Role of Machine Learning in Intrusion Detection System: A Systematic Review

Areej Alhasani1 , Faten Al omrani2 , Taghreed Alzahrani3 , Rehab alFahhad4, Mohamed Alotaibi5
412010325@stu.ut.edu.sa , 412010319@stu.ut.edu.sa , 412010320@stu.ut.edu.sa 412010344@stu.ut.edu.sa , mmalotaibi@ut.edu.sa
College of Computer and Information Technology, University of Tabuk, Saudi Arabia

Summary

Over the last 10 years, there has been rapid growth in the use of Machine Learning (ML) techniques to automate the process of intrusion threat detection at a scale never imagined before. This has prompted researchers, software engineers, and network specialists to rethink the applications of machine ML techniques particularly in the area of cybersecurity. As a result there exists numerous research documentations on the use ML techniques to detect and block cyber-attacks. This article is a systematic review involving the identification of published scholarly articles as found on IEEE Explore and Scopus databases. The articles exclusively related to the use of machine learning in Intrusion Detection Systems (IDS). Methods, concepts, results, and conclusions as found in the texts are analyzed. A description on the process taken in the identification of the research articles included: First, an introduction to the topic which is followed by a methodology section. A table is used to list identified research articles in the form of title, authors, methodology, and key findings.

Keywords: *Cybersecurity, Cyber-Attacks, Network Security, Intrusion Detection, Machine Learning, Artificial intelligence.*

1. Introduction

The internet has exponentially advanced since its inception so have information systems that use or are hosted on it, such as, the Worldwide Web. The internet is notorious for insecurity often being the source of most cyber-attacks. On the other hand virtually all industries have adopted automation characterized by information systems integrated with networked infrastructure often having access to the internet. Internet access compounds the problem further particularly because the internet is vast and attacks could be anywhere taking any form. Furthermore, the dynamic nature of technology means intrusion techniques keep refining calling for adaptive security protocols. In other words security protocols must be continuously improved to be steps ahead of intrusion techniques continuously advancing in sophistication. Existing security protocols employ Intrusion Detection Systems that use varying strategies to detect intruders. Typically, IDS monitor user activity while its Artificial Intelligence capabilities detect, block, and report anomalies.

IDS types vary in scope and can be classified as network based or host-based intrusion detection and prevention systems. Network based IDS monitor traffic within computer networks while the later characteristically inspect system files [1]. Nonetheless, rapid advancement of technology particularly in the 21st century has significantly increased the size and scope of networks. For instance, massive amount of critical data is generated and shared among network nodes. As a result a significant number of new assaults, either through mutation of an old assault or a novel attack, has made the security of these data and network nodes a difficult issue. Security concerns can affect almost every node in a network. Moreover, existing IDSs have demonstrated ineffectiveness in detecting a variety of threats, including zero-day attacks, and in lowering false alarms (FAR) [2]. This eventually led to the urgent need for efficient, accurate, and cost-effective IDSs.

Integrating machine learning techniques with IDSs had been proposed as a viable solution to meeting the above goals. The method utilizes AI concepts to learn patterns and behaviors from vast amount of data [3]. Typically machines are trained to recognize legitimate and intrusive patterns. To learn relevant information from network traffic, the ML-based IDS mainly relies on feature engineering [4]. After registering improved success use of ML techniques in detection and prevention of attacks has gained significant popularity. Researchers have proposed several ways of improving machine learning techniques in detecting and preventing intrusions as evident in the literature review. The goal of this research paper is to give an evidence based review of recent developments and improvements in machine learning-based IDS systems. The major goal is to provide up-to-date information on recent ML-based IDS as

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.21

a starting point for researchers who want to commence research on the subject matter.

2. Methodology

This survey was conducted in May 2021 and involved searching through different databases including Scopus and IEEE Explore. The aim was to identify scholarly articles or papers touching on the use of ML techniques to detect and prevent cyber-attacks. The search words were the terms machine learning and Intrusion Detection Systems. Step one involved identifying books, journals and articles about the topic by searching the Scopus and IEEE databases. 116 documentations were identified from the Scopus database and 210 from the IEEE. Step two was about screening the identified articles to determine relevance of contents to the thesis statement. Screening test narrowed down the number of relevant documentations to 57. The third step involved scheming trough abstracts of the remaining documentations to further filter them in terms of relevance to the topic. This eligibility test resulted in 23 documentations being excluded leaving only 34. Lastly, step five involved digging deeper into the contents of remaining documentations. Figure 1 below simplifies the five steps. Table 1: Margin specifications

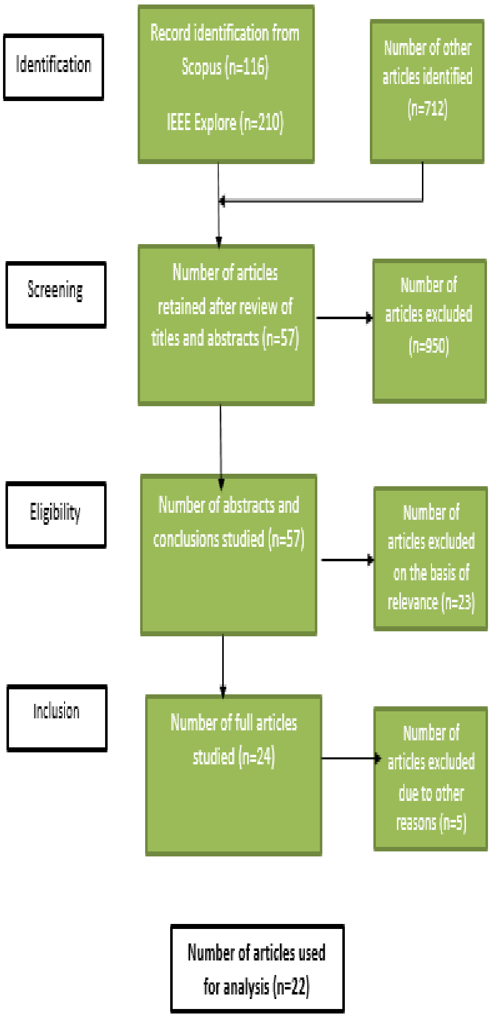
Identification
Record identification from Scopus (n=116)
IEEE Explore (n=210)
Number of other articles identified (n=712)
Screening
Number of articles retained after review of titles and abstracts (n=57)
Number of articles excluded (n=950)
Eligibility
Number of abstracts and conclusions studied (n=57)
Number of articles excluded on the basis of relevance (n=23)
Inclusion
Number of full articles studied (n=24)
Number of articles excluded due to other reasons (n=5)
Number of articles used for analysis (n=22)

Figure 1: PRISMA flow diagram for the review process of documentations related to the use of machine learning in integration with IDS systems

3. Results

. Table 1: List of studies that fit the study criteria

	Study Reference	***Study Method***	Study Outcomes/Results
[1]	Sultana, Nasrin, Naveen Chilamkurti, Wei Peng, and Rabei Alhadad. "Survey on SDN based network intrusion detection system using machine learning approaches." Peer-to-Peer Networking and Applications 12, no. 2 (2019): 493-501.	A research survey on existing research studies about application of Machine Learning (ML) in intrusiondetection systems.	According to evidence from this scholarly documentation, there are various tools that are used to develop Network Intrusion Detection Systems (NIDS). In particular, the deep learning techniques that are used in the development of Software Defined Networking technologies (SDN) based on NIDS. Several challenges exist concerning the implementation of ML based NIDS
[2]	Verma, Abhishek, and Virender Ranga. "Machine learning based intrusion detection systems for IoT applications." Wireless Personal Communications 111, no. 4 (2020): 2287-2310.	Empirical research study on the effectiveness of classification algorithms as used in securing Internet of Things (IoT) against attacks by Denial of Service (DoS) malwares.	Most common datasets such as NSL-KDD, CIDDS-1 and UNSW-NB15 have only moderate success in the protection of IoT from DoS attacks as compared to defense systems based on Deep Learning and Machine Learning.
[3]	Liu, Hongyu, and Bo Lang. "Machine learning and deep learning methods for intrusion detection systems: A survey." applied sciences 9, no. 20 (2019): 4396.	A research survey that proposes an Intrusion Detection System (IDS) taxonomy. This taxonomy uses data objects as the primary dimension in the classification and summary of IDS based machine learning and deep learning literature.	Comprehensive classification of the concept of IDS and its taxonomy was achieved. The proposed classification system was effective in explaining how IDS issues can be solved through machine learning and deep learning techniques.
Nun	***Study Reference***	***Study Method***	Study Outcomes/Results
[4]	Shah, Syed Ali Raza, and Biju Issac. "Performance comparison of intrusion detection systems and application of machine learning to Snort system." Future Generation Computer Systems 80 (2019): 157-170	An empirical research study to investigate the effectiveness of Snort and Suricata as applied to open source IDS to detect malicious threats to computer networks.	The Suricata IDS has the ability to process higher network speeds as compared to Snort but consumes higher operational and computational resources. According to the publication, Snort is more accurate in threat detection. However, it triggers large numbers of false alarms. A combination of Support Vector Machine (SVM) and fuzzy logic had better accuracy in terms of threat identification.
[5]	Wang, Yu, Weizhi Meng, Wenjuan Li, Zhe Liu, Yang Liu, and Hanxiao Xue. "Adaptive machine learning-based alarm reduction via edge computing for distributed intrusion detection systems." *Concurrency and Computation: Practice and Experience* 31, no. 19 (2019): e5101.	Empirical research to develop a framework to utilize machine learning and deep learning algorithms in the development of energy efficient IDS for use in cloud computer systems.	The proposed framework has the potential to improve IDS by reducing false alarms through the use of deep learning and machine learning applications. The framework can also reduce the strain placed on central servers and delays in threat detection as compared to other methods.

[6]	Othman, Suad Mohammed, Fadl Mutaher Ba-Alwi, Nabeel T. Alsohybe, and Amal Y. Al-Hashida. "Intrusion detection model using machine learning algorithm on Big Data environment." *Journal of Big Data* 5, no. 1 (2019): 1-12.	Empirical research to compare the effectiveness of the Spark Chi-SVM intrusion detection system and the Chi-Logistic Regression Classifier system. Experiment results showed that Spark-Chi-SVM model has high performance, reduces the training time and is efficient for Big Data.	The Spark-Chi-SVM IDS Model performs better than the Chi-Logistic Regression Classifier, it reduces the amount of training time required and it is efficient for use in Big Data systems.

	Study Reference	***Study Method***	Study Outcomes/Results
[7]	Biswas, Saroj Kr. "Intrusion detection using machine learning: A comparison study." *International Journal of pure and applied mathematics* 118, no. 19 (2019): 101-114.	A study to propose an IDS model that utilizes machine learning networks, a combination of feature selective techniques, and the most popular selection classifiers and techniques to increase efficiency	The K-NN classifier as a feature selection method performs better than the others. The information gain ratio as a feature selection method is better than the other classifiers.
[8]	Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., & Foozy, C. F. M. (2021). Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. IEEE Access, 9, 22351-22370.	A survey on existing literature on the effectiveness of the anomaly based IDS (AIDS) system in the detection of complex network attacks.	The DT-AIDS, k-NN-AIDS and the NB-AIDS models produce the best results and have greater capacities to detect web attacks in comparison with other models that produce irregular and inferior results. In general, the k-NN-AIDS, DT-AIDS, and NB-AIDS models obtain the best results and show a greater capability in detecting web attacks compared with other models that demonstrate irregular and inferior results.
[9]	Çavuşoğlu, Ü. (2019). A new hybrid approach for intrusion detection using machine learning methods. Applied Intelligence, 49(7), 2735-2761.	A research survey of existing literature about the development of hybrid, layered IDS. Its basis is a combination of various feature selection and machine learning techniques to achieve high performance in terms of detecting varying attack types.	The proposed system has high accuracy of intrusion detection and its false positive rate is comparatively lower for all types of attacks

	Study Reference	***Study Method***	Study Outcomes/Results
[10]	Wang, M., Zheng, K., Yang, Y., & Wang, X. (2020). An explainable machine learning framework for intrusion detection systems. *IEEE Access*, *8*, 73127-73141.	A research survey to propose a framework to give a standard explanation of IDS. Local and international explanations of IDS were used to derive a universal meaning and interpretation of IDS.	The proposed framework leads to transparency in the explanation and interpretation of IDS at the local and international level which will helps developers develop better and more efficient IDS systems.
[11]	Kumar, G., Thakur, K., & Ayyagari, M. R. (2020). MLEsIDSs: machine learning-based ensembles for intrusion detection systems—a review. *The Journal of Supercomputing*, 1-34.	A research on the motivation to use ML and comprehensive review of IDS based on the combination of a variety of machine learning applications.	There is great variety in the motivation for the use of a variety of machine learning applications in the development of IDS according to evidence from existing scholarly research.
[12]	Alqahtani, Hamed, Iqbal H. Sarker, Asra Kalim, Syed Md Minhaz Hossain, Sheikh Ikhlaq, and Sohrab Hossain. "Cyber Intrusion Detection Using Machine Learning Classification Techniques." In *International Conference on Computing Science,*	An empirical research study on the effectiveness of popular machine learning classification algorisms to provide intelligent detection services in the cybersecurity domain.	There are varying levels of effectiveness as per each popular machine learning classification algorithm as used to intelligently detect threats.

	Study Reference	***Study Method***	Study Outcomes/Results
[13]	Magán-Carrión, R., Urda, D., Díaz-Cano, I. and Dorronsoro, B., 2020. Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches. Applied Sciences, 10(5), p.1775.	A comprehensive survey of existing literature on NIDS applications based on machine learning and the development of structured methods that address problems related to network attacks. .	Most of the existing scholarly literature do not comprehensively accomplish the reliable evaluation and comparison of NIDS. The proposed structured methodology is highly reliable in evaluating and comparing the NIDS and in addressing problems of network attacks.
[14]	Belouch, Mustapha, Salah El Hadaj, and Mohamed Idhammad. "Performance evaluation of intrusion detection based on machine learning using Apache Spark." *Procedia Computer Science* 127 (2019): 1-6.	. Based on this framework, the paper in hand evaluates the performance of four well-known classification algorithms; SVM, Naïve Bayes, Decision Tree and Random Forest. It uses Apache Spark, a big data processing tool for intrusion detection in network traffic. The overall performance comparison is evaluated in terms of detection accuracy, building time and prediction time. Experimental results on UNSW-NB15, a recent public dataset for network intrusion detection.	Moreover, it show an important advantage of using Random Forest classifier among other well-known classifiers in terms of detection accuracy and prediction time. This is particularly so when the complete dataset with all 42 features is used.
[15]	Alrowaily, Mohammed, Freeh Alenezi, and Zhuo Lu. "Effectiveness of machine learning based intrusion detection systems." In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, pp. 277-288. Springer, Cham, 2019.	Empirical research to evaluate the performance of seven machine learning algorithms that use the CIODS201Y intrusion detection dataset.	The K-Nearest Neighbors (KNN) classifier is the most effective in terms of recall, F1-score, accuracy and precision as compared other types of machine learning classifiers

	Study Reference	***Study Method***	Study Outcomes/Results
[16]	Kilincer, Ilhan Firat, Fatih Ertam, and Abdulkadir Sengur. "Machine learning methods for cyber security intrusion detection: Datasets and comparative study." *Computer Networks* 188 (2021): 107840.	A survey on the scholarly literature on the effectiveness of the various types of different approaches used in the development of IDS.	According to most of the available research evidence; for an approach to be successful in the development of IDS, it must be based on the use of artificial intelligence applications such as machine learning.
[17]	Pawlicki, Marek, Michał Choraś, and Rafał Kozik. "Defending network intrusion detection systems against adversarial evasion attacks." Future Generation Computer Systems 110 (2020): 148-154.	An empirical research study to evaluate the likelihood of well-known detection algorithms deteriorating when adversarial attacks are used. Attacks are created or used basing on the four methods proposed recently and identifying most suitable ways of	There is lack of comprehensive research supporting use of artificial as they can be applied IDS
[18]	Mishra, Preeti, Vijay Varadharajan, Uday Tupakula, and Emmanuel S. Pilli. "A detailed investigation and analysis of using machine learning techniques for intrusion detection." *IEEE Communications Surveys & Tutorials* 21, no. 1 (2019): 686-728.	A comprehensive literature review analyzing different machine learning techniques used in intrusion detection systems.	Most of the existing research studies analyze and compare the machine learning techniques in terms of their capability to detect different types of intrusion attacks. In addition, most of the literature analyze the limitation of such techniques and provide recommendations for future improvements.

	Study Reference	*Study Method*	Study Outcomes/Results
[19]	Ever, Yoney Kirsal, Boran Sekeroglu, and Kamil Dimililer. "Classification analysis of intrusion detection on NSL-KDD using machine learning algorithms." In International Conference on Mobile Web and Intelligent Information Systems, pp. 111-122. Springer, Cham, 2019.	An empirical research study to test the effectiveness of the widely used NSL-KDD dataset in the detection of intrusion by running tests.	The degradation or increment of training ratio for attack instances in datasets has no direct effects on the performance of the IDS techniques.
[20]	Amouri, Amar, Vishwa T. Alaparthy, and Salvatore D. Morgera. "A machine learning based intrusion detection system for mobile Internet of Things." *Sensors* 20, no. 2 (2020): 461.	An empirical research study to compare the effectiveness of high and low power/node scenarios in the detection of DoS intrusion attacks.	High power/node scenarios have a 98% and above detection rate while low power/node scenarios have a 90% detection rate for DoS intrusion attacks.
[21]	Vimala, S., V. Khanaa, and C. Nalini. "A study on supervised machine learning algorithm to improvise intrusion detection systems for mobile ad hoc networks." *Cluster Computing* 22, no. 2 (2019): 4065-4074.	A research survey to propose a new method for application in an adaptive fault tolerant IDS based on a mobile agent.	The proposed model results in significant improvement in real time performance without compromising on efficiency.
[22]	Thakur, Soumyadeep, Anuran Chakraborty, Rajonya De, Neeraj Kumar, and Ram Sarkar. "Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model." Computers & Electrical Engineering 91, pp 44, 2021.	An empirical research study to propose a new method of Intrusion threat detection using machine learning algorithms by classifying of intrusion attacks.	The proposed intrusion detection system takes the form unique Generic-Specific auto-encoder architecture, with new benchmark results set on the CICIDS2017 dataset

4. Discussions

There is a huge collection of scholarly articles on the Scopus and IEEE Explore databases concerning use of Machine Language in Intrusion Detection Systems. Most of the articles are fairly recent, however in the last three years starting 2019 there has been a significant increase in the number of scholarly articles published on the topic. A significant portion of the published scholarly articles involves conducting research and targeted surveys on the existing literature on various aspects of the topic. Also, several techniques are proposed on how to better integrate IDS with ML techniques.

In addition, there is a large collection of articles that involve conducting empirical research to test the effectiveness of the current IDS in the detection of intrusion attacks. The systematic literature review identified that researchers used different approaches to determine the applications of machine learning to (IDS). Three major approaches manifested: review of existing literature, the development of new IDS models, and evaluation of their effectiveness in intrusion detection.

In this regard, 9 articles were surveys to determine how previous research has demonstrated the application of machine learning in IDS. 13 articles involved empirical studies to determine the effectiveness of specific machine learning techniques to detect intrusive threats. From the research survey articles, 5 of them had a sample size of above 50 while the rest had a sample size of below 50. Of all of the empirical research studies, 13 contained findings applying machine learning techniques to traditional intrusion detection systems significantly improved detection capabilities. In essence, research showed that machine learning methods can be very effective in detecting and blocking intrusions into information systems.

5. Conclusion

This paper provides a comprehensive analysis of available literature on intrusion detection systems based on the Mac hine learning techniques. It updates researchers already researching on the topic and more so those that are about to start. Updates include knowledge on available literature, areas relating to the topic that have been researched and subsequently published, and trends. In general, conducting this task helped to identify a large pool of scholarly publications on Scopus and IEEE Explore databases. The most relevant publications related to the topic were arrived at after a thorough review of articles initially identified. After conducting the task it's clear that there is very vibrant research on the use of Machine Learning in Intrusion Detection Systems.

Acknowledgments

We thank the University of Tabuk for providing research support and facilities. We would like to thank all the reference authors of whom their input made this article a reality.

References

[1] M. Wu and Y. B. Moon, "Intrusion Detection System for Cyber Manufacturing System," J. Manuf. Sci. Eng., vol. 141, no. 3, p. 031007, Jan. 2019.

[2] Hoque MS, Mukit M, Bikas M, Naser A," An implementation of intrusion detection system using genetic algorithm;" 2012. arXiv preprint arXiv:1204.1336.

[3] Prasad R, Rohokale V. "Artificial intelligence and machine learning in cyber security. Cyber Security: The Lifeline of Information and Communication Technology". New York, NY: Springer; 2020:231-247.

[4] Najafabadi MM, Villanustre F, Khoshgoftaar TM, Seliya N, Wald R, Muharemagic E. Deep learning applications and challenges in big data analytics. J Big Data. 2015;2(1):1. https://doi.org/10.1186/s40537-014-0007-7.

[5] Amouri, Amar, Vishwa T. Alaparthy, and Salvatore D. Morgera. "A machine learning based intrusion detection system for mobile Internet of Things." Sensors 20, no. 2 pp 461, 2020.

[6] Alrowaily, Mohammed, Freeh Alenezi, and Zhuo Lu. "Effectiveness of machine learning based intrusion detection systems." In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, pp. 277-288. Springer, Cham, 2019.

[7] Alqahtani, Hamed, Iqbal H. Sarker, Asra Kalim, Syed Md Minhaz Hossain, Sheikh Ikhlaq, and Sohrab Hossain. "Cyber Intrusion Detection Using Machine Learning Classification Techniques." In International Conference on Computing Science, Communication and Security, pp. 121-131. Springer, Singapore, 2020.

[8] Belouch, Mustapha, Salah El Hadaj, and Mohamed Idhammad. "Performance evaluation of intrusion detection based on machine learning using Apache Spark." Procedia Computer Science 127, pp 1-6, 2019.

[9] Biswas, Saroj Kr. "Intrusion detection using machine learning: A comparison study." International Journal of pure and applied mathematics 118, no. 19, pp 101-114, 2019.

[10] Çavuşoğlu, Ünal. "A new hybrid approach for intrusion detection using machine learning methods." Applied Intelligence 49, no. 7, pp 2735-2761, 2019.

[11] Ever, Yoney Kirsal, Boran Sekeroglu, and Kamil Dimililer. "Classification analysis of intrusion detection on NSL-KDD using machine learning algorithms." In International Conference on Mobile Web and Intelligent Information Systems, pp. 111-122. Springer, Cham, 2019.

[12] Liu, Hongyu, and Bo Lang. "Machine learning and deep learning methods for intrusion detection systems: A survey." applied sciences 9, no. 20, pp 4396, 2019.

[12] Kilincer, Ilhan Firat, Fatih Ertam, and Abdulkadir Sengur. "Machine learning methods for cyber security intrusion detection: Datasets and comparative study." Computer Networks 1,pp 188-198, 2021.

[13] Kumar, Gulshan, Kutub Thakur, and Maruthi Rohit Ayyagari. "MLEsIDSs: machine learning-based ensembles for intrusion detection systems—a review." The Journal of Supercomputing, pp 1-34, 2020.

[14] Magán-Carrión, Roberto, Daniel Urda, Ignacio Díaz-Cano, and Bernabé Dorronsoro. "Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches." Applied Sciences 10, no. 5, pp 1775, 2020.

[15] Maseer, Ziadoon Kamil, Robiah Yusof, Nazrulazhar Bahaman, Salama A. Mostafa, and Cik Feresa Mohd Foozy. "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset." IEEE Access 9, pp 50-70, 2021.

[16] Mishrati, Vijay Varadharajan, Uday Tupakula, and Emmanuel S. Pilli. "A detailed investigation and analysis of using machine learning techniques for intrusion detection." IEEE Communications Surveys & Tutorials 21, no. 1, pp 686-728, 2019.

[17] Othman, Suad Mohammed, Fadl Mutaher Ba-Alwi, Nabeel T. Alsohybe, and Amal Y. Al-Hashida. "Intrusion detection model using machine learning algorithm on Big Data environment." Journal of Big Data 5, no. 1, pp 1-12, 2019.

[18] Pawlicki, Marek, Michał Choraś, and Rafał Kozik. "Defending network intrusion detection systems against adversarial evasion attacks." Future Generation Computer Systems 110, pp 148-154, 2020.

[19] Thakur, Soumyadeep, Anuran Chakraborty, Rajonya De, Neeraj Kumar, and Ram Sarkar. "Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model." Computers & Electrical Engineering 91, pp 44, 2021.

[20] Shah, Syed Ali Raza, and Biju Issac. "Performance comparison of intrusion detection systems and application of machine learning to Snort system." Future Generation Computer Systems 80, pp 157-170, 2019.

[21] Sultana, Nasrin, Naveen Chilamkurti, Wei Peng, and Rabei Alhadad. "Survey on SDN based network intrusion detection system using machine learning approaches." Peer-to-Peer Networking and Applications 12, no. 2, pp 493-501, 2019.

[22] Verma, Abhishek, and Virender Ranga. "Machine learning based intrusion detection systems for IoT applications."

Wireless Personal Communications 111, no. 4, pp 2287-2310, 2020.

[23] Vimala, S., V. Khanaa, and C. Nalini. "A study on supervised machine learning algorithm to improvise intrusion detection systems for mobile ad hoc networks." Cluster Computing 22, no. 2, pp 4065-4074, 2019.

[24] Wang, Yu, Weizhi Meng, Enjoin Li, Zhe Liu, Yang Liu, and Hanxiao Xue. "Adaptive machine learning-based alarm reduction via edge computing for distributed intrusion detection systems." Concurrency and Computation: Practice and Experience 31, no. 19, e5101, 2019.

[25] Wang, Maonan, Kangfeng Zheng, Yanqing Yang, and Xiujuan Wang. "An explainable machine learning framework for intrusion detection systems." IEEE Access 8, pp 27-42, 2020.