Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic

Mian Muhammad Abdullah[1]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
amian1886@gmail.com

Hamayun Khan[2]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Sabestean[3]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
sabesteansumar10@gmail.com

Muhammad Farhan[4]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
farhanshoukatali37@gmail.com

Farhan Khadim[5]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
Farhankhadim32102@gmail.com

Hafiz-ul-Asad[6]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
asadhch12345@gmail.com

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

SES

Abstract

With the growth in the number of network users because of improvements in network technologies, there has been a corresponding increase in the traffic data on networks, which has become susceptible to attacks and intrusions. Hence, there is a growing need for effective security mechanisms for anomaly detection and prevention of intrusions. Of late, network security has drawn much attention from researchers and labs. This paper discusses the present review of current progressions of anomaly detection based on published studies in the past five years. Modern techniques and opportunities are considered along with discussing various applications of such technologies as WSNs, the Internet of Things (IoT), high-performance computing, industrial control systems, and SDNs. Advancement in machine learning and artificial intelligence has improved techniques for anomaly detection. Supervised, unsupervised, and semi-supervised learning improve the detectability of attacks. Supervised models make use of labeled datasets to recognize known attack patterns, while unsupervised models identify new ones by analyzing traffic behavior without prior threat knowledge. Hybrid approaches that combine multiple approaches are becoming a robust solution to the complexities of network traffic. The paper further introduces ongoing challenges in enhancing the anomaly detection system with regard to the handling and reduction of false positives in high-dimensional data and achieving real-time processing for increased reliability. All this detailed analysis is done to make an attempt at a clearer picture of the present scenario with regard to anomaly detection and the upcoming trends in network security.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

INDEX TERMS: Anomaly Detection, Networks, Supervised, Intrusion, Unsupervised, Anomaly Detection

Introduction

The detection of anomalies and abnormal activity in the network have become the most common problem in the industrial research area [1]. Anomaly detection is widely used in different types of applications, such as health monitoring systems, fault detection in critical systems, fraud detection, crime investigation, and cyber-intrusion detection [2]. With the rapid development of extensive-scale network technology along with users and services, the security of information is becoming imperative for any network system. Therefore, many studies and researches took a broad scope in the security area, with various methods and techniques that helped many researchers to work on the development of algorithms and feasible methods in the detection of abnormal activities innetwork traffic. The machine learning (ML) concept has been actively present in the last decade in many applications to solve various problems in network security. The major problem to whichML techniques are applied is anomaly detection in the network. Many ML techniques have been used or proposed for this purpose in different aspects and different methods, but the most used techniques are categorized under supervised and unsupervised machine learning. Based on review studies in this area, these two types of ML have received considerable attention by researchers, who suggested these techniques to be used either separately or combined [3]. In fact, several researchers have used these two ML techniques and their results have led to improved performance of attack detection and increased anomaly detection efficiency. The question that remains is: how do researchers decide which ML (unsupervised or supervised) technique to use for a specific problem or dataset? In other words, how do we know which ML technique is going to fit better with our dataset and lead to better results?

These questions motivated us to investigate the differences between the supervised and unsupervised approaches in recent applications related to anomaly detection systems. The main aim of this survey is to review various ML techniques used for anomaly detection to provide maximal understanding amongst the existing techniques that may help interested researchers toboost their future work in this direction. The paper is structured as follows.

In section 2, we discuss the different types of anomalies. Section 3 describes the use of ML for anomaly detection. In section 4, we explain the significant types of network attacks. Sections 5 and 6 discuss the supervised and unsupervised techniques recently used and their variations are evaluated. In section 7, we compare the supervised and unsupervised techniques. Section 8 presents the work on semi-supervised techniques briefly. Finally, we conclude our work and highlight some open issues and challenges in section 9.

A computer network is a combination of many individual entities assembled together to provide complete and various communication services. Anomalies in these networks are network activities that differ from standard, usual or expected behavior, and are suspected from a security perspective. They are also known as abnormal activities that attempt to disrupt the normal functions of the network.

Define anomalies as "patterns in data that do not conform to a well- defined notion of normal behavior". express the term as "a point in time where the behavior of the system is unusual and significantly different from previous, normal behavior [4]. Anomalies are also called abnormalities, outliers, or exceptions. They have been defined in manyways by different authors with different backgrounds, resulting in creating confusion of the terms related to anomalies. To understanding those definitions, the first step to knowing what isabnormal in a network system is understanding the normality. There are various types of network anomalies [5], which can be categorized into three types: point anomalies, contextual anomalies, and collective anomalies, as shown in Figure 1.

A point anomaly is considered as the simplest type of anomaly, where any single point of data has different attributes from its group of data. For example, in credit card transactions, the dailyspend of money is a hundred dollars, but on a specific day the spending rises to four hundred dollars. This type of anomaly transaction is called a point anomaly [6].

A contextual anomaly also known as a conditional anomaly, where the data behave anomalously in a specific context. However, conditional anomalies are usually applied to time- series data. For example, admission for short courses during summer takes typically 30 to 40 students for each course. If the admissions in some courses are below 15 students, we considered this as an anomaly. A collective anomaly is detected when a collection of data groups behaves anomalously within the whole dataset. In this type, individual anomaly behaviour is not considered as anomalies. Nevertheless, the frequent occurrence in these data is considered an anomaly. For a better understanding of the concept, the following example is given: in the computer, there is a sequence of actions that occurs together, such as buffer-overflow, HTTP-web, FTP, HTTP-web, SSH, HTTP-web, SSH, buffer-overflow, HTTP-web [6].

Anomaly Detection Use Machine Learning

Anomaly detection is the process of finding an effective way to discover anomalous values in a dataset that behave abnormally in the system. The importance of this process lies in that anomalies in data are translated into important practical information in a wide range of application areas. Anomaly detection provides a method of identifying a possible threat behavior and takes appropriate action when it occurs [7]. Generally, the anomaly detection system is an automated security system used for monitoring, analyzing, and detecting abnormal activities within a network or host report that there are four major elements to be considered when creating an anomaly or intrusion detection system: resources to protect, models to identify the typical behavior of the resources, techniques that compare the actual activities of these resources with their healthy behavior's, and, finally, identifying what is considered anomalous or unwelcome objects. In this paper, we focus on anomaly-based intrusion detection systems (AIDS) [8]. However, the investigation of network intrusion using AIDS has been of interest to many researchers and authors. The researchers have presented a detailed description of various aspects and types of anomaly detection systems along with various models and techniques used to defend many attacks that we will discuss in detail later. In any network computer system, there is potentially a large number of activities, traffic, and log information available on it [9]. The majority of activities are standard, but a tiny number of activities may be outside the border of what is usual or expected. Those unexpected activities are potential anomalies or intrusions. However, as the dataset of such systems is extremely large, diverse, and ever-growing, the patterns of the anomaly may not be evident and easy

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

to find. The ideas of the concept of machine learning may be an essential way to find potential intrusion patterns. Machine learning aims to extract valid, potentially helpful, and significative patterns torecognize intricate patterns in existing datasets to help to make intelligent decisions or predictions, by using a nontrivial learning mechanism [10].

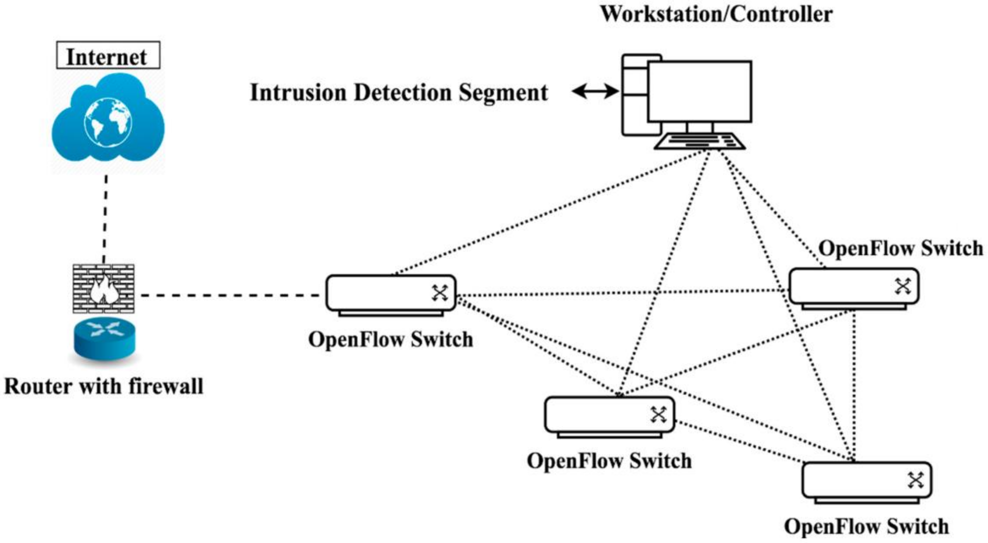

Figure 1. Anomaly in ML based Networks

In general,all machine learning algorithms follow standard steps to classify the anomalies and intrusions, as follows:

Data Cleaning and Noise Removal: in this stage, the data is cleaned by removing outliers and unwanted data. This will improve the quality of the training data andlead to a better and more accurate prediction model. classify or label the data into normal or abnormal [11].

Named Entity Recognition: it is necessary to know some entities to predict anomalies such as packets, IP address, time, size, and activity, then classify them as positive normal, or abnormal.

Subjectivity Classification: Subjectivity is a term referring to any attributes, events, or the properties of entities.

Feature Selection: the process of automatically selecting the features which are relevant to our data to predict the interested variables or output and help the system to detect anomalies [12]

The basic idea of using a machine learning algorithm is to provide the ability to learn from a given dataset and address the problems in a similar dataset automatically without human intervention. Several algorithms and methods have beenused by researchers and developers to overcome the network security challenges and avoid network attacks. Primarily, the machine learning approaches can be categorized into three main classes as shown in Figure 2:supervised learning, unsupervised learning and semi-supervised learning. Supervised learning is mainly used for classification or prediction, whereas unsupervised learning is used for clustering. The semi-supervised class is a hybrid approach between supervised and unsupervised classes [13, 14]. Figure2 also shows some examples of well-known classification and clustering algorithms.

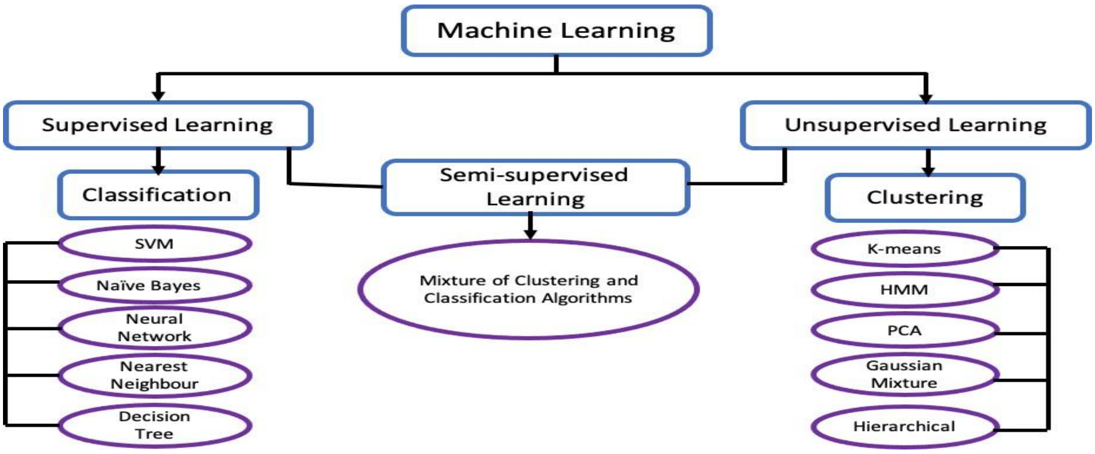

Figure 2. Machine Learning Techniques used in Networks [15]

Literature Review

A network attack is an illegal attempt to avail of the vulnerability of a computer or network, attempting to break through the security of the network system. Researcher in [16] classifies attackers into two types: external and internal. External attackers are unauthorized users in the systems they attack, whereas internal attackers have the authority to access the system, but do not have access to the root or super user. Classify attacks into seven main types based on the implementation of those attacks, as shown in Table 1. In this article, we will concentrate on the most critical and recent attacks from different categories with different examples. Also, we will highlight ML approaches and algorithms used to detect those attacks.

Table 1. Attack categories Supervised Learning

Main category	Definition	Examples	Ref
Infection	Aim to infect the target system either by tampering or by installing evil files in the system.	Viruses, Worms, Trojans.	[16]
Exploding	Seek to explode or overflow the target system with bugs.	Buffer Overflow.	[17]
Prop	Gather information about the target system through tools.	Sniffing, Port sweep, IP sweep.	[18]
Cheat	Typical examples of this category include attempts to use a fake identity.	IP Spoofing, MAC Spoofing, DNS Spoofing, Session Hijacking, XSS Attacks, Hidden Area Operation.	[19]
Traverse	Attempts to crack a victim system through a dull match against all possible keys.	Brute Force, Dictionary Attacks,	[20]

		Doorknob Attacks.	
Concurrency	Victimize a system or a service by sending a mass of identical requests which exceeds the capacity that the system or the service could supply.	Flooding, DDoS (Distributed Denial of Service).	[21]
Others	These attacks attempt to infect the target system by using system bugs or weaknesses directly.		

Classification is one of the terms which refers to supervised learning. Applying supervisedtechniques on the network data sets allows us to build a model, and the data instances can be labelled using a set of attributes. Many supervised algorithms are used to detect anomalies and intrusions in the network traffic and have proven effectiveness and efficiency, such as Support Vector Machine(SVM), Artificial Neural Network(ANN), Nearest Neighbour algorithm, DecisionTrees, K-nearest neighbour, Ensembles classifiers, and Naïve Bayes classifier. These algorithms are more commonly used in the supervised learning approach. In the following, we summarize the research works that have been done using these supervised learning algorithms for anomaly detection in the past five years.

Support Vector Machine (SVM)

Introduced a new Intrusion Detection model based on a Particle Swarm Optimization algorithm(PSO), which joins a feature selection algorithm using information gain with a SVM classifier. The authors concluded that, by combining feature selection and parameter optimization for SVM, training and testing time are reduced and the effectiveness of the SVM Classifier is improved. The proposed model

FS PSO-SVM results in obtaining ahigh detection rate and the lowest false positive rate. They tested the effectiveness of the proposed model by using the NSL-KDD Dataset, which includes 41 features, and by testing the model through 4 types of network attacks: DoS, R2L, U2Rand Prob [22]. Proposed an intrusion detection (ID) framework based on the SVM ensemble classifier with increasing features selection. Their idea is to integrate the powerful quality-improved transformation with the SVM ensemble. They built a robust intrusion detection framework with low training complexity, powerful performance, and high accuracy. However, they considered only the binary case of intrusion detection problems. They applied their proposal on the NSL-KDD Dataset and used a cross-validation (10-fold) method to train and test the model. The result of their experiment showed that the proposed framework could achieve robust performance, a high detection rate, and a low false alarm rate [23].

Presented a novel framework to enhance the resilience of SVMs against training-data-integrity attacks. The proposed approach uses random projections on top of the learners. This makes it challenging for the attacker to guess the specific configurations of the learners. They introduce novel indices that ensure the shrinking of the data and increase the detection accuracy.Their contribution is characterized by the use of nonlinear random projections for defense techniques for learners (SVMs/One Class SVMs). Several datasets were used in this experiment, such as MNIST, CIFAR- 10, and SVHN.The results indicated that SVM and OCSVM could be significantly affected if an attacker can manipulate the trained data [24].

Another approach using the SVM algorithm is proposed by

[25] to address the problem of the long training time of the prediction model, the authors proposed a prediction model based on the map-reduce technique and SVM classifier. They used an SVM classifier as a base classifier for the model and optimal parameters performed by the Cuckoo Search (CS).They used the Map Reduce (MR) technique and CS algorithm to enhance the SVM classifier to optimally solve the general problem of parameter optimization. They stated that the proposed model reached better results in terms of accuracy and it reduced training-time costs. [26] developed a Naïve Bayesian (NB) model for network intrusion detection based on PCA (Principal Component Analysis). The model utilized NB with PCA to extract new properties that helped them to improve the traditional NB algorithm, where traditional NB cannot consider the problem of weights in attributes. KDD CUP 99 was the experimental data set, and the type of attacks that dataset included were DoS, U2L, R2L, and Probe attack. This experiment has a good result in the detection rate with weighted Naïve Bayes classification, and it solves the problem of feature redundancy.

Author in [27] proposed a version of a Naïve Bayesian one-class classifier, OCPAD, for payload-based anomalies detection. OCPAD is a content method that identifies network packets with untrusted payload content. They have done many experiments with a large dataset showing that OCPAD can perform at an excellent level to detect anomalies with increasing Detection Rate as well as an agreeable False Positive Rate.

Author in [28] introduced a novel algorithm based on the Naïve Bayes model to detect attacks in data training. In their study, they conducted four testing data stages on the Kyoto 2006+ dataset. The training dataset contained 5000 average records and

5000 attacks, and all the four tests were evaluated by the Naïve Bayes model, which resulted in higher accuracy and detection rate. Author in [29] presented a new model of using the Naïve Bayes algorithm- based intrusion detection system. The proposed approach aims to protect the Internet of Things (IoT) infrastructure from Distributed Denial of Service (DDoS) attacks generated by the intruders and the complexity of IoT, where the data comes from heterogeneous resources that helped this type of attack to spreadin the IoT network.

The authors implemented a multi-agent- based IDS (NB-MAIDS). An NB classifier was applied with a multi-agent system (MAS) throughout the network and agents. They collected the information from sensors which help the system to report the activities of the abnormal nodes on the IoT network. This proved the efficiency of the NB classifier with multi-agents in the proposed approach, giving better performance to prevent attacks very quicklywith low execution costs. The experiment of proposed classifier effectiveness was tested on the NSL- KDD dataset.

Table 2. Supervised Anomaly detection approaches

Year	ML Technique	Anomaly type	Dataset	Detection :curacy (%)
[30]	MR-SVM classifier	generic attack in network	KDD, DARPA	96.16%
[31]	PSO – SVM Classifier	DoS, R2L, U2R and Prob	NSL-KDD	99.5%
[32]	SVM ensemble classifier	binary case of intrusion detection	NSL-KDD	99.36%

		problems		
[33]	SVM and OCSVM	training-data-integrity attacks	MNIST, CIFAR-10, SVHN	97%
[34]	Naïve Bayesian with PCA	DoS, R2L, U2R, and Prob	KDD CUP 99	87%
[35]	Naïve Bayesian OCPAD	Generic attack	HTTP dataset.	100%
[36]	Naïve Bayes(ANADA)	Generic attack	Kyoto 2006+	96.66%
[37]	NB-MAIDS	DDoS attack	NSL-KDD	90%

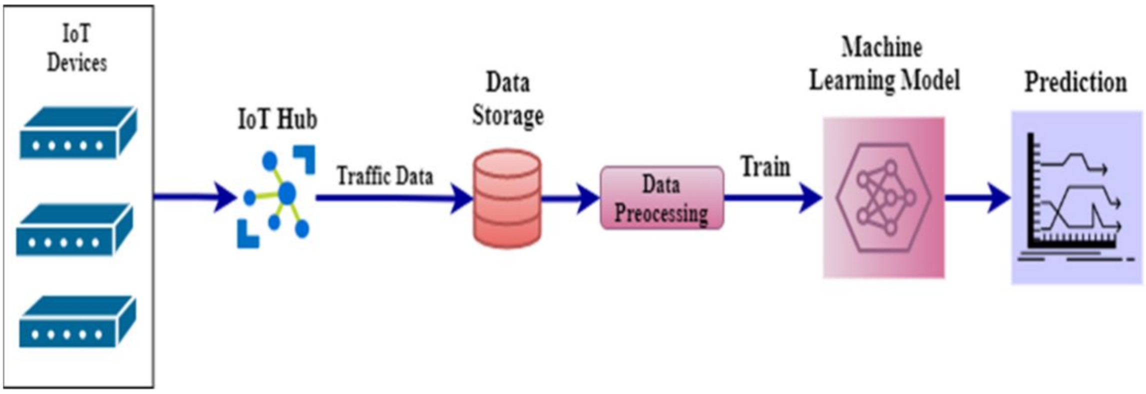

Figure 3. Delay in packets in Machine Learning Techniques used in Networks [37]

Nearest Neighbour

The nearest neighbour classifier is one of the supervised learning techniques that is widely used for anomaly detection. [38] introduced an effective detection technique based on CKNN to detect DDoS attacks. This method is applied across a data centre network by utilizing the training data correlation information and CKNN classification. Their contribution provideda novel approach

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

throughout the use of a CKNN classifier with correlation information. This helped to reduce the size of training data and to improve the classifier accuracy in detecting DDoS attacks with low cost and minimum response time. In this work, the authors used three types of dataset: broad, real, and KDD99.

Regarding the new type of Software Defined Networking (SDN) and their network flow problems [39] presented an SDN-based anomaly flow detection. This work was implemented for DDoS anomaly detection, where the K-nearest neighbour algorithm was the classification technique performed to detect flows using P-value. The results of the experiment showed that the DPTCM-KNN algorithm increases the detection accuracy rate of the anomalous flow detection, as well as reducing the false positive rate. This confirms that the algorithm has very good-performance in SDN platforms.

Background and Findings based on Anomaly types

Table 2 shows a comparison between the above research works that used the different supervised learning algorithms for anomaly detection. The comparison is in terms of publication year, supervised learning technique used, type of anomaly detected, dataset used, and accuracy

Table 3. Unsupervised anomaly detection approaches (SoA: State-of-the-art)

Year	ML Technique	Anomaly type	Dataset	Detection Accuracy (%)
[40]	HMM	Generic network attack	Real-time network	93.2%
[41]	HMM	Normal,DoS,MFCI,MPC	Collected by researchers	93.4%

		I,MSCI,CMRI		
[42]	HMM	Benign, DoS Hulk, Port Scan, DDoS, DoS, FTP Patator	CICIDS2017	97.9%
[43]	weighted HMM	DDOS attacks	DARPA2000	Better than the SoA
[44]	PCA	DDoS attacks	Abilene network dataset	93.33%
[45]	PCA	generic attack	KDD-CUP and UNB-ISCX	98.8%
[46]	Robust PCA	DDoS attacks, IP sweeps and probing and breaking	DARPA	Better than the SoA.
[47]	PCA	Generic attack	Kyoto Honeypot	Better than the SoA
[48]	Gaussian Mixture Model	Generic attack	WNS simulation	Better than the SoA
[49]	Gaussian Mixture - GMMs	Zero-day	UNIBS-2009	98.7%
[50]	GMMs	Outliers	Collected by researchers	Better than the SoA
[51]	GMMs	DoS, R2L, U2R, and	NSL- KDD	Better than

		Prob		the SoA
[52]	hierarchical approach	DoS, R2L, U2R, and Prob	NSL-KDD	96.1%
[53]	GAFCM + SVM	DoS, R2L, U2R and Prob	NSL-KDD	99.76%
[54]	dynamic hierarchical clustering	DoS, R2L, U2R, and Prob	KDD-Cup-99	98.2%
[55]	hierarchical clustering	BOT, DoS, R2L, U2R,Prob, PSCAN, Web Attacks	CICIDS2017	99%

Conclusion

With our lives getting more and more digitized, computer networks grow more critical and reliable service. At the same time, however, they become increasingly liable to anomalies and worse-than-those malicious attacks. Therefore, this motivates many researchers to propose various solution approaches to the broad overall problem of anomaly detection in network traffic, especially machine learning-based techniques, whether supervised or unsupervised.

In this paper we surveyed works in the area of anomaly detection using machine learning in the last five years. To begin with, we explained the context relevant to our research work: (i) the types of network anomalies;(ii) the categories of machine learning approaches; and (iii) the types of network attacks. After that, we have studied, classified and commented the papers that utilize machine learning technologies for anomaly detection. Finally, we emphasized some open issues that will be the key towards

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

enhancement of anomaly detection systems. Based on the above research, we were able to identify a plethora of things that deserve greater attention by For instance, detection rate, process complexity, and high false alarm rate, among others are examples of the research community within the anomaly detection area. We also find that an important challenge continues to be in realizing real-time anomaly detection systems, particularly where the type of data coming is constant in the changes of the stream. Finally, we observe that despite more than enough having gone into anomaly detection on normal computer networks, spread of the IoT and consequently their pervasiveness is what increases the need for them.For more scalable and accurate anomaly detection methods, oriented towards handling different data types, the security level of the IoT network infrastructure has to be top-notch.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[2] Aburomman, A. A., &Reaz, M. B. I. (2017). A survey of intrusion detection systems based on ensemble and hybrid classifiers.Computers & Security,65, 135-152.

[3] Agrawal, S., & Agrawal, J. (2015). Survey on anomaly detection using data mining techniques.Procedia Computer Science,60, 708-713.

[4] Ahmad, S., Lavin, A., Purdy, S., & Agha, Z. (2017). Unsupervised real-time anomaly detection for streaming data.Neurocomputing,262, 134-147.

[5] Akhi, A. B., Kanon, E. J., Kabir, A., &Banu, A. (2019).Network Intrusion Classification Employing Machine Learning: A Survey. (Doctoral dissertation)Department of Computer Science and Engineering, United International University, Bangladesh.

[6] Alizadeh, H., Khoshrou, A., &Zuquete, A. (2015). Traffic classification and verification using unsupervised learning of Gaussian Mixture Models. In2015 IEEE international workshop on measurements & networking (M&N). 1-6. IEEE. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[7] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[8] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[9] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[10] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A

Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[11] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[12] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[13] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[14] Khan, A. Yasmeen, S. Jan, U. Hashmi, "ENHANCED RESOURCE LEVELING INDYNAMIC POWER MANAGEMENT TECHNIQUEOF IMPROVEMENT IN PERFORMANCE FOR MULTI-CORE PROCESSORS" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[15] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[16] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020

3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[17] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[18] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[19] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[20] M. S. Abdul Razak, S. P. A. Gothandapani, N. Kamal, and K. Chellappan, “Presenting the Secure Collapsible Makerspace with Biometric Authentication”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 1, pp. 12880–12886, Feb. 2024.

[21] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[22] Amangele, P., Reed, M. J., Al-Naday, M., Thomos, N., & Nowak, M. (2019). Hierarchical Machine Learning for IoT Anomaly Detection in SDN. In2019 International Conference on Information Technologies (InfoTech). 1-4. IEEE.

[23] Anderson, J. P. (1980). Computer security threat monitoring and surveillance.Technical Report, Fort Washington, PA, James P. Anderson Co.

[24] Aung, Y. Y., & Min, M. M (2018). An analysis of K-means algorithm based network intrusion detection system. Advances in Science, Technology and Engineering Systems Journal,3(1), 496-501. Bauer, F. C., Muir, D. R., &Indiveri, G (2019). Real-Time Ultra-Low Power ECG Anomaly Detection

[25] Bhati, B. S., Rai, C. S., Balamurugan, B., & Al-Turjman, F. (2020). An intrusion detection scheme based on the ensemble of discriminant classifiers.Computers & Electrical Engineering,86, 106742.

[26] Bhattacharyya, D. K., &Kalita, J. K. (2013).Network anomaly detection: A machine learning perspective. CRCPress.

[27] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[28] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[29] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[30] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[31] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[32] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[33] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[34] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[35] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[36] Haripriya, L.A., Jabbar, M., &Seetharamulu, B. (2018). A Novel Intrusion Detection System Using Artificial Neural Networks and Feature Subset Selection. International Journal of Engineering and Technology, 7(4), 181. http://doi.org/10.14419/ijet.v7i4.6.20458

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[37] Hoang, D. H., & Nguyen, H. D. (2018). A PCA-based method for IoT network traffic anomaly detection. In2018 20th International Conference on Advanced Communication Technology (ICACT), 381-386. IEEE.

[38] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson,
R. (2016). Threat analysis of IoT networks using artificial neural network intrusiondetection system. In2016 International Symposium on Networks, Computers and Communications (ISNCC), 1-6. IEEE.

[39] Blanco, R., Malagón, P., Briongos, S., & Moya, J. M. (2019). Anomaly Detection Using Gaussian Mixture Probability Model to Implement Intrusion Detection System. InInternational Conference on Hybrid Artificial Intelligence Systems, 648-659. Springer, Cham.

[40] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey.ACM Computing Surveys (CSUR),41(3), 1-58.

[41] Chauhan, P., & Shukla, M. (2015). A review on outlier detection techniques on data stream by using different approaches of K-Means algorithm. In2015 International Conference on Advances in Computer Engineering and Applications. 580-585. IEEE.

[42] Chen, C. M., Guan, D. J., Huang, Y. Z., &Ou, Y. H. (2016). Anomaly network intrusion detection using hidden Markov model.International Journal of Innovative Computing, Information and Control,12, 569-580.

[43] Chew, Y. J., Ooi, S. Y., Wong, K. S., & Pang, Y. H. (2020). Decision Tree with Sensitive Pruning in Network-based Intrusion Detection System. InComputational Science and Technology, 1-10. Springer, Singapore.

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

SES

[44] Ding, M., & Tian, H. (2016). PCA-based network traffic anomaly detection.Tsinghua Science and Technology,21(5), 500-509.

[45] Dua, S., & Du, X. (2016).Data mining and machine learning in cybersecurity. CRC press.ernandes G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., &Proença, M. L. (2019). A comprehensive survey on network anomaly detection.Telecommunication Systems,70(3), 447-489.

[46] Gu, J., Wang, L., Wang, H., & Wang, S. (2019). A novel approach to intrusion detection using SVM ensemble with feature augmentation.Computers & Security,86, 53-62.

[47] Han, X., Xu, L., Ren, M., &Gu, W. (2015). A Naive Bayesian network intrusion detection algorithm based on Principal Component Analysis. In2015 7th International Conference on Information Technology in Medicine and Education (ITME), 325-328. IEEE.

[48] Hu, J., Ma, D., Liu, C., Shi, Z., Yan, H., & Hu, C. (2019). Network Security Situation Prediction Based on MR-SVM.IEEE Access,7, 130937-130945.

[49] Karim, S., Rousanuzzaman, P. A. Y., Khan, P. H., & Asif, M. (2019). Implementation of K-Means Clustering for Intrusion Detection. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5, 1232–41.

[50] Kevric, J., Jukic, S., &Subasi, A. (2017). An effective combining classifier approach using tree algorithms for network intrusion detection.Neural Computing and Applications,28(1), 1051- 1058.

[51] Khraisat, A., Gondal, I., &Vamplew, P. (2018). An anomaly intrusion detection system using C5 decision tree classifier. InPacific-Asia Conference on Knowledge Discovery and Data Mining, 149-155. Springer, Cham.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X
SES

[52] Kim, E., & Kim, S. (2015). A novel hierarchical detection method for enhancing anomaly detection efficiency. In2015 International Conference on Computational Intelligence and Communication Networks (CICN), 1018-1022. IEEE.

[53] Knapp, E. D., &Langill, J. T. (2014).Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress.

[54] Kotu, V., & Deshpande, B. (2018).Data Science: Concepts and Practice. Morgan Kaufmann.

[55] Kumar, D. A., &Venugopalan, S. R. (2018). A novel algorithm for network anomaly detection using adaptive machine learning. InProgress in Advanced Computing and Intelligent Engineering, 59-69. Springer, Singapore.