomaly detection systems," in *Proc. 6th Int. Conf. Data Mining (ICDM)*, Dec. 2006, pp. 488–498.
[245] A. M. Vartouni, S. S. Kashi, and M. Teshnehlab, "An anomaly detection method to detect Web attacks using stacked auto-encoder," in *Proc. 6th Iranian Joint Congr. Fuzzy Intell. Syst. (CFIS)*, 2018, pp. 131–134.
[246] M. Fugate and J. R. Gattiker, "Anomaly detection enhanced classification in computer intrusion detection," in *Proc. Int. Workshop Support Vector Mach.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 2388, 2002, pp. 186–197, doi: 10.1007/3-540-45665-1_15.
[247] C. C. Michael and A. Ghosh, "Simple, state-based approaches to program-based anomaly detection," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 3, pp. 203–237, Aug. 2002, doi: 10.1145/545186.545187.
[248] Y. Liao, V. R. Vemuri, and A. Pasos, "Adaptive anomaly detection with evolving connectionist systems," *J. Netw. Comput. Appl.*, vol. 30, no. 1, pp. 60–80, Jan. 2007, doi: 10.1016/j.jnca.2005.08.005.
[249] V. R. Jakkula, A. S. Crandall, and D. J. Cook, "Enhancing anomaly detection using temporal pattern discovery," in *Advanced Intelligent Environments*. Boston, MA, USA: Springer, 2009, pp. 175–194.
[250] B. Vrat, N. Aggarwal, and S. Venkatesan, "Anomaly detection in IPv4 and IPv6 networks using machine learning," in *Proc. Annu. IEEE India Conf. (INDICON)*, Dec. 2015, pp. 1–6, doi: 10.1109/INDICON.2015.7443752.
[251] S. Muller, J. Lancrenon, C. Harpes, Y. Le Traon, S. Gombault, and J.-M. Bonnin, "A training-resistant anomaly detection system," *Comput. Secur.*, vol. 76, pp. 1–11, Jul. 2018.
[252] S. Xiuyao, W. Mingxi, C. Jermaine, and S. Ranka, "Conditional anomaly detection," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 5, pp. 631–644, May 2007, doi: 10.1109/TKDE.2007.1009.
[253] R. Jain and H. Shah, "An anomaly detection in smart cities modeled as wireless sensor network," in *Proc. Int. Conf. Signal Inf. Process. (IConSIP)*, Oct. 2016, pp. 1–5, doi: 10.1109/ICONSIP.2016.7857445.
[254] X. R. Wang, J. T. Lizier, O. Obst, M. Prokopenko, and P. Wang, "Spatiotemporal anomaly detection in gas monitoring sensor networks," in *Proc. Eur. Conf. Wireless Sensor Netw.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 4913, 2008, pp. 90–105, doi: 10.1007/978-3-540-77690-1_6.
[255] W. Li and Q. Li, "Using naive Bayes with AdaBoost to enhance network anomaly intrusion detection," in *Proc. 3rd Int. Conf. Intell. Netw. Intell. Syst. (ICINIS)*, Nov. 2010, pp. 486–489, doi: 10.1109/ICINIS.2010.133.
[256] X. Hang and H. Dai, "Applying both positive and negative selection to supervised learning for anomaly detection," in *Proc. Conf. Genet. Evol. Comput. (GECCO)*, 2005, pp. 345–352, doi: 10.1145/1068009.1068064.
[257] Y.-K. Wang, C.-T. Fan, K.-Y. Cheng, and P. S. Deng, "Real-time camera anomaly detection for real-world video surveillance," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 4, Jul. 2011, pp. 1520–1525, doi: 10.1109/ICMLC.2011.6017032.
[258] R. C. Aygun and A. G. Yavuz, "Network anomaly detection with stochastically improved autoencoder based models," in *Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, Jun. 2017, pp. 193–198, doi: 10.1109/CSCloud.2017.39.
[259] Y. Feng, Y. Yuan, and X. Lu, "Learning deep event models for crowd anomaly detection," *Neurocomputing*, vol. 219, pp. 548–556, Jan. 2017, doi: 10.1016/j.neucom.2016.09.063.
[260] S. Akcay, A. Atapour-Abarghouei, and T. P. Breckon, "GANomaly: Semi-supervised anomaly detection via adversarial training," in *Proc. Asian Conf. Comput. Vis.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 11363, 2019, pp. 622–637, doi: 10.1007/978-3-030-20893-6_39.
[261] M. Chang, A. Terzis, and P. Bonnet, "Mote-based online anomaly detection using echo state networks," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 5516, 2009, pp. 72–86, doi: 10.1007/978-3-642-02085-8_6.
[262] A. S. A. Aziz, A. T. Azar, M. A. Salama, A. E. Hassanien, and S. E.-O. Hanafy, "Genetic algorithm with different feature selection techniques for anomaly detectors generation," in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2013, pp. 769–774.
[263] G. Marín, P. Casas, and G. Capdehourat, "RawPower: Deep learning based anomaly detection from raw network traffic measurements," in *Proc. ACM SIGCOMM Conf. Posters Demos*, Aug. 2018, pp. 75–77, doi: 10.1145/3234200.3234238.
[264] P. Casas, F. Soro, J. Vanerio, G. Settanni, and A. D'Alconzo, "Network security and anomaly detection with big-DAMA, a big data analytics framework," in *Proc. IEEE 6th Int. Conf. Cloud Netw. (CloudNet)*, Sep. 2017, pp. 1–7, doi: 10.1109/CloudNet.2017.8071525.
[265] X. A. Hoang and J. Hu, "An efficient hidden Markov model training scheme for anomaly intrusion detection of server applications based on system calls," in *Proc. 12th IEEE Int. Conf. Netw. (ICON)*, vol. 4, Nov. 2004, pp. 470–474, doi: 10.1109/ICON.2004.1409210.
[266] I. O. de Urbina Cazenave, E. Köşlük, and M. C. Ganiz, "An anomaly detection framework for BGP," in *Proc. Int. Symp. Innov. Intell. Syst. Appl.*, Jun. 2011, pp. 107–111, doi: 10.1109/INISTA.2011.5946083.
[267] O. Raz, P. Koopman, and M. Shaw, "Semantic anomaly detection in online data sources," in *Proc. Int. Conf. Softw. Eng.*, 2002, pp. 302–312, doi: 10.1145/581339.581378.
[268] H. M. Anwer, M. Farouk, and A. Abdel-Hamid, "A framework for efficient network anomaly intrusion detection with features selection," in *Proc. 9th Int. Conf. Inf. Commun. Syst. (ICICS)*, Apr. 2018, pp. 157–162, doi: 10.1109/IACS.2018.8355459.
[269] X. Wang, J. S. Wong, F. Stanley, and S. Basu, "Cross-layer based anomaly detection in wireless mesh networks," in *Proc. 9th Annu. Int. Symp. Appl. Internet (SAINT)*, Jul. 2009, pp. 9–15, doi: 10.1109/SAINT.2009.11.
[270] K. Alrawashdeh and C. Purdy, "Reducing calculation requirements in FPGA implementation of deep learning algorithms for online anomaly intrusion detection," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Jun. 2017, pp. 57–62, doi: 10.1109/NAECON.2017.8268745.

[271] R. Kumari, Sheetanshu, M. K. Singh, R. Jha, and N. K. Singh, "Anomaly detection in network traffic using K-mean clustering," in *Proc. 3rd Int. Conf. Recent Adv. Inf. Technol. (RAIT)*, Mar. 2016, pp. 387–393, doi: 10.1109/RAIT.2016.7507933.

[272] P. Mulinka and P. Casas, "Stream-based machine learning for network security and anomaly detection," in *Proc. Workshop Big Data Anal. Mach. Learn. Data Commun. Netw.*, Aug. 2018, pp. 1–7, doi: 10.1145/3229607.3229612.

[273] T. Ahmed, M. Coates, and A. Lakhina, "Multivariate online anomaly detection using kernel recursive least squares," in *Proc. 26th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, May 2007, pp. 625–633.

[274] V. L. Cao, M. Nicolau, and J. McDermott, "A hybrid autoencoder and density estimation model for anomaly detection," in *Proc. Int. Conf. Parallel Problem Solving From Nature*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 9921, 2016, pp. 717–726, doi: 10.1007/978-3-319-45823-6_67.

[275] D. Narsingyani and O. Kale, "Optimizing false positive in anomaly based intrusion detection using genetic algorithm," in *Proc. IEEE 3rd Int. Conf. MOOCs, Innov. Technol. Educ. (MITE)*, Oct. 2015, pp. 72–77, doi: 10.1109/MITE.2015.7375291.

[276] M. Sabokrou, M. Fayyaz, M. Fathy, Z. Moayed, and R. Klette, "Deep-anomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes," *Comput. Vis. Image Understand.*, vol. 172, pp. 88–97, Jul. 2018, doi: 10.1016/j.cviu.2018.02.006.

[277] R. Chalapathy, E. Toth, and S. Chawla, "Group anomaly detection using deep generative models," in *Proc. Joint Eur. Conf. Mach. Learn. Knowl. Discovery Databases*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 11051, 2019, pp. 173–189, doi: 10.1007/978-3-030-10925-7_11.

[278] F. Doelitzscher, M. Knahl, C. Reich, and N. Clarke, "Anomaly detection in IaaS clouds," in *Proc. IEEE 5th Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, vol. 1, Dec. 2013, pp. 387–394, doi: 10.1109/CloudCom.2013.57.

[279] N. F. Haq, A. R. Onik, and F. M. Shah, "An ensemble framework of anomaly detection using hybridized feature selection approach (HFSA)," in *Proc. SAI Intell. Syst. Conf. (IntelliSys)*, Nov. 2015, pp. 989–995, doi: 10.1109/IntelliSys.2015.7361264.

[280] J. Tian and H. Gu, "Anomaly detection combining one-class SVMs and particle swarm optimization algorithms," *Nonlinear Dyn.*, vol. 61, nos. 1–2, pp. 303–310, Jul. 2010, doi: 10.1007/s11071-009-9650-5.

[281] G. A. Susto, A. Beghi, and S. McLoone, "Anomaly detection through on-line isolation forest: An application to plasma etching," in *Proc. 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2017, pp. 89–94, doi: 10.23919/mipro.2017.7966552.

[282] I. Paredes-Oliva, I. Castell-Uroz, P. Barlet-Ros, X. Dimitropoulos, and J. Sole-Pareta, "Practical anomaly detection based on classifying frequent traffic patterns," in *Proc. IEEE INFOCOM Workshops*, Mar. 2012, pp. 49–54.

[283] I. Ullah and Q. H. Mahmoud, "A hybrid model for anomaly-based intrusion detection in SCADA networks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 2160–2167, doi: 10.1109/BigData.2017.8258164.

[284] X.-Q. Zhang and C.-H. Gu, "CH-SVM based network anomaly detection," in *Proc. Int. Conf. Mach. Learn. Cybern. (ICMLC)*, vol. 6, 2007, pp. 3261–3266, doi: 10.1109/ICMLC.2007.4370710.

[285] D. Li, D. Chen, B. Jin, L. Shi, J. Goh, and S.-K. Ng, "MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks," in *Proc. Int. Conf. Artif. Neural Netw.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 11730, 2019, pp. 703–716, doi: 10.1007/978-3-030-30490-4_56.

[286] T. Sipola, A. Juvonen, and J. Lehtonen, "Anomaly detection from network logs using diffusion maps," in *Proc. IFIP Int. Conf. Artif. Intell. Appl. Innov.*, vol. 363, 2011, pp. 172–181, doi: 10.1007/978-3-642-23957-1_20.

[287] M. Zhu, K. Ye, Y. Wang, and C. Z. Xu, "A deep learning approach for network anomaly detection based on AMF-LSTM," in *Proc. IFIP Int. Conf. Netw. Parallel Comput.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 11276, 2018, pp. 137–141, doi: 10.1007/978-3-030-05677-3_13.

[288] B. Shah and B. H. Trivedi, "Reducing features of KDD CUP 1999 dataset for anomaly detection using back propagation neural network," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Technol.*, Feb. 2015, pp. 247–251, doi: 10.1109/ACCT.2015.131.

[289] X. Gu and H. Wang, "Online anomaly prediction for robust cluster systems," in *Proc. IEEE 25th Int. Conf. Data Eng.*, Mar. 2009, pp. 1000–1011.

[290] A. Chiang, E. David, Y.-J. Lee, G. Leshem, and Y.-R. Yeh, "A study on anomaly detection ensembles," *J. Appl. Log.*, vol. 21, pp. 1–13, May 2017, doi: 10.1016/j.jal.2016.12.002.

[291] D. S. Terzi, R. Terzi, and S. Sagiroglu, "Big data analytics for network anomaly detection from netflow data," in *Proc. Int. Conf. Comput. Sci. Eng. (UBMK)*, Oct. 2017, pp. 592–597, doi: 10.1109/UBMK.2017.8093473.

[292] N. T. Van, T. N. Thinh, and L. T. Sach, "An anomaly-based network intrusion detection system using deep learning," in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, Jul. 2017, pp. 210–214, doi: 10.1109/ICSSE.2017.8030867.

[293] R. K. Malaiya, D. Kwon, S. C. Suh, H. Kim, I. Kim, and J. Kim, "An empirical evaluation of deep learning for network anomaly detection," *IEEE Access*, vol. 7, pp. 140806–140817, 2019, doi: 10.1109/ACCESS.2019.2943249.

[294] D. Yao, M. Yin, J. Luo, and S. Zhang, "Network anomaly detection using random forests and entropy of traffic features," in *Proc. 4th Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, Nov. 2012, pp. 926–929, doi: 10.1109/MINES.2012.146.

[295] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Quarter sphere based distributed anomaly detection in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 3864–3869, doi: 10.1109/ICC.2007.637.

[296] D. Boro, B. Nongpoh, and D. K. Bhattacharyya, "Anomaly based intrusion detection using meta ensemble classifier," in *Proc. 5th Int. Conf. Secur. Inf. Netw. (SIN)*, 2012, pp. 143–147, doi: 10.1145/2388576.2388596.

[297] F. Yihunie, E. Abdelfattah, and A. Regmi, "Applying machine learning to anomaly-based intrusion detection systems," in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, May 2019, pp. 1–5, doi: 10.1109/LISAT.2019.8817340.

[298] L. Bontemps, V. L. Cao, J. McDermott, and N. A. Le-Khac, "Collective anomaly detection based on long short-term memory recurrent neural networks," in *Proc. Int. Conf. Future Data Secur. Eng.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 10018, 2016, pp. 141–152, doi: 10.1007/978-3-319-48057-2_9.

[299] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 305–310, doi: 10.1109/CCWC.2019.8666450.

[300] S. Rayana and L. Akoglu, "Less is more: Building selective anomaly ensembles," *ACM Trans. Knowl. Discovery From Data*, vol. 10, no. 4, pp. 1–33, Jul. 2016, doi: 10.1145/2890508.

[301] D. Damopoulos, G. Kambourakis, and G. Portokalidis, "The best of both worlds: A framework for the synergistic operation of host and cloud anomaly-based IDS for smartphones," in *Proc. 7th Eur. Workshop Syst. Secur.*, 2014, pp. 1–6, doi: 10.1145/2592791.2592797.

[302] D. Ippoliti and X. Zhou, "A-GHSOM: An adaptive growing hierarchical self organizing map for network anomaly detection," *J. Parallel Distrib. Comput.*, vol. 72, no. 12, pp. 1576–1590, Dec. 2012, doi: 10.1016/j.jpdc.2012.09.004.

[303] D. Cozzolino and L. Verdoliva, "Single-image splicing localization through autoencoder-based anomaly detection," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2016, pp. 1–6, doi: 10.1109/WIFS.2016.7823921.

[304] M. Al-Subaie and M. Zulkernine, "Efficacy of hidden Markov models over neural networks in anomaly intrusion detection," in *Proc. 30th Annu. Int. Comput. Softw. Appl. Conf. (COMPSAC)*, Sep. 2006, pp. 325–332, doi: 10.1109/COMPSAC.2006.40.

[305] R. Fujimaki, T. Yairi, and K. Machida, "An approach to spacecraft anomaly detection problem using kernel feature space," in *Proc. 11th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2005, pp. 401–410, doi: 10.1145/1081870.1081917.

[306] I. Khokhlov, M. Perez, and L. Reznik, "Machine learning in anomaly detection: Example of colluded applications attack in Android devices," in *Proc. 18th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2019, pp. 1328–1333, doi: 10.1109/ICMLA.2019.00216.

[307] A. Selvaraj, R. Patan, A. H. Gandomi, G. G. Deverajan, and M. Pushparaj, "Optimal virtual machine selection for anomaly detection using a swarm intelligence approach," *Appl. Soft Comput.*, vol. 84, Nov. 2019, Art. no. 105686, doi: 10.1016/j.asoc.2019.105686.

[308] R. Punmiya, O. Zyabkina, S. Choe, and J. Meyer, "Anomaly detection in power quality measurements using proximity-based unsupervised machine learning techniques," in *Proc. Electr. Power Qual. Supply Rel. Conf. (PQ), Symp. Electr. Eng. Mechatronics (SEEM)*, Jun. 2019, pp. 1–6, doi: 10.1109/PQ.2019.8818236.

[309] Y. Li, X. Luo, Y. Qian, and X. Zhao, "Network-wide traffic anomaly detection and localization based on robust multivariate probabilistic calibration model," *Math. Problems Eng.*, vol. 2015, pp. 1–26, Jan. 2015, doi: 10.1155/2015/923792.

[310] E. Quatrini, F. Costantino, G. Di Gravio, and R. Patriarca, "Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities," *J. Manuf. Syst.*, vol. 56, pp. 117–132, Jul. 2020, doi: 10.1016/j.jmsy.2020.05.013.

[311] Y. Liu, Z. Pang, M. Karlsson, and S. Gong, "Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control," *Building Environ.*, vol. 183, Oct. 2020, Art. no. 107212, doi: 10.1016/j.buildenv.2020.107212.

[312] P. Tang, W. Qiu, Z. Huang, S. Chen, M. Yan, H. Lian, and Z. Li, "Anomaly detection in electronic invoice systems based on machine learning," *Inf. Sci.*, vol. 535, pp. 172–186, Oct. 2020, doi: 10.1016/j.ins.2020.03.089.

[313] I. G. A. Poornima and B. Paramasivan, "Anomaly detection in wireless sensor network using machine learning algorithm," *Comput. Commun.*, vol. 151, pp. 331–337, Feb. 2020, doi: 10.1016/j.comcom.2020.01.005.

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

[315] H. A. Nguyen, T. Van Nguyen, D. I. Kim, and D. Choi, "Network traffic anomalies detection and identification with flow monitoring," in *Proc. 5th IFIP Int. Conf. Wireless Opt. Commun. Netw. (WOCN)*, May 2008, pp. 1–5, doi: 10.1109/WOCN.2008.4542524.

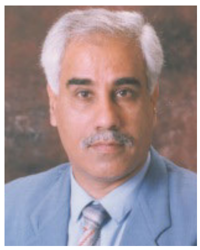
[316] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, *Network Traffic Anomaly Detection and Prevention*. Springer, 2017.

[317] X. Lu, P. Liu, and J. Lin, "Network traffic anomaly detection based on information gain and deep learning," in *Proc. 3rd Int. Conf. Inf. Syst. Data Mining (ICISDM)*, 2019, pp. 11–15, doi: 10.1145/3325917.3325946.

[318] Y. Gu, A. McCallum, and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," in *Proc. 5th ACM SIGCOMM Conf. Internet Meas. (IMC)*, 2005, p. 32, doi: 10.1145/1330107.1330148.

ALI BOU NASSIF (Member, IEEE) received the master's degree in computer science and the Ph.D. degree in electrical and computer engineering from Western University, Canada, in 2009 and 2012, respectively. He is currently the Assistant Dean of graduate studies with the University of Sharjah, United Arab Emirates. He is also an Associate Professor with the Department of Computer Engineering and an Adjunct Research Professor with Western University. He is also a registered Professional Engineer (P.Eng.) in ON, Canada. He has published more than 65 refereed conference papers and journal articles. His research interests include the applications of statistical and artificial intelligence models in different areas, such as software engineering, electrical engineering, e-learning, security, networking, signal processing, and social media. He is a member of IEEE Computer Society.

MANAR ABU TALIB (Senior Member, IEEE) is currently teaching with the University of Sharjah, United Arab Emirates. She is also working on ISO standards for measuring the functional size of software and has been involved in developing the Arabic version of ISO 19761 (COSMIC-FFP measurement method). She published more than 50 refereed conferences, journals, manuals, and technical reports. Her research interests include software engineering with substantial experience and knowledge in conducting research in software measurement, software quality, software testing, ISO 27001 for information security, and open source software. She is also the ArabWIC VP of Chapters with Arab Women in Computing Association (ArabWIC), the Google Women Tech Maker Lead, the Co-coordinator of OpenUAE Research and Development Group, and the International Collaborator with the Software Engineering Research Laboratory, Montreal, Canada.



QASSIM NASIR has been an Associate Professor with the University of Sharjah, since 2009, and the Chairman of Scientific Publishing Unit. Prior to joining the University of Sharjah, he was with Nortel Networks, Canada, as a Senior System Designer in the Network Management Group for OC-192 SONET. He was a Visiting Professor with the Helsinki University of Technology, Finland, from Summer 2002 to Summer 2009, and the GIPSA-lab, Grenoble, France, to work on a joint research project on "MAC protocol and MIMO" and "Sensor Networks and MIMO." He is also a co-coordinator with the OpenUAE Research Group, which focuses on blockchain performance and security and the use of artificial intelligence in security applications. He also conducts research in drone and GPS jamming as well. He has published over 90 refereed conferences, journals, book chapter, and technical reports. His current research interests include telecommunication and network security, such as in CPS and the IoT.

FATIMA MOHAMAD DAKALBAB received the bachelor's degree in information technology multimedia with a 3.92/4 GPA. She is currently pursuing the M.Sc. degree in computer science with the University of Sharjah, United Arab Emirates. She is also a Graduate Research Assistant with the University of Sharjah and the OpenUAE Research and Development Group. Her research interests include inter-blockchain communication, the Internet of things (IoT), and machine learning in anomaly detection. Since 2016, she has been a member of the Sharjah Google Developer Group (GDG) and Arab Women in Computing Association (ArabWIC). In addition to being a Events and Workshops Co-Coordinator in the student chapter, United Arab Emirates, for the Association for Computing Machinery (ACM).