Babylonian Journal of Internet of Things
Vol.2024, **pp**. 79–86
DOI: https://doi.org/10.58496/BJIoT/2024/010; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

CNN- based intrusion detection software for network operating system environment

Sundos A. Hameed Alazawi [1,*], Huda Abdulaali Abdulbaqi [1], Ahmed Hussein Ali [2]

[1] *Computer Science Dep., Mustansiriyah Unevirsity, 10052 , Baghdad, Iraq.*

[2] *College of Education, Aliraqia University, Baghdad, Iraq*.

A R T I C L E I N F O

Article History

Received 01 Jun 2024
Accepted 10 Jul 2024
Published 02 Aug 2024

Keywords

Digital Technology

IOT

Cybersecurity

CNN

intrusion detection software

vital importance

A B S T R A C T

Cybersecurity represents an important challenge specific to digital technology in the modern world, and is of vital importance for reducing or even preventing the impact of cybercrime. The Linux operating system is designed as open-source software that includes some features of software tools intended for network security and cybersecurity systems, such as intruder detection and penetration testing. With these tools in Linux, we need a special system to constantly detect intrusions into connected network devices. This research presents a method for detecting intrusion attacks based on analyzing the natural behavior of the system by building a special convolutional network to achieve this goal. The classification and detection results of the proposed convolutional neural network were compared with the regular machine learning method (SVM), with feature selection by correlation for both methods. Same datasets were used to train and test each of CNN and SVM. Some metrics were determined to evaluate the performance of classification and prediction models for a specific type of regular attacks, DoS and BOT attacks, where both SVM and CNN obtained an accuracy of 85.58% and 95.59%, respectively.

1. INTRODUCTION

One of the most important systems that identify malicious activities are intrusion detection systems and network traffic classification. The most important network identifiers are the server and host, which allow the transmission of data and packets in the network. This process is managed by the network operating system on the server side. These packets transmitted over the network may contain malicious activity that may be ineffective if the packets are isolated or have a harmful effect on the network if they are not isolated and target network servers [1, 2].

The primary objective of cybersecurity is to reduce risks and ensure safety and privacy within network environments [4,3]. To achieve this, cybersecurity experts and professionals collaborate extensively, creating a wide array of defense systems and tools aimed at protecting the core pillars of information security: confidentiality, integrity, and availability (often referred to as the CIA triad) [5].

Intrusion Detection Systems (IDSs) play a crucial role in this landscape and can be broadly classified into three categories: signature-based IDSs, anomaly-based IDSs, and hybrid IDSs [6]. Signature-based IDSs are designed to identify known attacks by recognizing patterns or signatures that have already been documented. While these systems are highly effective at detecting familiar threats, they fall short when it comes to identifying new or zero-day attacks, as these threats lack predefined signatures [7].

In contrast, anomaly-based IDSs excel at spotting zero-day attacks by identifying behaviors that deviate from established normal activities [8,9].However, their effectiveness in detecting known attacks is generally lower compared to signature-based systems. To address the limitations of both approaches, hybrid IDSs have been developed. These systems combine the strengths of both signature-based and anomaly-based methods, enabling them to detect both known and unknown threats [10]

In the field of artificial intelligence, the need to rely on this technology has accelerated in many areas, including the neural network and machine learning, and its use in examining the network and communication devices in the computer and

*Corresponding author. Email: ss.aa.cs@uomustansiriyah.edu.iq

detecting defects in them. Hence, a network sequence detection system was adopted using machine learning and neural network methodologies, which is important in the field of intrusion detection systems [11, 12].
Machine Learning (ML) techniques have recently emerged as promising solutions for the development of Intrusion Detection Systems (IDSs). ML involves a set of methods that use mathematical models to automatically identify, analyze, and extract patterns from data. By uncovering meaningful information, these models can make informed decisions and predictions. ML [13,14] algorithms are generally divided into two categories: supervised and unsupervised learning [15]. Supervised learning algorithms rely on labeled data to map input variables to a specific target variable. Examples of these algorithms include K-Nearest Neighbors (KNN), Decision Tree (DT) models, and Deep Learning (DL) techniques, among others[16], etc.
Some Linux operating systems are among the most important systems designed in the field of cybersecurity in terms of the tools and distributions attached to them, such as intruder detection systems [17].
But it is important to design and develop a special model based on artificial intelligence algorithms, and not limit the use of special Linux operating systems designed for this purpose[18]. Therefore, we resorted to presenting a proposal to classify and then detect intrusion attacks based on recent data, taking into account the multiple classification of the main known attacks.

1.1 Intrusion detection system

An intrusion detection system (IDS) typically incorporates a network intrusion detection method into an architecture that includes additional related sub-components. This amalgamation forms a functional standalone system capable of conducting the entire spectrum of tasks required for intrusion detection. Throughout the discussion of various intrusion detection categories, several IDSs, along with their architectures and constituents, are presented [19].
The general structure of network intrusion detection is shown in the Figure 1, which includes data processing stages such as coding and pre-processing, then choosing methods that can be used to classify and detect network anomalies, such as machine learning and deep learning methods and algorithms [20, 21].

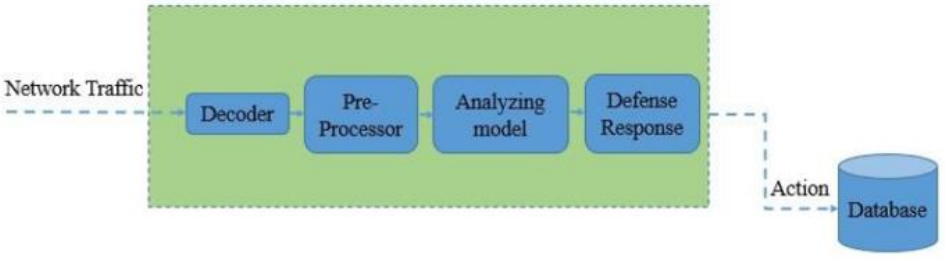

Fig .1. General structure of network intrusion detection

1.2 Types of Intrusion detection systems

Intrusion Detection Systems (IDSs) come in various forms, each with distinct methods and capabilities for detecting suspicious activity. Network Intrusion Detection Systems (NIDS) are strategically placed across the network at key points, where they monitor inbound and outbound traffic for all connected devices. They analyze this traffic, comparing it against known attack signatures, and generate alerts if anomalous activity is detected. [20]Host Intrusion Detection Systems (HIDS) operate on individual hosts and devices within the network, particularly those with internet access. They monitor each host's activities, tracking the status of all files on an endpoint and detecting unusual activities such as file deletions or modifications.
Protocol-based Intrusion Detection Systems (PIDS) are typically deployed on web servers, where they monitor and analyze communications between network devices and external online resources. They scan data transmitted over protocols like HTTP/HTTPS to identify potential threats. Application Protocol-based Intrusion Detection Systems (APIDS) focus on monitoring communication between users and applications. They examine packets transmitted over application-specific protocols, identifying and tracing suspicious instructions back to individual users.

1.3 IDS detection methods

Depending on the type of intrusion detection system the security solution will rely on a few different detection methods. Signature-based intrusion detection system (SIDS) aims to identify patterns and match them with known signs of intrusions [22]. Anomaly-Based Intrusion Detection System (AIDS) can identify these new zero-day intrusions [23]. Anytime traffic deviates from this typical behavior, the system flags it as suspicious. Hybrid Intrusion Detection system can flag new and

existing intrusion strategies [24]. It is defined exactly as its name implies: a combination of two or more types of Intrusion Detection Systems (IDSs). In this hybrid type, the capabilities of multiple systems are integrated to enhance detection and protection[24, 25].

2. RELATED WORKS

Cybersecurity presents a crucial challenge for both current and future generations of networks. While numerous papers have been published on the development of Intrusion Detection Systems (IDS),

Tahri, Rachid, et al 2022 [26] was suggested to use machine learning algorithms SVM and KNN to determine the best accuracy in detecting network intruders in the USNW NB 15 and NSL-KDD data sets, where SVM proved high efficiency and detection accuracy of up to 97.29 for the NSL-KDD dataset, and 97.77 for UNSW-NB15 dataset

Hussein et al. 2021 [27] improve detection rate accuracy for every individual attack types and all types of attacks, which will help us to identify attacks and particular category of attacks. They used datasets are NSL-KDD and UNSW-NB15 in their proposal method. The method is evaluated using k-fold cross validation, and the experimental results of all the three classifiers with and without feature selection are compared together.

Dini, Pierpaolo, and Sergio Saponara 2021 [28] presented a proposal for applying machine learning algorithms to analyze network traffic using the KNN and ANN algorithms based on multiple classification, and used belongs to CSE-CIC-IDS 2018. The authors demonstrated the superiority of KNN, as it obtained an accuracy rate of 0.9957, while the accuracy rate of ANN was lower, reaching 0.9923.

Kanimozhi, V., and T. Prem Jacob 2019 [29] Integrating multiple classification methods KNN, NB, DT, and SVM classifier based on the CSE-CIC dataset - ID 2018. The authors used calibration curve analysis and measurement methods to verify all the proposed classifiers in evaluating their performance. The work proved the superiority of SVM to other classifiers, obtaining an accuracy rate of 0.999

Hooshmand, DA Mohammad Kazim 2019 [30] In the first classification of anomalies, the authors proposed the use of Random Forest. Based on the UNSW-NB15 dataset, the authors also used a neural network to evaluate the proposed system to classify inputs as attacks or not. The evaluation results for the proposed model obtained an accuracy of 0.93.

Hooshmand, Mohammad Kazim [31] 2018 presented a study on feature selection and classification techniques using the UNSW-NB15 dataset. The authors relied on regular machine learning algorithms such as DT, R F, and KNN to detect the attack or not. The highest accuracy value in detecting the attack using Random Forest was about (0.99).

Songma, S., Sathuphan, T., & Pamutha, T 2018 [32] Use the CSE-CIC-IDS 2018 dataset to detect network and sequence anomalies using supervised machine learning algorithms. DT, KNN, and XGBoost machine learning algorithms were evaluated with PCA for each algorithm in the feature selection process. XGBoost obtained the highest accuracy value of approximately 0.997698 when using PCA

Wang et al. 2020 [33], proposes an intrusion detection method based on convolutional neural network. The system is built by several open-source tools, it consists of data preprocessing, neural network training, network testing and intrusion response based on Linux. By experiment the result with NSL-KDD dataset, the proposed IDS-CNN system can not only efficiently detect intrusion of network data flows, but also its detection accuracy is better from the most modern method.

Thirimanne, Sharuka Promodya, et al. 2022 [34], proposed for real-time network intrusion detection, they used 28 features to train a deep neural network that receives encoded data by real-time machine learning pipeline. The author used a data analysis method for the input traffic from the NSL-KDD dataset used to train the DNN. The system obtained an accuracy of 81%, less than the intrusion detection systems used for the same data set, but the important feature in this research is the adoption of real time in the data flow.

Balyan, Amit Kumar, et al. 2022 [35], the authors presented a hybrid network-based intrusion detection system adopting a hybrid optimization algorithm that combines genetic, particle swarm, and random forest methods. they used hybrid optimization methods to enhance secondary data and extract new data with features that work more accurately. The performance of the proposed system was tested with machine learning methods using NSL-KDD standard data sets. The researchers demonstrated that the proposed method achieved an accuracy of up to 98.979 percent on the NSL-KDD data set.

Jahanzaib et al. 2020 [36], presented a paper that introduces a security protection architecture specifically tailored to safeguard the control layer of a software defined network. This platform combines the capabilities of Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) techniques to provide a proficient and effective intrusion detection system (IDS), in this study the Centralized control intelligence in SDNs faces scalability challenges, especially as networks grow in size and complexity.

3. RESEARCH METHODOLOGY

The general structure of the proposed system is shown in the Figure 2, where the system requires performing some necessary procedures on the data set in order to use it in the classification model, such as data pre-processing operations by data normalization and data balancing.
After the pre-processing operations mentioned above, the best features are selected to facilitate the extraction of important features within the CNN network. Classification models were trained on the CSE-CIC-IDS dataset for binary and multi-class types. multi-class was adopted to detect the intrusion type, while binary classification was used to detect whether the type of intrusion was normal or harmful Attack.

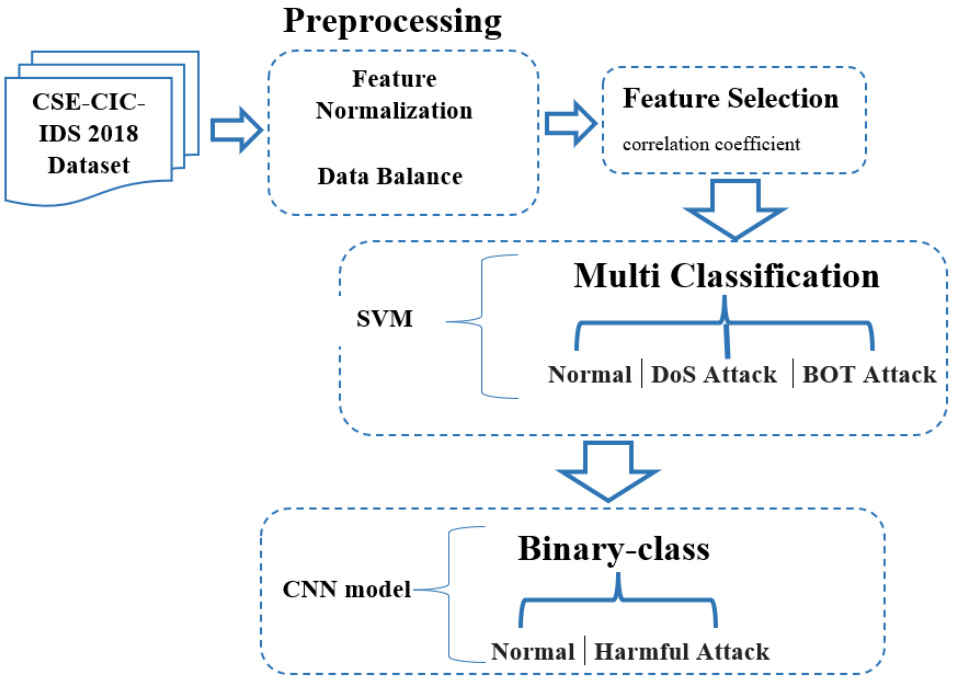

Fig .2. General Structure of Proposed System

3.1 Dataset Balancing

The CSE-CIC-IDS dataset has various distributions that are not equal or skewed. This ranges from a slight to a severe imbalance in terms of balance. This imbalance poses a challenge to the classifier's parameters, as most algorithms assume that the classes are equal in distribution. [37, 38]. Table 1 including the distribution of features for CSE-CIC-IDS dataset in binary classification

TABLE I. ATTACK DISTRIBUTION IN BINARY CLASSIFICATION

CSE-CIC-IDS dataset	
Normal	Attack
83.1 %	16.9 %

Table 2. and Figure 3 including the distribution of features for CSE-CIC-IDS dataset in Multi classification

TABLE II. ATTACK DISTRIBUTION IN MULTI CLASSIFICATION.

CSE-CIC-IDS dataset	
Attack type	Percent
Normal	63.111
DoS Attack	28.497
BOT Attack	6.324
filtration Attack	2.056
Brute Force	0.011
SQL injection	0.001

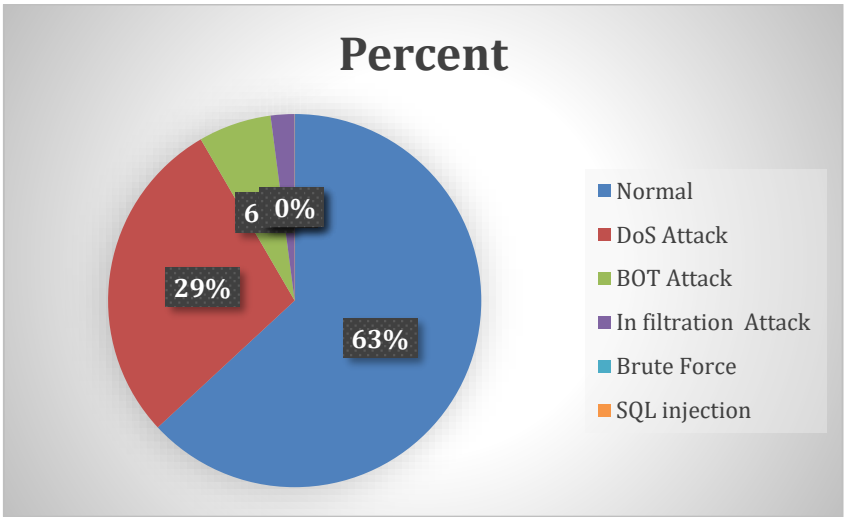

Fig .3. Attacks distribution in Multi classification

Hence, it was important to balance and clean the data sets before entering them into the workbook as part of the pre-processing stage. Equ.1 is used for the calculation of the imbalance ratio [39, 40]:

$$\text{Imbalance Ratio} = \frac{\{max C_i\}}{\{min C_i\}} \quad \ldots\ldots\ldots\ldots\ldots\ldots 1$$

where: CiCi shows the data size in the class i.

3.2 Feature selection

The metric of Pearson's correlation coefficient is utilized for assessing the linear association between the variables. Let a sample with size w, there is w of data are transformed into grade data, a linear correlation level between two variables (correlation coefficient of i and j) is given in Equ.2 [41, 42].

$$Corr_{i,j} = \frac{\sum(i-\bar{i})(j-\bar{j})}{(\sqrt{\sum_1^w (j_k-\bar{j})^2})(\sqrt{\sum_1^w (j_k-\bar{j})^2})} \quad \ldots\ldots\ldots 2$$

3.3 Intrusion detection model

After the data set undergoes the pre-processing stage of normalization and balancing, and then selecting the features - the selected data is concentrated on three main types of attacks as multi-class, namely natural, DoS, and BOT attacks.
For the multi-class approach, the system has two models. The first multi-class intrusion detection method is the SVM algorithm. In binary classification, the CNN includes five layers containing 128, 256, 512, 1024, and 1024 layers. All hidden layers used ReLU activation functions, while the output layer consisted of two neurons with Softmax activation.

4 EXPERIMENTAL AND RESULTS

After perform the balancing operation to the CSE-CIC-IDS 2018 dataset, the number of attack classes decreased from 6 to 3. Some classes have been removed to ensure an equal number for each attack class except normal class. Table 3. and Figure 4 including the distribution of features for CSE-CIC-IDS dataset after Preprocessing operations.

TABLE III. ATTACKS DISTRIBUTION AFTER PREPROCESSING

CSE-CIC-IDS dataset	
Attack type	Percent
Normal	40 %
DoS Attack	30 %
BOT Attack	30 %

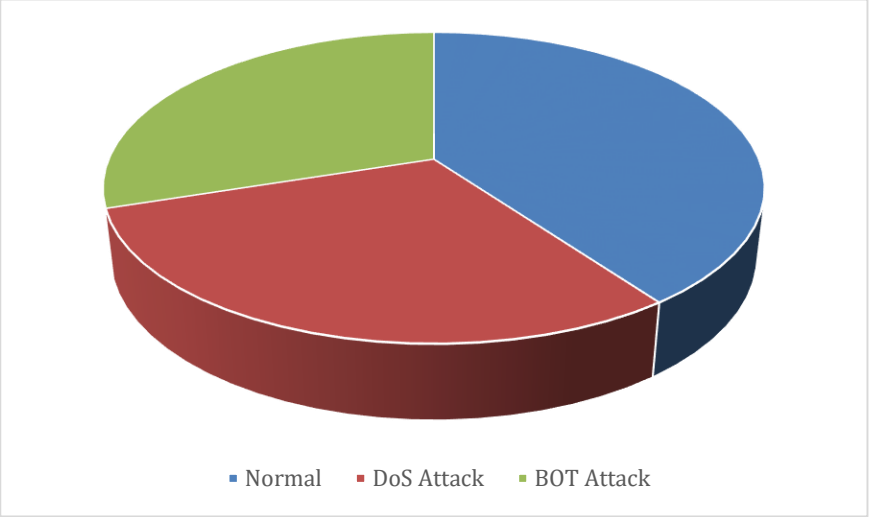

Fig .4. Attacks distribution after Preprocessing for CSE-CIC-IDS dataset

Models are trained to classify all types of attacks identified in the dataset. The performance evaluation of each model is based on the confusion matrix. In this work, some metrics were identified to evaluate the performance of classification and prediction models, such as sensitivity, Specificity, Precision, and Accuracy for identified type of attacks Normal, DoS, and BOT attacks. Table 4. Figure 5 shows the evaluation of the performance of each SVM and CNN in a multiple classification of the intrusion attack-network.

TABLE IV. PERFORMANCE EVALUATION FOR SVM AND CNN MODELS

Model	Sensitivity	*Specificity*	*Precision*	*Accuracy*
SVM	85.57%	97.42%	89.87%	85.58%
CNN	**95.59%**	**99.55%**	**97.30%**	**95.59%**

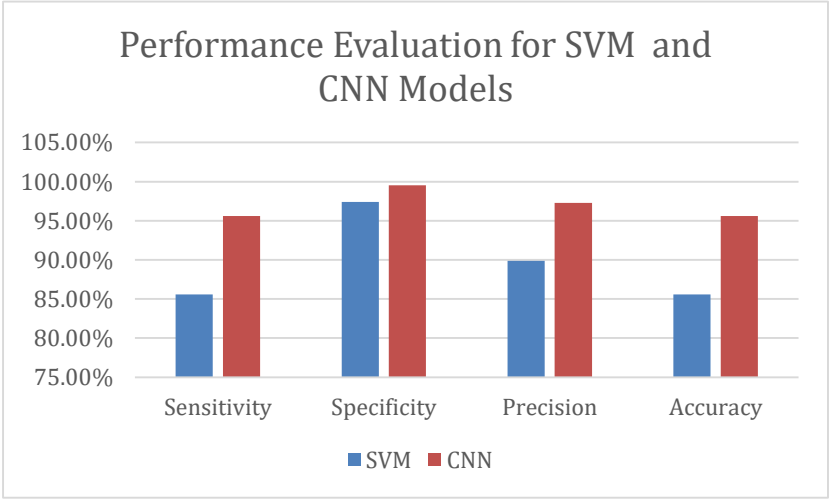

Fig .5. Performance Evaluation for SVM and CNN models

5. CONCLUSION

The work in this paper was based on the recent CSE-CIC IDS2018 multi-classification dataset. Since the collected data may contain a number of spaces and characteristics that affect the accuracy of the classification and its intended purpose, a balancing act was made to reduce the dimensions of the data and three main attacks Normal, DoS, and BOT, were adopted for the work. A convolutional neural network model was designed to classify and detect network anomaly and hacking attacks, comparing the CNN classifier to one of the well-known machine learning algorithms, which is SVM. The proposed CNN classifier proved to have very high accuracy, which led to its selection in the detection stage. Network anomaly of data used

Funding

The author's paper explicitly states that the research project did not receive any funding from institutions or sponsors.

Conflicts Of Interest

The author's paper clearly states that no conflicts of interest exist in relation to the research or its publication.

Acknowledgment

The authors are thankful to the Department of Computer Science, College of Science, Mustansiriyah University (https://uomustansiriyah.edu.iq/e-newsite.php), for supporting this work.

References

[1] G. D. C. Bertoli, L. A. P. Júnior, O. Saotome, A. L. Dos Santos, F. A. N. Verri, C. A. C. Marcondes, S. Barbieri, M. S. Rodrigues, and J. M. P. De Oliveira, “An end-to-end framework for machine learning-based network intrusion detection system,” IEEE Access, vol. 9, pp. 106790-106805, 2021.

[2] M. Ozkan-Okay, R. Samet, Ö. Aslan, and D. Gupta, “A comprehensive systematic literature review on intrusion detection systems,” IEEE Access, vol. 9, pp. 157727-157760, 2021.

[3] M. Lehto, "The ways, means and ends in cyber security strategies." pp. 182-190.

[4] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel, “Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation,” Risk Analysis, vol. 42, no. 8, pp. 1643-1669, 2022.

[5] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, “Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1143-1155, 2017.

[6] S. Einy, C. Oz, and Y. D. Navaei, “The anomaly-and signature-based IDS for network security using hybrid inference systems,” Mathematical Problems in Engineering, vol. 2021, pp. 1-10, 2021.

[7] J. Díaz-Verdejo, J. Muñoz-Calle, A. Estepa Alonso, R. Estepa Alonso, and G. Madinabeitia, “On the detection capabilities of signature-based intrusion detection systems in the context of web attacks,” Applied Sciences, vol. 12, no. 2, pp. 852, 2022.

[8] H. Hindy, R. Atkinson, C. Tachtatzis, J.-N. Colin, E. Bayne, and X. Bellekens, “Utilising deep learning techniques for effective zero-day attack detection,” Electronics, vol. 9, no. 10, pp. 1684, 2020.

[9] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, and M. Nasser, “Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review,” Applied sciences, vol. 11, no. 18, pp. 8383, 2021.

[10] S. Kaur, and M. Singh, “Hybrid intrusion detection and signature generation using deep recurrent neural networks,” Neural Computing and Applications, vol. 32, no. 12, pp. 7859-7877, 2020.

[11] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, “A survey of neural networks usage for intrusion detection systems,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 1, pp. 497-514, 2021.

[12] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, pp. e4150, 2021.

[13] G. Kocher, and G. Kumar, “Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges,” Soft Computing, vol. 25, no. 15, pp. 9731-9763, 2021.

[14] G. Kumar, K. Thakur, and M. R. Ayyagari, “MLEsIDSs: machine learning-based ensembles for intrusion detection systems—a review,” The Journal of Supercomputing, vol. 76, no. 11, pp. 8938-8971, 2020.

[15] P. Shukla, "ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things." pp. 234-240.

[16] A. O. Alzahrani, and M. J. Alenazi, “ML-IDSDN: Machine learning based intrusion detection system for software-defined network,” Concurrency and Computation: Practice and Experience, vol. 35, no. 1, pp. e7438, 2023.

[17] M. A. Ismaili, “Enhancing Cybersecurity: Exploring Effective Ethical Hacking Techniques with Kali Linux,” Research and Applications Towards Mathematics and Computer Science, pp. 135, 2023.

[18] N. S. Priya, S. Meyyappan, K. Balasubramanian, and A. Pruthiev, "Network Attack Detection using Machine Learning." pp. 342-346.

[19] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “Network anomaly detection: methods, systems and tools,” Ieee communications surveys & tutorials, vol. 16, no. 1, pp. 303-336, 2013.
[20] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, “A systematic literature review for network intrusion detection system (IDS),” International journal of information security, vol. 22, no. 5, pp. 1125-1162, 2023.
[21] J. Du, K. Yang, Y. Hu, and L. Jiang, “NIDS-CNNLSTM: Network intrusion detection classification model based on deep learning,” IEEE Access, vol. 11, pp. 24808-24821, 2023.
[22] S. Einy, C. Oz, and Y. D. Navaei, “The anomaly-and signature-based IDS for network security using hybrid inference systems,” Mathematical Problems in Engineering, vol. 2021, no. 1, pp. 6639714, 2021.
[23] S. Jin, J.-G. Chung, and Y. Xu, "Signature-based intrusion detection system (IDS) for in-vehicle CAN bus network." pp. 1-5.
[24] E. M. Maseno, Z. Wang, and H. Xing, “A systematic review on hybrid intrusion detection system,” Security and Communication Networks, vol. 2022, no. 1, pp. 9663052, 2022.
[25] S. Smys, A. Basar, and H. Wang, “Hybrid intrusion detection system for internet of things (IoT),” Journal of ISMAC, vol. 2, no. 04, pp. 190-199, 2020.
[26] R. Tahri, Y. Balouki, A. Jarrar, and A. Lasbahani, "Intrusion detection system using machine learning algorithms." p. 02003.
[27] S. A. Hussein, A. A. Mahmood, and E. O. Oraby, “Network Intrusion Detection System Using Ensemble Learning Approaches,” Technology, vol. 18, pp. 962-974, 2021.
[28] P. Dini, and S. Saponara, “Analysis, design, and comparison of machine-learning techniques for networking intrusion detection,” Designs, vol. 5, no. 1, pp. 9, 2021.
[29] V. Kanimozhi, and T. P. Jacob, “Calibration of various optimized machine learning classifiers in network intrusion detection system on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing,” International Journal of Engineering Applied Sciences and Technology, vol. 4, no. 6, pp. 2455-2143, 2019.
[30] D. M. K. Hooshmand, “Machine learning based network anomaly detection,” Int. J. Recent Technol. Eng, vol. 8, no. 4, pp. 542-548, 2019.
[31] M. K. Hooshmand, “Network Traffic Data Classification Using Machine Learning Algorithms.”
[32] S. Songma, T. Sathuphan, and T. Pamutha, “Optimizing Intrusion Detection Systems in Three Phases on the CSE-CIC-IDS-2018 Dataset,” Computers, vol. 12, no. 12, pp. 245, 2023.
[33] H. Wang, Z. Cao, and B. Hong, “A network intrusion detection system based on convolutional neural network,” Journal of Intelligent & Fuzzy Systems, vol. 38, no. 6, pp. 7623-7637, 2020.
[34] S. P. Thirimanne, L. Jayawardana, L. Yasakethu, P. Liyanaarachchi, and C. Hewage, “Deep neural network based real-time intrusion detection system,” SN Computer Science, vol. 3, no. 2, pp. 145, 2022.
[35] A. K. Balyan, S. Ahuja, U. K. Lilhore, S. K. Sharma, P. Manoharan, A. D. Algarni, H. Elmannai, and K. Raahemifar, “A hybrid intrusion detection model using ega-pso and improved random forest method,” Sensors, vol. 22, no. 16, pp. 5986, 2022.
[36] J. Malik, A. Akhunzada, I. Bibi, M. Imran, A. Musaddiq, and S. W. Kim, “Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in SDN,” IEEE Access, vol. 8, pp. 134695-134706, 2020.
[37] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, “Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity,” Applied Sciences, vol. 13, no. 13, pp. 7507, 2023.
[38] R. S. ARSLAN, “FastTrafficAnalyzer: An efficient method for intrusion detection systems to analyze network traffic,” Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, vol. 12, no. 4, pp. 565-572, 2021.
[39] F. Thabtah, S. Hammoud, F. Kamalov, and A. Gonsalves, “Data imbalance in classification: Experimental evaluation,” Information Sciences, vol. 513, pp. 429-441, 2020.
[40] D. Ramyachitra, and P. Manikandan, “Imbalanced dataset classification and solutions: a review,” International Journal of Computing and Business Research (IJCBR), vol. 5, no. 4, pp. 1-29, 2014.
[41] P. Chen, F. Li, and C. Wu, "Research on intrusion detection method based on Pearson correlation coefficient feature selection algorithm." p. 012054.
[42] Y. Fan, J. Liu, J. Tang, P. Liu, Y. Lin, and Y. Du, “Learning correlation information for multi-label feature selection,” Pattern Recognition, vol. 145, pp. 109899, 2024.