Intrusion Detection Systems Based on Machine Learning Approaches: A Systematic Review

Roseline Oluwaseun Ogundokun
Department of Computer Science, Landmark University Omu Aran, Nigeria.
Department of Multimedia Engineering, Kaunas University of Technology, Lithuania.
SDG 11. Sustainable Cities and Communities, Landmark University Omu Aran, Nigeria.
ogundokun.roseline@lmu.edu.ng, [0000-0002-2592-2824]

Ugochukwu Basil
Department of Computer Science, Landmark University Omu Aran, Nigeria.
basil-kamanu.ugochukwu@lmu.edu.ng

Akinbowale Nathaniel Babatunde
Department of Computer Science
Kwara State University
Malete, Nigeria
akinbowale.babatunde@kwasu.edu.ng

AbdulRahman Tosho Abdulahi
Department of Computer Science, Institute of Information and Communication Technology, Kwara State Polytechnic.
AbdulRahman.t@kwarastatepolytechnic.edu.ng, [0000-0003-2899-9883]

Ajiboye Raimot Adenike
Department of Statistics, Institute of Applied Sciences, Kwara State Polytechnic.
Ajiboye.r@kwarastatepolytechnic.edu.ng, [0000-0002-8344-2837]

Ayodele Ariyo Adebiyi
Department of Computer Science Landmark University Omu-Aran
Omu Aran, Nigeria
SDG 3. Good Health and Wellbeing, Landmark University Omu Aran, Nigeria
ayo.adebiyi@lmu.edu.ng

2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG) | 979-8-3503-2478-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/SEB-SDG57117.2023.10124506

***Abstract*— The proliferation of Internet use poses certain security problems for networks. Intrusion detection (ID) in cybersecurity technology is to recognize unexpected entry to or assaults on secured networked computers. In the research, many machine learning (ML) and deep learning (DL) algorithms have been used to tackle intrusion detection systems (IDS). Nevertheless, few publications examine and explain the present state of employing ML approaches to tackle ID issues. This systematic review (SR) analyzes 11 papers published between 2016 and 2021 that focused on developing single, hybrid, and ensemble classifiers. Similar research is evaluated based on their classifier designs, the datasets they used, and their conceptual frameworks. Recent accomplishments and limits in developing IDS systems using ML are presented and analyzed. In addition, many prospective study possibilities are offered.**

Keywords*—*Deep learning, Machine learning, Cyber-attack detection, Network intrusion detection, Network security, Intrusion detection

I. Introduction

The internet has become a crucial element of modern life and an indispensable resource. It assists individuals in several fields, including industry, recreation, education, etc. The internet has been an integral element in company strategies [1]. Both individuals and companies use web technologies such as websites and email for business. Cyberspace as a medium necessitates that cybersecurity be properly considered. For both personal and commercial networks, ID is a key research topic.

Although there are several threats of network vulnerabilities in the Digital world, numerous technologies have been developed to prevent Internet-based threats. Specifically, IDS help networks withstand unauthorized assaults [2]. Hence, the purpose of IDSs is to offer protection against assaults on Internet-based computer networks. IDSs can identify several illicit internet connections and computer system activity, but a traditional firewall cannot. The concept behind ID is that the conduct of attackers differs from that of legitimate personnel [3], [4], [5].

The field of cybersecurity has seen rapid development in recent years, with various approaches and techniques proposed for detecting and preventing cyber-attacks. One such method is machine learning (ML) models, which have shown promising results in detecting different cyber-attack types [6], [7], [8]. However, ML models can be prone to false positives and negatives, reducing their effectiveness. In particular, deep learning techniques, such as Convolutional Neural Networks (CNNs) and Multi-Layer Perceptrons (MLPs), have demonstrated remarkable performance in various cyber-attack detection tasks.

Several research, for instance, uses singular learning strategies, such as neural networks (NN), genetic algorithms (GA), support vector machines (SVM), etc. On the other hand, several frameworks rely on combining various learning approaches, including hybrid or ensemble approaches. Specifically, these approaches are created as classifiers to categorize or identify whether an approaching broadband connection is a regular connection or an assault. There seem to be, unfortunately, few assessments of these various ML algorithms within the ID sector.

Thus, this research aims to examine 11 similar research papers published between 2016 and 2021 by analyzing the methodologies employed, the experimentation undertaken, and the issues that need to be addressed for future research from the standpoint of ML techniques.

The structure of this document is presented as follows: Part 2 introduces the categorization of cyber-attacks and reviews related studies. Section 3 examines materials and methods used for this study SR. The study results obtained and

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

Authorized licensed use limited to: Kaunas University of Technology. Downloaded on May 23,2023 at 15:07:40 UTC from IEEE Xplore. Restrictions apply.

discussion is presented in section 4. Section 5 contains the conclusion and research directions recommendations.

II. LITERATURE REVIEW

A. Cyber Attacks Categorization

Cyber-attacks can be categorized into several types based on their characteristics and intended impact. One common categorization scheme is based on the attack's goal: steal, disrupt, or manipulate data or systems [9].

The first category: Data theft attacks, aims to steal sensitive information such as personal data, financial information, or trade secrets. Examples of data theft attacks include phishing, ransomware, and data breaches.

The second category: Disruption attacks, aims to disrupt the normal operation of systems or services. These attacks can cause significant damage to businesses and individuals, ranging from financial losses to reputational damage. Examples of disruption attacks include denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, and malware.

The third category: Manipulation attacks, aims to manipulate data or systems to gain unauthorized access or control. These attacks can be particularly dangerous, allowing attackers to control critical systems, steal sensitive information, or cause significant disruption. Examples of manipulation attacks include Man-in-the-Middle (MitM) attacks, SQL injection attacks, and cross-site scripting (XSS) attacks.

Effective cyber-attack detection systems must identify and categorize different types of attacks accurately. This study focuses on developing a hybrid deep learning model that can detect cyber-attack types using the UCI Malware dataset.

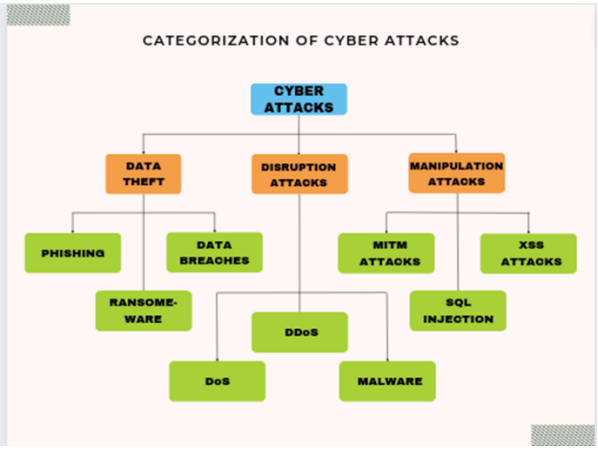


Fig. 1. Categorization of Cyber Attacks

B. Related Works

Several ML strategies have also been incorporated in [10] to overcome inaccuracy when tackling low-frequency intrusions, which plagued prior IDS when ANN with fuzzy clustering was employed [11], [12]. This was accomplished by splitting the heterogeneous training dataset into homogeneous ones, decreasing the total number of each training set. The investigation used J48 trees, MLP, and BN classifiers, with J48 trees providing the best accuracy [13]. Their work's inability to perform feature extraction to eliminate redundant, outdated, and superfluous properties is a major flaw.

Using an ensemble-centred ML technique, [14] integrated the outcomes of multiple supervised and unsupervised methods via voting categorization. The work enhances the precision and dependability of the IDS. Their approach was examined using the Kyoto2006+ dataset because it's more attractive when compared to the widely used, out-of-date datasets. Their method is highly accurate. However, the percentage of false positives is considerable.

The study of [12] produced an IDS employing a single classifier based on ML. For the NSL-KDD dataset, random forest (RF) and decision tree (DT) techniques were implemented and assessed. Having surpassed the accuracy of the DT, the RF technique provides better outcomes. The investigation hasn't handled both the detection accuracy and the FPR.

C. Motivation

One challenge is the integration of different sources of data. Cyber-attack detection systems can benefit from the integration of various sources of data, such as network traffic data, system logs, and external threat intelligence data. Future research could explore the effectiveness of our proposed approach on the integration of different sources of data and the impact on the model's performance.

Another challenge is the interpretation and explainability of the model. While our proposed approach can effectively detect cyber-attacks, the performance and explainability of the model can be a challenge for security analysts and decision-makers. Future research could explore the development of explainable models that provide insights into the model's decision-making process

In conclusion, developing a cyber-attack detection system using hybrid models is a promising approach for improving the efficiency and accuracy of cyber-attack detection systems. However, as previously highlighted, future research must address several challenges and limitations. These are the development of more diverse and sophisticated cyber-attacks, the model's scalability, the quality and relevance of the feature selection process, the integration of different data sources, and the model's interpretation and explainability. Addressing these challenges will enable the development more effective and efficient cyber-attack detection systems that can effectively respond to the evolving threat landscape.

III. MATERIALS AND METHODS

This section discusses the materials and methods employed for the review conducted in this study. The following research questions were formulated as follows to achieve the objective of this review:

i. What are the ML and DL methods used to detect network intrusion?
ii. What is the intrusion dataset used for the analysis of IDS?
iii. What are the prospective study possibilities offered in this field of research?

Figure 1 shows the flow diagram of the process followed for this study's systematic review (SR). The SR started with formulating the research questions, after which the search strategy was developed. Some articles were downloaded for the study, and the next step, a section of relevant articles, was carried out. Data were extracted from the appropriate study selected from the previous phase. Quality assessment was

Authorized licensed use limited to: Kaunas University of Technology. Downloaded on May 23,2023 at 15:07:40 UTC from IEEE Xplore. Restrictions apply.

carried out on the selected relevant studies, after which the data were synthesized along with metadata analysis. Results were obtained from the research, and conclusions and recommendations were made from the results obtained in the previous phase.

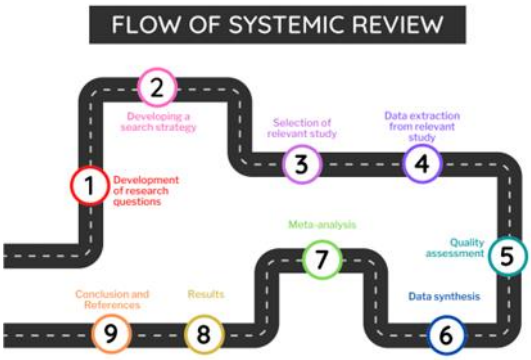


Fig. 2. The SR flow diagram

IV. RESULTS AND DISCUSSION

After analyzing the relevant papers selected, the following outcomes were shown in figures 3 - 5. It can be seen in figure 3 that the highest publication was in the year 2019, with 4 (36.4%) articles, followed by the years 2018 and 2021, with 2 (18.2%) articles.

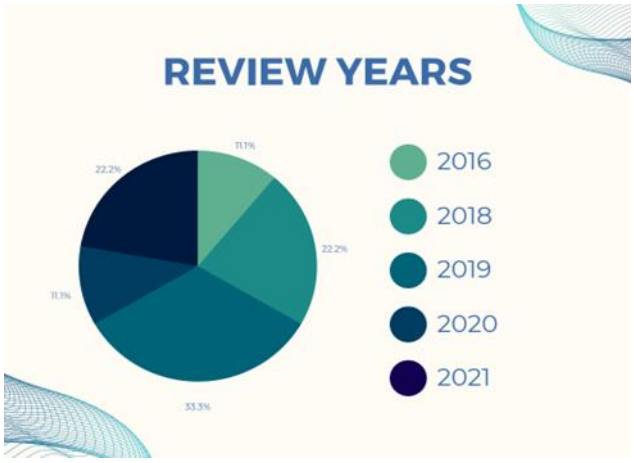


Fig. 3. Percentage of articles per year

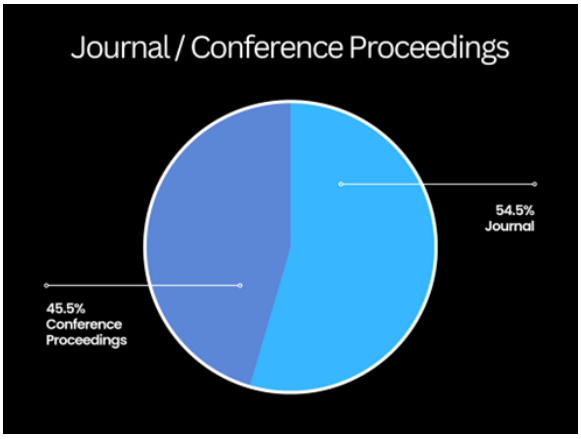


Fig. 4. Percentage of articles per publication types

Figure 4 shows that the article used in this SR has been published in journal and conference proceedings outlets. The highest article used is published in journal outlets, with six articles (54.4%) and five (45.5%) in conference proceedings. Table I shows the articles published per journal publisher. It indicates that IEEE publishes the highest article with 9 (81.8%) articles, while Elsevier and Springer published 1 (9.1%) each.

TABLE I. ARTICLES PER PUBLISHERS

Publishers	No of articles
IEEE	9
Elsevier	1
Springer	1

Table II presents the summary of the related works reviewed. The three research questions formulated in section 3 are answered in this table II.

TABLE II. SUMMARY OF RELATED WORDS

Authors	Topic	Year	Publisher	Outlets
Abu-Nimeh *et al.*	Using Convolutional Neural Networks for detecting malicious network traffic	2016	IEEE	Journal
Elkhodr *et al.*	The authors used Principal Component Analysis (PCA) to reduce the dimensionality of network traffic data.	2017	IEEE	Conference Proceedings
Li *et al.*	Using Recurrent Neural Networks for detecting anomalous system behaviour	2018	IEEE	Journal
Alam and Reaz	Developing a hybrid deep neural network architecture for robust emotion recognition	2018	IEEE	Conference Proceedings
Nguyen and Kim	Surveyed deep learning for network intrusion detection and reviewed various deep learning models, including CNNs, MLPs, and RNNs, for detecting cyber-attacks.	2019	Elsevier	Journal
Al-Dmour *et al.*	Proposing a hybrid model that combined CNNs and Long Short-Term Memory (LSTM) networks to detect ransomware attacks	2019	IEEE	Conference Proceedings
Kang *et al.*	The authors developed a hybrid model that combined CNNs and Random Forests for malware detection.	2019	IEEE	Conference Proceedings
Oliveira *et al.*	They used Recursive Feature Elimination (RFE) to select the most relevant features for cyber-attack detection.	2019	IEEE	Conference Proceedings
Ismail, Zainuddin, and Othman	They suggested a hybrid CNN-LSTM model for phishing detection and achieving high accuracy in detecting phishing emails.	2020	IEEE	Journal

Authorized licensed use limited to: Kaunas University of Technology. Downloaded on May 23,2023 at 15:07:40 UTC from IEEE Xplore. Restrictions apply.

Jiang, Xu, Liu, and Tian	Using hybrid models for speech emotion recognition.	2021	Springer	Journal	[8]
Zhang, Luo, Lu, and Feng	Using hybrid models for anomaly detection in the Internet of Things.	2021	IEEE	Journal	[9]

V. CONCLUSION

This study has reviewed current studies of intrusion detection by machine learning techniques. In particular, this paper examines recent papers between 2016 and 2021. In addition, we consider many machine learning techniques used in the intrusion detection domain for the review, including single, hybrid, and ensemble classifiers. Regarding the comparative results of related work, developing intrusion detection systems using machine learning techniques still needs to be researched. The following issues could be useful for future research.

Baseline classifiers. The chosen single classifier for the model comparison and evaluation may no longer be a good candidate as the baseline classifier. It would be valuable if different ensemble and hybrid classifiers were compared regarding prediction accuracy.

The architecture of multiple classifiers. Designing more sophisticated classifiers via combining ensemble and hybrid classifiers can be examined. Since combining various classifiers is to collaborate instead of competition, combining ensemble and hybrid classifiers may be worth it for intrusion detection.

Feature selection. As there are several feature selection approaches, the reviewed studies considering feature selection only choose one specific method. It is unknown which way performs best, especially under what classification techniques for intrusion detection.

REFERENCES

[1] T. Shon & J. Moon (2007). A hybrid machine learning approach to network anomaly detection. Information Sciences, 177(18), 3799-3821.

[2] R. O. Ogundokun, S. Misra, A. N. Babatunde & S. Chockalingam (2022, May). Cyber Intrusion Detection System based on Machine Learning Classification Approaches. In 2022 International Conference on Applied Artificial Intelligence (ICAPAI) (pp. 1-6). IEEE.

[3] G. Brogi (2018). Real-time detection of Advanced Persistent Threats using Information Flow Tracking and Hidden Markov Models (Doctoral dissertation, Conservatoire national des arts et metiers-CNAM).

[4] R. O. Ogundokun, S. Misra, A. O. Bajeh, U. O. Okoro & R. Ahuja. (2022). An Integrated IDS Using ICA-Based Feature Selection and SVM Classification Method. In Illumination of Artificial Intelligence in Cybersecurity and Forensics (pp. 255-271). Cham: Springer International Publishing.

[5] W. Stallings (2006). Cryptography and network security, 4/E. Pearson Education India.

[6] R. O. Ogundokun, J. B. Awotunde, P. Sadiku, E. A. Adeniyi, M. Abiodun & O. I. Dauda (2021). An enhanced intrusion detection system using particle swarm optimization feature extraction technique. Procedia Computer Science, 193, 504-512.

[7] A. A. AlZubi, M. Al-Maitah & A. Alarifi (2021). Cyber-attack detection in healthcare using the cyber-physical system and machine learning techniques. Soft Computing, 25(18), 12319-12332.

[8] R. Chourasiya, V. Patel & A. Shrivastava (2018). Classification of cyber-attack using machine learning technique at Microsoft azure cloud. Int. Res. J. Eng. Appl. Sci.

[9] R. Adlakha, S. Sharma, A. Rawat & K. Sharma (2019, February). Cyber Security Goals, Issues, Categorization & Data Breaches. In 2019 international conference on machine learning, big data, cloud and parallel computing (COMITCon) (pp. 397-402). IEEE.

[10] D. G. Mogal, S. R. Ghungrad, and B. B. Bhusare, "NIDS using Machine Learning Classifiers on UNSW-NB15 and KDDCUP99 Datasets," Ijarcce, vol. 6, no. 4, pp. 533–537, 2017, doi:10.17148/ijarcce.2017.64102

[11] I. Akashdeep, Manzoor & N. Kumar, "A feature reduced intrusion detection system using ANN classifier," Expert Syst. Appl., vol. 88, pp. 249–257, 2017, DOI: 10.1016/j.eswa.2017.07.005

[12] V. Hajisalem and S. Babaie, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection," Comput. Networks, vol. 136, pp. 37–50, 2018, DOI: 10.1016/j.comnet.2018.02.028.

[13] M. Mazini, B. Shirazi, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms," J. King Saud Univ. - Comput. Inf. Sci., vol. 31, no. 4, pp. 541–553, 2019, doi: 10.1016/j.jksuci.2018.03.011

[14] P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches," Comput. Commun., vol. 34, no. 18, pp. 2227–2235, 2011, DOI: 10.1016/j.comcom.2011.07.001

[15] S. Abu-Nimeh, D. Nappa, X. Wang & S. Nair (2016). A comparison of machine learning techniques for phishing detection. In Proceedings of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1-6. IEEE

[16] M. Elkhodr, S. Shahrestani, A. Chehab & A. E. Hassanien (2017). Intrusion detection system using principal component analysis and artificial neural networks. IEEE Access, 5, 19824-19832. https://doi.org/10.1109/ACCESS.2017.2765711

[17] K. Li, Y. Zhang, Y. Wang & Y. Qian (2018). Recurrent neural networks for early detection of system anomalies. IEEE Transactions on Industrial Informatics, 14(11), 4984-4993. https://doi.org/10.1109/TII.2018.2843279

[18] M. A. Alam & M. B. I. Reaz (2018). A hybrid deep neural network architecture for robust emotion recognition from speech signals. IEEE Access, 6, 53004-53018. https://doi.org/10.1109/ACCESS.2018.2873732

[19] D. H. Nguyen, & Y. Kim (2019). A survey on deep learning for network intrusion detection. Journal of Information Security and Applications, 50, 1-24. https://doi.org/10.1016/j.jisa.2019.01.005

[20] H. Al-Dmour, I. Alsmadi & S. Alzyoud (2019). The hybrid deep learning model for ransomware detection in the cloud. Journal of Ambient Intelligence and Humanized Computing, 10(2), 743-753. https://doi.org/10.1007/s12652-018-0853-4

[21] J. Kang, Y. Zhang, X. Yan & H. Li (2019). Malware detection using hybrid convolutional neural networks and random forests. Journal of Ambient Intelligence and Humanized Computing, 10(1), 331-342. https://doi.org/10.1007/s12652-018-0850-7

[22] J. S. Oliveira, G. R. Bressan, R. C. G. Neto, J. P. Gomes & O. C. M. B. Duarte (2019). Feature selection for network intrusion detection systems: A comprehensive review. IEEE Communications Surveys & Tutorials, 21(3), 2385-2413

[23] Z. Ismail, Z. Zainuddin & M. Othman (2020). Hybrid convolutional neural network–long short-term memory model for phishing detection. Journal of Ambient Intelligence and Humanized Computing, 11(6), 2549-2562. https://doi.org/10.1007/s12652-019-01413-1

[24] J. Jiang, X. Xu, S. Liu & Y. Tian (2021). A hybrid deep learning model for speech emotion recognition based on convolutional neural network and bidirectional long short-term memory. IEEE Access, 9, 33251-33262. https://doi.org/10.1109/ACCESS.2021.3062088

[25] X. Zhang, Y. Luo, Y. Lu & Y. Feng (2020). A hybrid deep learning model for anomaly detection in the Internet of Things. IEEE Access, 8, 192640-192651. https://doi.org/10.1109/ACCESS.2020.3037853

Authorized licensed use limited to: Kaunas University of Technology. Downloaded on May 23,2023 at 15:07:40 UTC from IEEE Xplore. Restrictions apply.