Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Machine Learning Approach for Network Cyber Intrusion Detection

Osamah Adil Raheem

University of Wasit, Wasit, Kut 52001, Iraq.Email:oalmusawi@uowasit.edu.iq

ARTICLE INFO

Article history:
Received: 3 /1/2025
Rrevised form: 21 /1/2025
Accepted : 4 /2/2025
Available online: 30 /3/2025

Keywords:

Machine learning,

Cybersecurity ,

Network intrusion detection,
KDD'99 cup database GNB classifier

ABSTRACT

Nowadays, everyone is interconnected through the Internet for exchanging digital information. This information is stored using cloud technology. However, the rapid growth of cloud technology has led to an accumulation of the volume of digital data, as well as network intrusions. Consequently, protecting this data has become crucial for various reasons. Therefore, this study presented a method for detecting network cyber intrusions. The instances of network cyber intrusions were gathered from the KDD'99 Cup database. Furthermore, the proposed method employed the Gaussian Naïve Bayes (GNB) approach to identify instances of cyberattacks. The proposed method utilized various measurements for the purpose of generally assessing the performance of the GNB classifier. The experimental results have been demonstrated that the proposed GNB classifier has achieved 94.28% accuracy in the detection of network attacks. In addition, the GNB has achieved 98.32% precision, 94.28% sensitivity, and 95.89% F-measure. The proposed GNB algorithm demonstrated its efficiency in detecting network attacks, outperforming its counterparts in terms of detection accuracy.

MSC..

https://doi.org/10.29304/jqcsm.2025.17.11966

1. Introduction

In the last decades, there has been a high concern regarding cybersecurity and defending against various cyber threats [1]. This heightened attention is primarily due to the significant expansion of computer networks and the extensive array of applications utilized by individuals or groups, both for personal and commercial purposes, particularly following the widespread adoption of the Internet of Things (IoT) [2]. Cyberattacks inflict significant harm and result in substantial financial losses within extensive network infrastructures. These attacks can disrupt operations, compromise sensitive data, and incur considerable expenses for remediation efforts, including system repairs, legal fees, and damage control measures [3]. Additionally, they often lead to diminished consumer trust, tarnished reputation, and potential legal liabilities, amplifying the overall impact on affected organizations [4]. The current solutions, such as hardware and software firewalls, user authentication measures, and data encryption techniques, are not sufficient to address the escalating demands posed by emerging threats, rendering computer networks vulnerable to various cyber risks. These traditional security measures demonstrated inadequate in safeguarding against the rapidly evolving intrusion systems [5]. While firewalls regulate access between networks,

∗Corresponding author

Email addresses:

Communicated by 'sub etitor'

they lack the capability to detect internal attacks, leaving networks susceptible to breaches [6]. Hence, there's a critical need to develop more advanced defense mechanisms, such as machine learning techniques for Intrusion Detection Systems (IDS), to bolster system security and effectively combat modern cyber threats.

Generally, the IDS is a software or system designed to detect malicious activities and policy violations within a network or system. It works by identifying anomalies and aberrant behavior during routine network operations, aiming to uncover potential security risks or attacks, such as denial-of-service (DoS) incidents. Moreover, the IDS assists in pinpointing, assessing, and managing unauthorized activities within the system, including unauthorized access, modifications, or tampering [7]. To build computational techniques for recognizing diverse cyber threats, it is essential to analyze distinct incident patterns and forecast potential dangers using cybersecurity data. This approach is termed as a data-driven intelligent IDS. Constructing such a system necessitates expertise in artificial intelligence, specifically machine learning methods.

The methods of machine learning were applied in various applications and obtained sufficient results in the detection and classification parts [8]. For instance, cellular network [9], voice pathology detection [10], emotion recognition [11], license plate identification [12, intrusion detection [13], COVID-19 detection [14], and language identification [16]. Additionally, these methods have been used in the IDS for the detection of network attacks [15]. However, there are some works that yet suffer from low accuracy detection rates in the detection of cyber-attacks. Moreover, most existing works ignored to evaluate their works in terms of other performance metrics such as precision, G-mean, specificity, and F-measure (i.e., F1-score). Therefore, the main aims of this work are listed as follows:

- • This work proposes the Gaussian Naïve Bayes (GNB) approach for the detection of cyber network attacks.
- • The GNB classifier is trained and tested based on the KDD'99 cup database, which is considered the most popular database that has been used widely in the detection of network attacks.
- • The performance of the proposed GNB approach is assessed through many evaluation measurements which are accuracy, precision, sensitivity (i.e., recall), F-measure (i.e., F1-score), specificity, and G-mean.
- • The proposed model is able to achieve high experimental results for the detection of cyber network attacks.

The rest of this paper is organized as follows: Section 2 provides the previous studies that were presented in the detection of network attacks. Section 3 presents the proposed method, where this Section includes the database and the classification technique used for the detection of network attacks. Section 4 presents and discusses the experimental outcomes that achieved by the proposed classifier. Section 5 concludes this paper.

2. Previous studies

The detection of network attacks using machine learning has garnered significant attention in recent years due to its potential to enhance cybersecurity measures. Numerous studies have explored various approaches and methodologies to effectively identify and mitigate cyber threats within network environments. Researchers have leveraged many approaches of machine learning to analyze various traffic patterns of networks, anomalies identification, and classify malicious activities. These efforts have resulted in the development of sophisticated intrusion detection systems capable of identifying known and unknown threats with high accuracy. In this section, we review the recent works presented for network attack detection using different approaches of deep learning and machine learning, highlighting the used methodologies and the obtained findings in such systems.

Network attack detection and analysis using different deep learning algorithms is proposed in [26]. In this work, the authors have used Long Short-Term Memory (LSTM), Convolutional Neural Network (CNN), and CNN with LSTM. The instances for normal and attack subjects were collected from the HTTP dataset CSIC 2010. The experimental outcomes showed that the proposed CNN with LSTM obtained higher results than CNN and LSTM, where it has been achieved 85% accuracy, 84% precision, 82% F-measure, and 85% sensitivity.

The work in [27] has been developed a deep learning model named the Learning Model for Cyber Attack Detection (LMCAD). In this work, the primary objective was to predict the real-time application layer with respect to attacks of Distributed Denial of Service (DDoS). Ensuring uninterrupted access to the system for authorized users falls under the duty of the availability component. In addition, the authors have modelled both denial-of-service attacks and normal network traffic. Subsequently, packet-level analysis was employed to distinguish between these two usage patterns. The Naïve Bayes classifier and LMCAD algorithm were employed to predict and identify various types of DDoS attacks. The highest obtained accuracies for the Naïve Bayes and LMCAD algorithms were 91.35% and 96.67%, respectively.

The authors in [28] have focused on Wireless Sensor Networks (WSNs) technology, which is an essential part of the Internet of Things (IoT). They have highlighted its susceptibility to routing incursions that target the Routing Protocol for Low-power and Lossy Networks (RPL). Additionally, they have examined various existing research endeavors aimed for intrusion detection and proposed a method for identifying 3 kinds of attacks on RPL. The simulation is carried out employing Contiki-Cooja, whereas there were 4 network scenarios that have been presented. The first scenario is normal, while the other 3 scenarios were for malicious in order to create training and test groups for the classification part, which is implemented using WEKA. In this work, the authors utilized different classification algorithms to differentiate whether the behavior is normal or malicious. The performance of this approach achieved a precision of 96%.

The deep learning approaches are also employed for an innovative anomaly-based IDS tailored for IoT networks [29]. Specifically, the Deep Neural Network (DNN) model is proposed for the purpose of attribute selection, where redundant features or those that have low effect on the classification are removed. Moreover, the model undergoes tuning with diverse hyperparameters. In this study, the UNSW-NB15 database is used, where this database encompasses 4 attack categories. The proposed model attained 84% accuracy for identifying network attacks. Additionally, this study addressed the issue of an imbalanced database by using Generative Adversarial Networks (GANs) to produce synthetic data for the minority category of attacks, which resulted in a balanced database and increased the accuracy of the proposed model to 91%.

The authors in [30] have proposed and employed many approaches to analyze traffic patterns and distinguish between malicious and normal traffic. Two different databases were used to train and test the classifiers, which are the DDoS attack SDN database and CICDDoS2019 database. Comprehensive preprocessing steps are conducted on both databases, including feature selection before applying detection techniques. Eight different models encompassing neural networks, ensembles, and machine learning approaches are chosen to analyze the databases. The model of deep neural networks demonstrated the highest performance and the most effective in identifying network attacks. The detection accuracy is further increased through optimizing the approach by hyperparameter tuning.

A group of authors in [31] have developed multiple machine learning models, where they aimed to detect intrusions utilizing a novel dataset called ALLFLOWMETER HIKARI2021. This dataset is comprised of 555,278 instances and 86 attributes collected by Zeek, encompasses six distinct types of attacks. In this work, the employed machine learning models are K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Random Forests (RF), and Multilayer Perceptron. These models exhibit a high detection accuracy rate of up to 99%.

3. Methodology

The proposed method in this work aims for detecting network cyber intrusions based on a machine learning technique. The samples of different network attacks are collected from the KDD'99 cup database. Meanwhile, these samples are then fed to the machine learning technique to detect network attacks. The GNB algorithm is used as the classifier for the detection part. The database and the machine learning technique will be described in detail in the next subsections, respectively.

3.1. Network intrusion dataset

Databases in the detection of network intrusion represent compilations of information entries comprising multiple attributes or characteristics alongside associated details pertinent to the cyber-security framework [32]. Therefore,

it is highly crucial for comprehending the composition of cyber-security data, encompassing diverse cyber-attacks and pertinent attributes. This understanding derives from the potential of basic security data that is sourced from relevant cyber channels to dissect varied patterns of security incidents or malicious activities, which facilitates the construction of a data-centric security model aligned with our objectives.

In this study, the KDD'99 cup database served as the foundation for constructing predictive models aimed at discerning the relationships between intrusions or various attacks [25]. This database encompasses 4,898,430 instances, each characterized by 41 attributes. Figure 1 provides an overview of the sample numbers for each class within the KDD'99 cup dataset.

Table 1 - An overview of the KDD'99 cup database.

Categories of attack	Attack name	Number of instances
DOS	SMURF	2807886
	NEPTUNE	1072017
	Back	2203
	POD	264
	Teardrop	979
U2R	Buffer overflow	30
	Load module	9
	PERL	3
	Rootkit	10
R2L	FTP Write	8
	Guess password	53
	IMAP	12
	MultiHop	7
	PHF	4
	SPY	2
	Warez client	1020
	Warez master	20
PROBE	IPSWEEP	12481
	NMAP	2316
	PORTSWEEP	10413
	SATAN	15892
Normal		972781

In this dataset, attacks are categorized into four principal groups. Table 1 shows the description of each attack group. The major purpose of utilizing this database is to train and test the GNB algorithm and make it able to detect or classify classes.

Accordingly, 90% of the KDD'99 cup database are used for training the GNB algorithm. Meanwhile, the remaining of 10% of the KDD'99 cup database are used for testing the GNB algorithm

Table 2: The description of attacks groups

Attacks Groups	Descriptions
Denial of Service (DoS)	It refers to a type of assault wherein a legitimate user is prevented from accessing system and network resources. This can impact services such as online banking and email. DoS attacks can manifest as Neptune attacks, Back attacks, and others.
Remote to Local (R2L)	R2L attacks occur when an unauthorized individual attempts to gain entry to a victim's machine without possessing valid credentials. R2L attacks include

	MultiHop attacks, Imap attacks, and others.
User to Root (U2R)	U2R attacks involve an assailant attempting to elevate their privileges after gaining local access to the victim's machine. U2R attacks include Load Module attacks, Perl attacks, and others.
PROBE	During a Probe attack, the perpetrator directs their efforts toward gathering information about the target host. PROBE attacks include Ipsweep attacks, Satan attacks, and others.

3.2. Classifier

In general, Network Intrusion Detection (NID) is the process of monitoring network traffic for malicious activities or unauthorized access attempts. It involves analyzing network packets, logs, and other data to identify potential security threats or breaches. In addition, the classification in NID involves categorizing network traffic into different classes, typically these classes labelled as normal class and intrusion (i.e., attack) class. This helps security analysts identify and respond to potential threats in real-time.

The Gaussian Naïve Bayes (GNB) classifier offers a straightforward yet effective approach to classification in network intrusion detection, leveraging probabilistic principles and the Gaussian distribution assumption to identify potentially malicious network traffic. While it has its limitations, where it remains a valuable tool in the arsenal of cybersecurity practitioners for detecting and mitigating security threats. Furthermore, the Bayes' theorem forms the foundation of the GNB algorithm. It describes the probability of a hypothesis given evidence and prior knowledge. In the detection of network intrusion, the GNB algorithm can identify or classify the class utilizing the next equation:

$$P(\text{ Class } | X) = \frac{P(X \mid \text{ Claas }) \times P(\text{ Class })}{P(X)} \qquad (1)$$

According to the equation (1), where P(" Class "|X) refers to the probability of a class given in the input data X, while the P(X|" Claas ") is the likelihood of observing the provided features (i.e., data) within the class, and P(" Class ") denotes the prior probability of the class. Lastly, P(X) means the total probability of observing the features. Furthermore, the GNB algorithm supposes that the data attributes are conditionally independent concerning the class label. In the detection of network intrusion, this means that the attributes of network traffic (e.g., source IP, destination IP, packet size) are independent of each other given whether the traffic is considered a normal class or attack class. The GNB model continuous features using Gaussian distributions. In other words, it assumes that the likelihood of observing a particular value of a feature comprised in a class follows a Gaussian distribution. Figure 2 illustrates the diagram of the GNB approach.

In the training phase, the parameters of the GNB algorithm are set and calculate the mean and standard deviation of each feature for each class in the training dataset. Then, the training process of the GNB algorithm is continued to train the algorithm based on the training set. Besides, the Gaussian distribution for each feature and class will be modeled. In the classification phase, for a data feature (e.g., network packet), the probability of it belonging to each class will be computed by using Bayes' theorem and the Gaussian distributions that have been modelled during the training phase. Then, the data features of the class are assigned with the highest probability. Subsequently, the performance of the GNB algorithm is evaluated in terms of various assessment measures. Finally, the experimental outcomes of the GNB approach are given in the detection of network attacks.

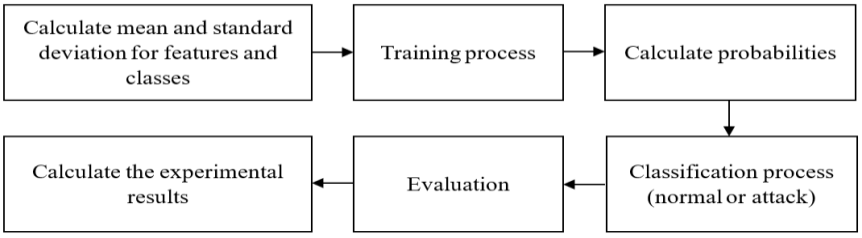

Figure 1. The diagram of the GNB approach

4. Results and discussion

The purpose of this work is to detect the network cyber-attacks based on the machine learning algorithm. The samples of network attacks category and normal category were collected from the KDD'99 cup database. Furthermore, in this database, there were 23 classes, where there 22 classes are considered network attacks and 1 class is considered normal. Besides, the database is split into 10% and 90% which were used for training and testing steps. The attributes of each class are fed to the machine learning model. The model of machine learning used in this work for the detection part is the GNB classifier. In this work, the experiments of the proposed model were performed using Python 3.10 over a PC Core i5 (2.40 GHz) and 6 GB RAM. The performance of the proposed model is assessed using various Key Performance Indicators (KPIs), namely accuracy, precision, sensitivity, F-measure (i.e., F1-score), specificity, and G-mean. These KPIs are computed by utilizing the subsequent equations:

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \quad (2)$$

$$Precision = \frac{TP}{TP + FP} \quad (3)$$

$$Sensitivity = \frac{TP}{TP + FN} \quad (4)$$

$$F1 - score = \frac{(2 \times Precision \times Sensitivity)}{(Precision + Sensitivity)} \quad (5)$$

$$Specificity = \frac{TN}{TN + FP} \quad (6)$$

$$G - Mean = \sqrt[2]{Specificity \times Sensitivity} \quad (7)$$

Figure 3 depicts the experimental results of the proposed GNB algorithm for the detection of network cyber-attacks. The experimental results show that the GNB algorithm has a high potential for the detection of network cyber-attacks. In other words, according to the obtained findings, the proposed GNB has been achieved 94.28% detection accuracy. This high accuracy score refers to that the proposed model performing correct predictions, where it indicates that the GNB algorithm has identified the class properly most of the time based on the used dataset. Additionally, the obtained results of precision and sensitivity were 98.32% and 94.28%, respectively. The results of precision and sensitivity metrics indicate that the proposed GNB algorithm predicts or detects the positive samples correctly. Meanwhile, the proposed GNB classifier has been achieved 95.89% F-measure. The high F-measure result denotes that the proposed GNB algorithm has been obtained high scores of precision and sensitivity metrics.

However, the GNB classifier has been obtained 59.23% and 53.01% for specificity and G-mean metrics, respectively. The result of the specificity metric indicates that the proposed GNB algorithm has a high error rate in terms of identifying the negative samples. Moreover, the results of specificity and G-mean metrics were not sufficient for the detection of network cyber-attacks. Hence, these results are considered the limitation of this work.

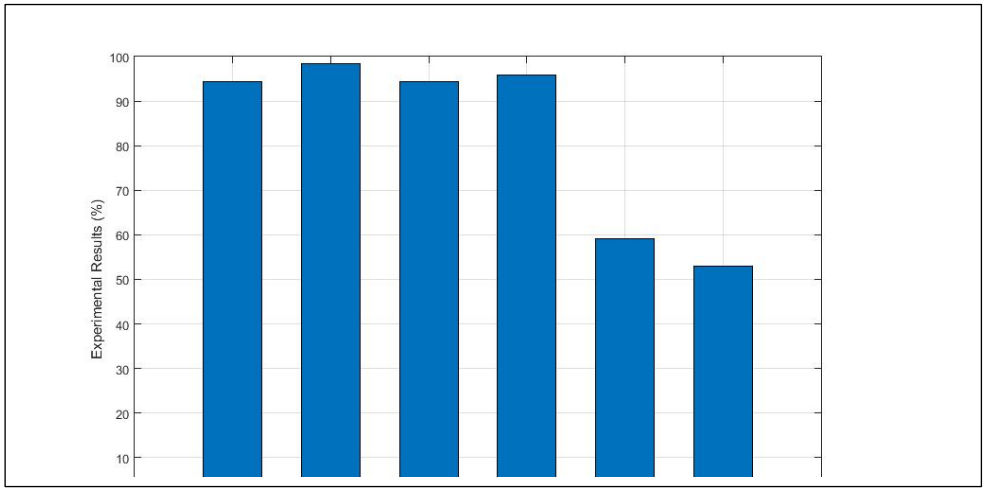

Figure 2. The experimental results of the GNB algorithm

The performance of the proposed GNB approach is compared with other works in detecting network attacks in terms of the detection accuracy [26]. These works have utilized the instances collected from the KDD cup database for training and testing various methods and approaches. The comparison outcomes show that the proposed GNB algorithm has been overcome the performance of all methods with respect to the detection accuracy of the network cyber intrusion. Table 2 presents the accuracy comparison between the proposed GNB approach with other algorithms.

Table 3: Comparison between algorithms for the detection of network attacks

Algorithms	Accuracy
The proposed GNB algorithm	**94.28%**
SVM [26]	**87.58%**
Logistic regression [26]	**88.86%**
KNN [27]	**78.1%**
RF [28]	**81.76%**
J48 [28]	**85.79%**
DNN [30]	**81:29%**
CNN [30]	**93:6%**
Deep learning [31]	**73.37%**

5. Conclusion

In the last decades, the Internet-connected everyone for the exchange of digital information, which was stored using cloud technology. However, the fast expansion of cloud technology has extremely increased digital data, which led to many network intrusions. Consequently, protecting this data became crucial for various reasons. Therefore, this study introduced a method for detecting network cyber intrusions. The instances of network cyber intrusions were collected from the KDD'99 Cup database. The proposed method employed the Gaussian Naïve Bayes (GNB) classifier to identify various instances of cyberattacks. Besides, the performance of the proposed GNB classifier has been evaluated utilizing numerous evaluation measures such as accuracy, precision, sensitivity, F-measure, specificity, and G-mean. The experimental results showed that the proposed GNB classifier achieved 94.28% accuracy, 98.32% precision, and 94.28% sensitivity. Additionally, the obtained result of the F-measure was 95.89%. However, the outcomes of specificity and G-mean obtained by the GNB classifier were 59.23% and 53.01%, respectively. The proposed GNB algorithm demonstrated its high performance in detecting network attacks, where it outperformed other methods in terms of detection accuracy. Future work can include developing the GNB algorithm and elevating its performance in the detection of cyberattacks.

References

[1] M. Albahar, "Cyber attacks and terrorism: A twenty-first century conundrum," Science and engineering ethics, vol. 25, pp. 993-1006, 2019.
[2] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management," Future internet, vol. 12, no. 9, p. 157, 2020.
[3] P. Lis and J. Mendel, "Cyberattacks on critical infrastructure: An economic perspective," Economics and Business Review, vol. 5, no. 2, pp. 24-47, 2019.
[4] A. Hassan and K. Ahmed, "Cybersecurity's impact on customer experience: an analysis of data breaches and trust erosion," Emerging Trends in Machine Intelligence and Big Data, vol. 15, no. 9, pp. 1-19, 2023.
[5] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, and H. Karimipour, "Cyber intrusion detection by combined feature selection algorithm," Journal of information security and applications, vol. 44, pp. 80-88, 2019.
[6] R. W. Anwar, T. Abdullah, and F. Pastore, "Firewall best practices for securing smart healthcare environment: A review," Applied Sciences, vol. 11, no. 19, p. 9183, 2021.
[7] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," Ieee access, vol. 6, pp. 35365-35381, 2018.
[8] F. T. Al-Dhief et al., "A survey of voice pathology surveillance systems based on internet of things and machine learning algorithms," IEEE Access, vol. 8, pp. 64514-64533, 2020.
[9] M. A. A. Albadr, M. Ayob, S. Tiun, F. T. Al-Dhief, A. Arram, and S. Khalaf, "Breast cancer diagnosis using the fast learning network algorithm," Frontiers in oncology, vol. 13, p. 1150840, 2023.
[10] O. S. Salman, N. M. A. A. Latiff, S. H. S. Arifin, O. H. Salman, and F. T. Al-Dhief, "Internet of medical things based telemedicine framework for remote patients triage and emergency medical services," in 2022 IEEE 6th International Symposium on Telecommunication Technologies (ISTT), 2022: IEEE, pp. 33-37.
[11] M. M. Hasan, S. Khandaker, N. Sulaiman, M. M. Hossain, and A. Islam, "Addressing Imbalanced EEG Data for Improved Microsleep Detection: An ADASYN, FFT and LDA-Based Approach," Diyala Journal of Engineering Sciences, pp. 45-57, 2024.
[12] H. M. Fadhil, Z. O. Dawood, and A. Al Mhdawi, "Enhancing Intrusion Detection Systems Using Metaheuristic Algorithms," Diyala Journal of Engineering Sciences, pp. 15-31, 2024.
[13] M. A. A. Albadr, S. Tiun, M. Ayob, and F. T. Al-Dhief, "Particle swarm optimization-based extreme learning machine for covid-19 detection," Cognitive Computation, pp. 1-16, 2022.
[14] M. A. A. Albadr, S. Tiun, M. Ayob, F. T. Al-Dhief, T.-A. N. Abdali, and A. F. Abbas, "Extreme learning machine for automatic language identification utilizing emotion speech data," in 2021 international conference on electrical, communication, and computer engineering (ICECCE), 2021: IEEE, pp. 1-6.
[15] K. Dhanya, S. Vajipayajula, K. Srinivasan, A. Tibrewal, T. S. Kumar, and T. G. Kumar, "Detection of network attacks using machine learning and deep learning models," Procedia Computer Science, vol. 218, pp. 57-66, 2023.
[16] A. Churcher et al., "An experimental analysis of attack classification using machine learning in IoT networks," Sensors, vol. 21, no. 2, p. 446, 2021.
[17] J. Alsamiri and K. Alsubhi, "Internet of things cyber attacks detection using machine learning," International Journal of Advanced Computer Science and Applications, vol. 10, no. 12, 2019.
[18] P. Varshini, K. Pavithra, and P. Anu, "Analysis of Network Attacks in Cyber Security using Deep Learning," in 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), 2024: IEEE, pp. 1-7.
[19] R. Karthiga, P. Kumar, S. Kumari, V. Sureka, and V. S. Pandi, "A Logical Cyber Security Enabled Methodology Design for Identifying Distributed Denial of Service Attacks Using Enhanced Learning Principles," in 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), 2023: IEEE, pp. 104-109.
[20] S. Rabhi, T. Abbes, and F. Zarai, "IoT routing attacks detection using machine learning algorithms," Wireless Personal Communications, vol. 128, no. 3, pp. 1839-1857, 2023.
[21] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," Computers and Electrical Engineering, vol. 107, p. 108626, 2023.
[22] M. D. T. Bennet, M. P. S. Bennet, and D. Anitha, "Securing Smart City Networks-Intelligent Detection Of DDoS Cyber Attacks," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 2022: IEEE, pp. 1575-1580.
[23] A. Ferriyan, A. H. Thamrin, K. Takeda, and J. Murai, "Generating network intrusion detection dataset based on real and encrypted synthetic attack traffic," Applied Sciences, vol. 11, no. 17, p. 7868, 2021.
[24] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," Journal of Big data, vol. 7, pp. 1-29, 2020.
[25] K. c. 99. [Online] Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[26] A. D. Vibhute, C. H. Patil, A. V. Mane, and K. V. Kale, "Towards detection of network anomalies using machine learning algorithms on the NSL-KDD benchmark datasets," Procedia Computer Science, vol. 233, pp. 960-969, 2024.
[27] J. Gao, "Network intrusion detection method combining CNN and BiLSTM in cloud computing environment," Computational intelligence and neuroscience, vol. 2022, 2022.
[28] A. Abirami, S. Lakshmanaprakash, R. Priya, V. Hirlekar, and B. Dalal, "Proactive Analysis and Detection of Cyber-attacks using Deep Learning Techniques," Indian Journal of Science and Technology, vol. 17, no. 15, pp. 1596-1605, 2024.
[29] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," Ieee Access, vol. 5, pp. 21954-21961, 2017.
[30] G. Andresini, A. Appice, and D. Malerba, "Nearest cluster-based intrusion detection through convolutional neural networks," Knowledge-Based Systems, vol. 216, p. 106798, 2021.
[31] D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Introducing deep learning self-adaptive misuse network intrusion detection systems," IEEE access, vol. 7, pp. 13546-13560, 2019.
[32] J Kravets,O Almusawi," Security management of the functioning of a multinode mobile cyber-physical system with a distributed registry based on an automatic model" Journal of Physics: Conference Series vol 2094 , pp 042040 ,2021