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)

Multi Level Deep Learning Model for Network Anomaly Detection

Maythem S. Derweesh*[*1], Sundos A. Hameed Alazawi[1], Anwar H. Al-Saleh[1]

[1] *Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq ,Email: maytham.salahdin@uomustansiriyah.edu.iq*

Email: ss.aa.cs@uomustansiriyah.edu.iq, Email: anwar.h.m@uomustansiriyah.edu.iq

ARTICLE INFO

Article history:
Received: 9 /11/2023
Rrevised form: 3 /12/2023
Accepted : 15 /12/2023
Available online: 30 /12/2023

Keywords:

Anomaly detection

Machine Learning

Deep Learning

cybersecurity

ABSTRACT

The increasing use of internet-based solutions and services in private and corporate sectors has resulted in a significant increase in personal internet involvement. This shift, concurrently exposed a heightened susceptibility to potential vulnerabilities, given the ability of malicious actors to exploit external networks, network services, or corporate infrastructures utilized for personal purposes. In recent times, there has been considerable interest in harnessing deep learning methodologies for enhancing cybersecurity, owing to their utilization of sophisticated learning algorithms for addressing pertinent online security challenges. Machine Learning (ML) and Deep Learning (DL) paradigms have been extensively applied across diverse dimensions of cybersecurity, encompassing tasks such as vulnerability assessment, malware classification, spam detection, and spoofing identification. In this paper, for hierarchical intrusion detection is proposed a novel multi-stage approach, The proposed system comprises two distinct classification modalities: multi-class classification and binary classification, contingent upon the nature of the attack within the dataset. the KDD99 dataset was leveraged to assess the classification performance of the proposed model. Both classification approaches involve main preprocessing steps, such as feature selection, feature normalization, building a Convolutional Neural Network (CNN) classifier apply on KDD99 dataset, deploying the CNN classifier for anomaly detection.

https:// 10.29304/jqcsm.2023.15.41346

1. Introduction

The issue of network security has become increasingly significant due to the exponential rise of computer network usage and the proliferation of billions of applications operating within this framework. Irrespective of individual or organizational users, contemporary hackers have identified more avenues to exploit vital information [1]. Hence, the reliable detection of assaults and anomalies in networks becomes increasingly crucial for intrusion detection systems (IDSs). It is crucial to priorities developing resilient detection techniques on Intrusion Detection Systems (IDSs) to effectively safeguard against the continuously expanding range of harmful behaviors [1, 2]. Network anomalies can arise from various factors, including network overload, device malfunctions, misconfigurations, malicious actions, or network attacks that intercept and analyze standard network services [3, 4]. In the contemporary age, safeguarding digital systems from cyber threats is a paramount concern for IT infrastructures and the broader technological landscape. The persistent endeavors to infiltrate national and organizational network structures underscore the insufficiency of traditional firewall and antivirus protections against advanced digital attacks. This insufficiency leads to potential vulnerabilities in systems. Recent times have

∗Maythem S. Derweesh

Email addresses: maytham.salahdin@uomustansiriyah.edu.iq

Communicated by 'sub etitor'

borne witness to numerous instances of organizations falling victim to cyber assaults and data breaches, culminating in substantial financial losses reaching millions of dollars and the exposure of customer information. Notable examples of these incidents include Twitter, SolarWinds, and Finastra. Projections indicate a staggering surge from $3 trillion to $10.5 trillion in costs attributed to cybercrime, positioning it as an unprecedented "transfer of economic wealth" [5].

The rapidly expanding network has brought efficiency, convenience, and a growing demand for high-quality service. Conventional machine learning techniques, including Bayesian [6], Support Vector Machines [7], Decision Trees [8] and Logistic Regression [9], have been extensively employed in network intrusion detection systems, and other similar methods. These strategies have yielded favorable outcomes. Nevertheless, these techniques are inadequate for handling extensive and complex data sets, and are incapable of addressing the issue of diminished classification accuracy caused by their susceptibility to outliers and noise. Simultaneously, traditional machine learning methods have struggled to match user demands due to the ongoing advancement of digital technology and the growing variety of cyberattacks.

There exist two distinct categories of Intrusion Detection Systems (IDSs). There are two types of attack detection methods: misuse detection, which identifies assaults by comparing them to known patterns, and anomaly detection, which identifies aberrant attacks by comparing them to regular usage patterns. While the detection of bad using makes the recognition of not-familiar attacks hard, the detection of abnormal states has the ability to detect the new attacks; however, the detection of abnormal attacks can generate a lot of false alarms because of the deficiencies in accurately detecting the normal patterns. Deep learning (DL) is a method to solve this limitation by developing unique attributes with a sophisticated neural network. Utilizing Deep Learning in Intrusion Detection Systems can mitigate the limitations of IDS. Machine Learning (ML) and Deep Learning (DL) autonomously acquire knowledge of an intrusion set and identify regular usage patterns, hence minimizing the occurrence of false alerts. Anomaly based system for intrusion detection is a solution for cyber security that aims to identify cyber attacks by monitoring and classifying the system and network activities as normal or abnormal procedures. The goal of these systems is to reach a balance between reducing false alarms and increasing the detection rate [10]. Anomaly detection, including conntinous monitoring and analysis of typical network patterns, allows for the detection of potential threats and the identification of deficiencies from the known standards. The anomaly events are considered significant because they refer to atypical events and may be critical, such as abnormal flows of traffic indicating of ongoing assaults or illicit transmission of data activities. Anomaly could be categorized as three distinct kinds: point, collective, and contextual. Each type of attack corresponds to specific security breaches, including Denial of Service (DoS), Probe, User to Root (U2R), and Remote to Local (R2L) attacks [11].

Efficiently spotting and categorizing these anomalies necessitates the adaptation of network intrusion detection systems (NIDS) to dynamic network settings, encompassing novel protocols and behaviors. Various approaches, such as statistical, knowledge-based, and machine-learning techniques, have been harnessed in anomaly-based NIDS. However, research challenges need addressing to enhance Performance and align these techniques with the ever-evolving characteristics of network data [12].

The frequency of internet attacks is on the rise, and in response to these threats, two fundamental methods are employed to safeguard information security with the principles of CIA (confidentiality, integrity, availability) [13] in mind: Identification based on signatures and detection based on anomalies. Signature-based methods rely on specific databases specifically created to identify and categorize potential risks. Research has demonstrated the effectiveness of this approach, but it necessitates continuous updates to the databases and the processing of new attack data. Furthermore, even with up-to-date databases, they remain susceptible to zero-day attacks, which are previously unseen threats that databases cannot defend against [14].

This paper proposes a hierarchical intrusion detection system consisting of multiple stages to determine whether data is normal or attack. Subsequently, data identified as an attack is classified into specific attack types. The proposed system is evaluated using the KDD99 dataset.

In our proposed model, binary classification is implemented as one stage, while multiple classification serves as a separate stage. This approach reduces the volume of data processed in the second stage (multi-class), resulting in more efficient processing and significantly reduced classification time.

in Section 2. related works are presented, in Sections 3 describe Network Anomaly Detection, in section 4 and 5, respectively. We develop our CNN based ADS model and test our model and in Section 5 the conclusion.

2. Related Works

Numerous research endeavors and studies have been dedicated to enhancing the precision and detection rates of identifying anomalous network traffic through the application of diverse technologies.
In 2019, Xiao et al. utilized a Convolutional Neural Network (CNN) within the framework of Intrusion Detection Systems (IDS). Their objective was to extract critical features from data that had undergone dimensionality reduction. The CNN model was employed to process and interpret the dimensionality-reduced data, ultimately enabling the detection of network intrusions [15]. In 2019, Yang et al, used (CNN) network that upgraded to detect wireless network attacks, the changes in (CNN) framework aim to increase the efficiency of detecting the wireless attacks [16]. In 2019, Lin et al, proposed combining LSTM and AM to improve pattern recognition. LSTM, known for its memory, helps remember network traffic patterns. The hierarchical neural network-based LSTM method combines current data with historical knowledge to improve classification outcomes. Deep learning uses LSTM to store and keep information, like the human brain. The Attention Mechanism (AM) replicates the brain's ability to focus on crucial details, helping the model detect significant data patterns. LSTM and AM increase network performance by identifying and interpreting complex data patterns [17]. In 2020, Karatas et al. used six machine learning methods to examine the CICIDS2018 dataset in 2020. The machine learning methods mentioned were adaptive boosting (AdaBoost), decision tree (DT), random forest (RF), k-nearest neighbours (KNN), gradient boosting (GB), and linear discriminant analysis. The not equal of assault types in the dataset was addressed via synthetic minority oversampling (SMOTE). Synthetic samples for underrepresented attack categories were generated using SMOTE, improving minority class case detection [18]. In 2020, Mohamed et al, study the CICIDS2018 and Bot-IoT datasets, they tests sevent methods to deep learning, used DNN, CNN, RNN, DBN, DBM, RBM, and deep autoencoder, this study test the efficiency of modern deep learning techniques inintrusion detection [19]. In 2020, Zhiquan et al, improved Intrusion Detection Systems using CNN and Adaptive Synthetic Sampling ADASYN. The IDS uses a uniform method to enhance the precision and dependability of its abilities to improve its network attack detection accuracy [20]. In 2020, Kaiyuan et al, created IDS by combines hybrid sampling with CNN and Bidirectional Long Short-Term Memory. The hybrid technique uses CNN and BiLSTM to monitor and analyze network operations to improve network intrusion detection using both (CNN) and (BiLSTM) techniques [21]. In 2020, Feng et al, used (LSTM-RNN) to develop full system to extract the complex attacks. their methodology included upgrade full structure that smoothly combine among data preparing, features extraction, training and detection. the system designed and engineered carefully to effectively deal with the various information channels, resulting to create extensive wide work to detect attacks. [22]. In 2020, Jahanzaib et al, this paper presents a security protection framework designed specifically to secure the control layer of a software defined network. For adept and prompt intrusion detection system (IDS), this platform employs the capabilities of (LSTM) and (CNN) methodologies [23]. In 2020, Jiyeon et al, the researchers made a study using KDD99 and CICIDS2018 datasets, that contained a wide range of attacks types. however, they mainly focus on defeat the Denial of Service (DoS) attacks. the choice of using these datasets inspired from the high international frequency of Distributed Denial of Service (DoS) attack incidents, which offered of a lot of chances for training and evaluate the proposed Convolutional Neural Network (CNN) architecture. The CNN architecture chosen because of it is efficiency in extracting the high value information from the extensive datasets via it is convolutional layers [24]. In 2021, Anzhelika et al, performed a study using the two datasets KDD99 and CICIDS2018. they used the structure of U-Net with temporal convolutional network (TCN) to identify the network threats. to enhance the accuracy, they combined the TCN and LSTM models, that resulted to enhanced the performance. TCN played a critical part in effective processing time series data by using the wide convolutions, that resulted to increase the convolution range and lead to higher outputs [25]. In 2021, Yakubu et al, proposed approach named (BiDLSTM) to intrusion detection system (IDS) to identify the attacks Remote-to-Local (R2L) and User-to-Root (U2R) accurately. during execute their model, they achieved high level of accuracy compared to using (LSTM) traditional approach [26]. In 2021, FatimaEzzahra et al, used Principal Component Analysis (PCA) on the dataset employing a mutual information technique. The goal was to reduce the number of dimensions and show important characteristics. The dataset performed Principal Component Analysis (PCA) using a mutual information technique to reduce dimensionality and find important characteristics. Upon finishing the feature extraction procedure, they proceeded to create a detection methodology for attacks in the dataset using (LSTM) [27]. In 2021, Satish Kumar et al, study the changing environment of network attacks and the importance (IDS) in ensuring network security.

The article reviews research trends in Network-based Intrusion Detection Systems (NIDS), covering approaches and commonly used datasets. It analyzes the popularity of various NIDS techniques based on citations and publications

over a 15-year period [28]. In 2022, Theyazn et al, Employing Convolutional Neural Networks (CNN) and a combination of CNN and Long Short-Term Memory (CNN-LSTM), the focus was on fortifying the security of autonomous vehicles from potential intrusions. undertook the task of training and assessing these techniques using an authentic dataset sourced from an autonomous vehicle network. dataset encompassed an array of attack types, including spoofing, flooding, and replay attacks, alongside legitimate packets [29]. In 2023, Tianhao Hou and colleagues proposed a approach for Network Intrusion Detection (NID) by integrating the log-cosh conditional variational autoencoder (LCVAE) with a convolutional bi-directional long short-term memory neural network (LCVAE-CBiLSTM) utilizing deep learning (DL) methodologies. This method enables virtual samples to acquire distinct threat data, hence augmenting the possible characteristics related to unbalanced assault types. In order to consider both the temporal and spatial elements of assaults, a hybrid feature extracting model is proposed. This model mixes (CNN) with (BiLSTM) networks [30]. In 2023, Jiaming Song et al, introduce a network intrusion detection model, denoted as CSK-CNN, which is built upon a two-layer convolutional neural network (CNN) and employs the Cluster-SMOTE + K-means algorithm to handle imbalanced datasets. The CSK-CNN model combines Cluster-SMOTE, a synthetic minority oversampling technique based on clustering, with a K-means-based under sampling approach. This two-layer network not only enables the identification of abnormal network traffic but also facilitates the classification of such traffic into specific attack categories [31].

We want intrusion detection systems to possess the capability to not only detect the presence of an attack but also accurately classify the specific type of attack. Consequently, certain researchers have utilized Convolutional Neural Networks (CNN) to build a multi-class intrusion detection system. Nevertheless, their investigations revealed that, akin to the real-world distribution of attacks, the dataset exhibits significant variation in the amount of data across different classes. Hence, the rate of recognition is unsatisfactory for attack categories that have a limited amount of training data. The strategy presented in this research aims to address the limitations identified in the previous investigations. The previous works are summarized in Table 1.

Table 1. Summary of recent researches

Research	Year	Methods	Dataset	Classification	Accuracy
[15]	2019	LSTM + AM	CSE-CIC-IDS2018	Multi-class	96.19%
[16]	2019	Improved CNN	NSLKDD	Multi-class	95.36%
[17]	2019	LSTM	CSE-CIC-IDS2018	Multi-class	96%
[18]	2020	Adaboost	CSE-CIC-IDS2018	Multi-class	99.69%
[19]	2020	DNN,	CSE-CIC-IDS2018	Multi-class	97.28%
		RNN,			97.31%
		CNN			97.38%
[20]	2020	ADASYN + CNN	NSLKDD	Multi-class	80.08%
[21]	2020	CNN + BiLSTM	NSL-KDD	Multi-class	83.58%
			UNSW-NB15		77.16%
[22]	2020	LSTM	KDD99	Binary	98.94%
[24]	2020	LSTM + CNN	CSE-CIC-IDS2017	Multi-class	98.60%
[25]	2021	TCN + LSTM	KDD99	Multi-class	92.05%
			CSE-CIC-IDS2018		97.77%
[26]	2021	TCN + LSTM	KDD99	Multi-class	92%
			CSE-CIC-IDS2018		97%
[27]	2021	BiLSTM	NSLKDD	Binary	94.26%
				Multi-class	91.36%
[29]	2022	CNN + LSTM	Collected data	Multi-class	97.30%
[30]	2023	CNN + BiLSTM	KDD99	Multi-class	87.30%
[31]	2023	CSK-CNN	UNSW-NB15	Multi-class	98.77%
			CSE-CIC-IDS2017		99.91

3. Network attacks

Network security's role is to protect digital information, preserving data confidentiality, integrity, and resource availability [30]. In simple terms, a threat or attack encompasses any entity with harmful attributes aimed at undermining a network. Weak network design, user negligence, and misconfiguration of software or hardware can render a network susceptible to such attacks [32].

The types of networks attack are:

1. Denial of Service (DoS): Denial-of-Service (DoS) assaults refer to malevolent endeavors aimed at impeding the regular operations of a certain system, network, or service by inundating it with an excessive volume of traffic or requests for resources [33, 34].
2. Probe: The initiation of a Probe attack is regarded as the initial stage in an authentic attempt to breach a host or network. While these attacks may not result in immediate damage, they are seen as significant risks to organizations due to their potential to acquire valuable information that could be utilized to execute subsequent devastating strikes [35].
3. User to Root (U2R): An attack is initiated when an assailant seeks to illicitly obtain access to an administrator account for the purpose of manipulating or exploiting critical resources [36].
4. Remote to User (R2U): The assault is initiated with the intention of obtaining local access to a specific computer, enabling the attacker to assume the role of a user and so get the privilege to transmit packets across its network. This type of attack is commonly referred to as a Remote-to-Local (R2L) attack [37].

Figure (1) illustrate the analysis of attack types within the dataset (KDD99).

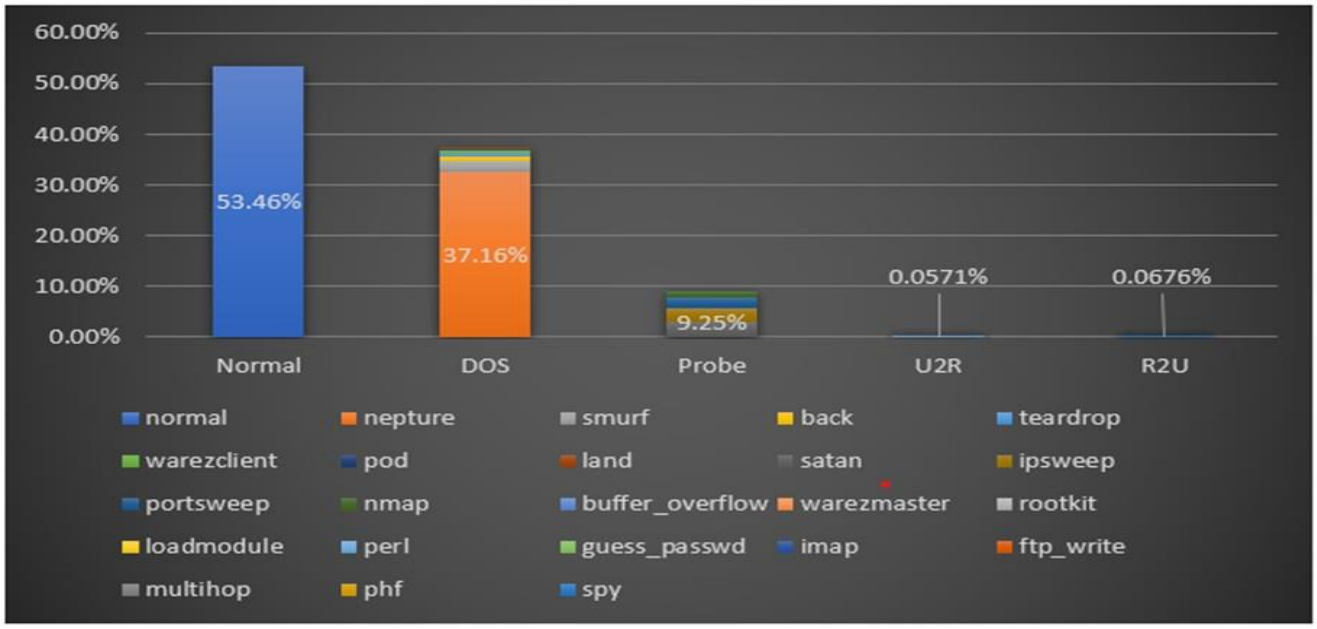

Figure 1. The attack types in dataset (KDD99)

4. Proposed Methodology

Figure 2 illustrates the overall architecture of the system's framework. During the dataset preprocessing phase, we executed a range of procedures and operations on the data. During the second stage, the characteristics of each data sample were standardized prior to being fed into the CNN model. During the third step, the most optimal characteristics are chosen. The CNN model underwent training and testing in the fourth step, utilizing the KDD99 dataset. Ultimately, we employed the Convolutional Neural Network (CNN) model for the purpose of anomaly detection.

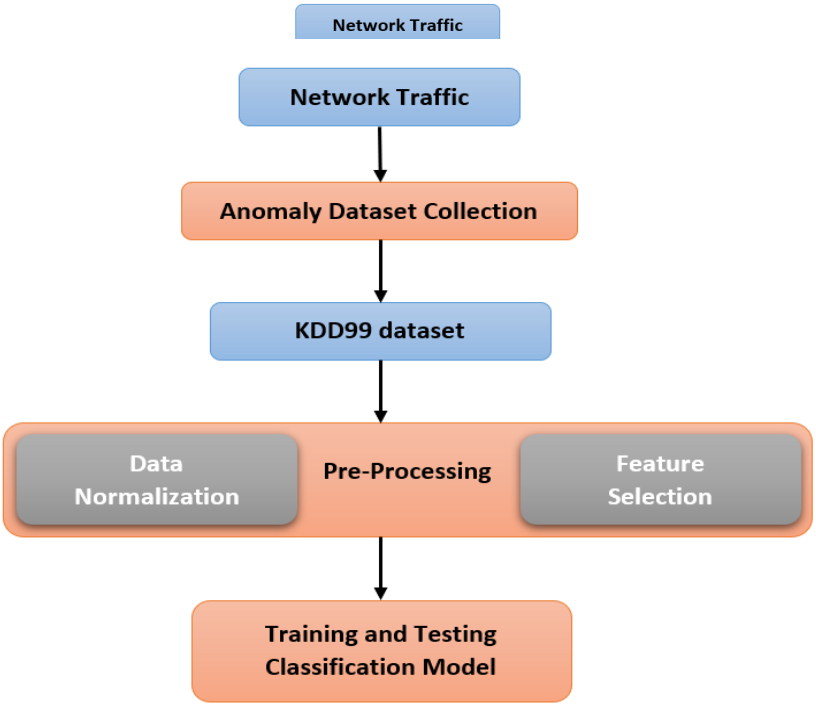

Figure 2. The general structure for Anomaly Detection System

The model trained by Lenovo laptop with hardware capabilities of 24 Gigabyte of RAM, Core i7 2.30GHz CPU, and 64-bit windows 1 professional system. All experimental results conducted python 3 environment. The main steps of the proposed system are summarized as follows:

Preprocessing

In order to get better results, the data goes through some necessary preprocessing procedures such as feature normalization and feature selection .Consequently, protocol types are converted into integer numerical values. Label encoding is particularly useful for unordered and case-sensitive categorical data, as it assigns each category an integer value in an alphabetical manner.

- Data Normalization and scaling

The current dataset consists of attributes that are measured on varying scales, significantly impacting the performance of the model. To address this issue, normalization is employed as a preprocessing step [34]. This process enhances flexibility and maintains consistent relationships among diverse data scales within both machine learning (ML) and deep learning (DL) models.

Therefore, the utilization of the min-max normalization approach is employed to transform characteristics into a range of values that is more appropriate and reliable, limited to the interval of [0, 1]. The Min-Max scaler, which is a component of the normalization function, is represented by equation (1):

$$\text{Xnormalized} = \frac{\text{X} - \text{Xmin}}{Xmax - Xmin} \qquad (1)$$

- Feature Selection

Feature engineering is a crucial preprocessing step that offers several benefits, such as reducing computing costs, saving time, and improving model performance. Additionally, it involves determining the most influential feature selection strategy from various types of feature selection strategies.

CNN model has feature selection inside his architecture, and we can add additional feature selection step before input data in the CNN model and we use (Information Gain) to decrease the number of features and reduce the process time.

- Dataset balancing

We employed the SMOTE technique to achieve dataset balancing. SMOTE is an oversampling method that creates synthetic samples specifically for the minority class. This technique mitigates the problem of overfitting caused by random oversampling. This approach focuses on the feature space. in order to produce novel instances by means of interpolation between closely located positive instances.

Anomaly Detection and Classification

The heart of our proposed methodology lies in the anomaly detection and classification stage, where Convolutional Neural Networks (CNNs) are employed to identify and categorize network intrusions.
The current stage is segmented into the subsequent phases:

- CNN Architecture

To commence, the initial step involves the development of a Convolutional Neural Network (CNN) structure specifically designed for the purpose of network intrusion detection. Figure 3 illustrates that the architecture consists of several convolutional layers, followed by pooling layers. These layers allow the model to autonomously acquire structured features from the preprocessed network traffic data.
The Conv1 and Conv2 Layers are 1D convolutional layers that are designed to learn local patterns or features in the input data, the choice of the number (64) of filters are based on empirical experimentation and to reach the best classification results.

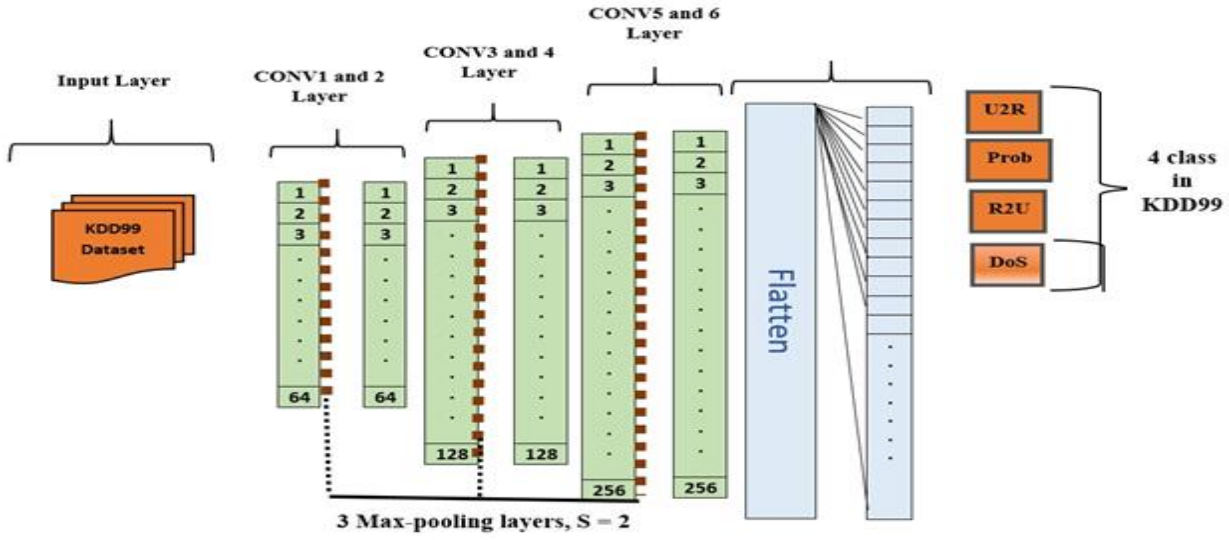

Figure 3. general structure for CNN

Table 2. The proposed model (CNN) layers and parameters settings

No.	Layer type	Filters	Size	Activation function
1	Convolutional	64	3	Leaky ReLU
2	Convolutional	64	3	Leaky ReLU
3	Max pooling	/	2	/
4	Convolutional	128	3	Leaky ReLU
5	Convolutional	128	3	Leaky ReLU
6	Max pooling	/	2	/
7	Convolutional	256	3	Leaky ReLU
8	Convolutional	256	3	Leaky ReLU
9	Max pooling	/	2	/
10	Flatten	/	/	/

11	Dense	256	/	Leaky ReLU
12	Dropout	/	0.3	/
13	Dense	128	/	Leaky ReLU
14	Dropout	/	0.3	/
15	Dense	64	/	Leaky ReLU
16	Dropout	/	0.3	/
17	Dense	/	/	Sigmoid

- Model training

The dataset split into training data (80%) and testing data (20%). The CNN model is trained on a labeled dataset that includes both normal network traffic and various types of intrusions. During training, the model learns to differentiate between normal and anomalous patterns by adjusting its internal parameters through backpropagation

- Classification and Detection of Anomalies

The classification of network anomalies was based on the content of the attributes of the dataset, normal, DoS, Probe, U2R, R2U for KDD99 dataset After training the model classifier, the system tests the model by entering untrained data (original preprocessed dataset) into the classifier and then examining the accuracy of the proposed model. Fig. 4 shown the classification structure for both data sets, where we notice that the data is shared of DoS attack, with the presence of cases that are considered normal and harmless to the network.

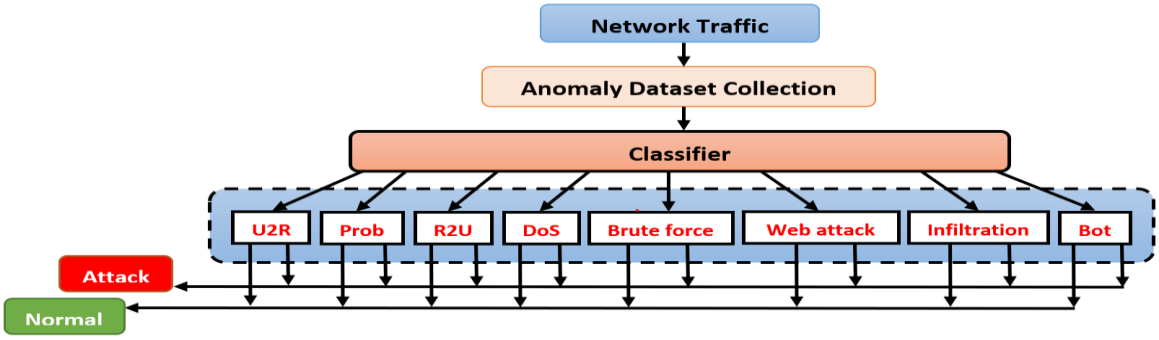

Figure 4. The Architecture of Anomaly Detection System

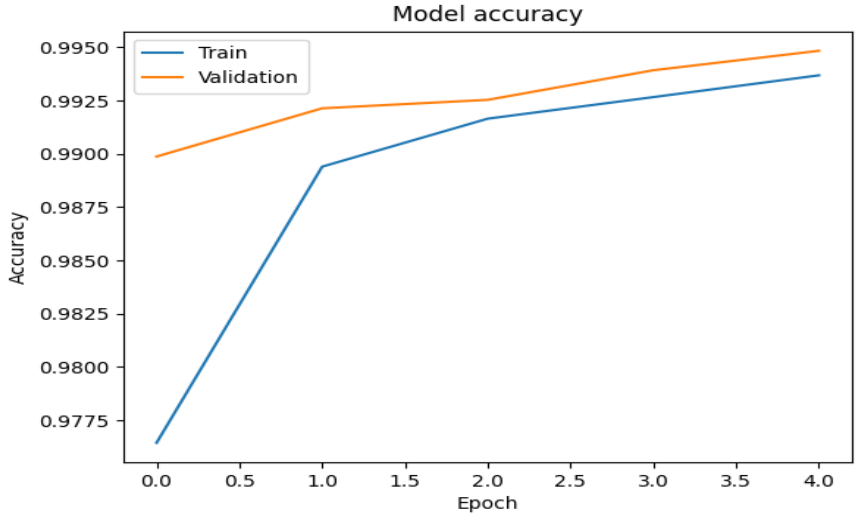

Figure 5. training & validation accuracy values

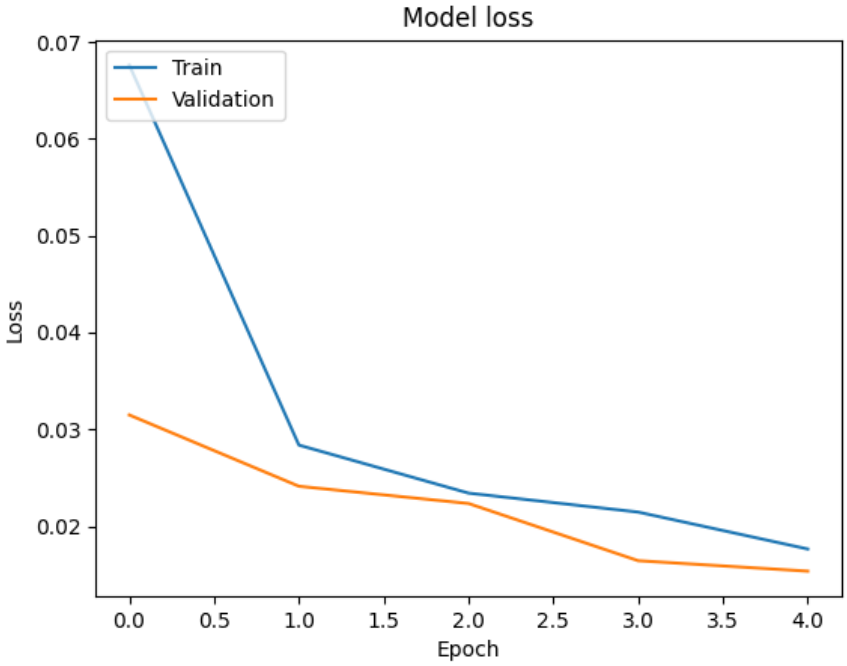

Figure 6. training & validation loss values

5. Results

Proposed method achieved good results, the accuracy for Binary classifying (0.9933) and for multi-classifying (0.9983) as presented in Table 3.

Table 3. illustrate the Performance of the classifiers on Binary and multi-class classification.

Table 3. performance metrics for the classifier

Stage 1				
		Binary		
Epoch	Accuracy	Precision	Recall	F1 score
5	0.9933	0.9960	0.9896	0.9928
Stage 2				
		Multi-class		
Epoch	Accuracy	Precision	Recall	F1 score
20	0.9983	0.9983	0.9983	0.9983
		Accuracy for each attack type		
Attack type	Accuracy	Attack type	Accuracy	

back	1.0	perl	1.0
buffer_overflow	0.6666	phf	1.0
guess_passwd	1.0	pod	1.0
imap	1.0	portsweep	0.9964
ipsweep	0.9958	resultssatan	0.9916
land	1.0	smurf	1.0
neptune	1.0	teardrop	1.0
nmap	0.9774	warezclient	1.0

In order to further verify the effectiveness of the anomaly detection model proposed in this paper, a performance comparison experiment is carried out in this part. Under identical experimental conditions, we evaluated the performance of well-known machine learning methods, including RNN, LSTM, and other state-of-the-art intrusion detection models, on the given dataset. The performance comparison is displayed in Table 4. The bold words signify the assessment criteria of the suggested model.

Table 4. Comparison of different models

Research	Methods	Dataset	Classification	Accuracy
[16]	Improved CNN	NSLKDD	Multi-class	95.36%
[19]	DNN, RNN, CNN	CSE-CIC-IDS2018	Multi-class	97.28% 97.31% 97.38%
[20]	ADASYN + CNN	NSLKDD	Multi-class	80.08%
[21]	CNN + BiLSTM	NSL-KDD UNSW-NB15	Multi-class	83.58% 77.16%
[22]	LSTM	KDD99	Binary	98.94%
[24]	LSTM + CNN	CSE-CIC-IDS2017	Multi-class	98.60%
[25]	TCN + LSTM	KDD99 CSE-CIC-IDS2018	Multi-class	92.05% 97.77%
[26]	TCN + LSTM	KDD99 CSE-CIC-IDS2018	Multi-class	92% 97%
[29]	CNN + LSTM	Collected data	Multi-class	97.30%
[30]	CNN + BiLSTM	KDD99	Multi-class	87.30%
Proposed model	**CNN**	**KDD99**	**Binary** **Multi-class**	**99.33%** **99.83**

6. Conclusion

We have created a convolutional neural network (CNN) model to detect anomalies in networks, specifically utilizing the KDD99 dataset. The KDD99 dataset consists of four attack categories, namely DoS (Denial of Service), U2R (User to Root), R2L (Remote to Local), and Probing. The majority of KDD studies that utilize deep learning techniques have focused on performing binary classifications to differentiate between normal and attack instances within the full dataset. These studies have also conducted multiclass classifications to differentiate the four groups in KDD. Our CNN model has been created taking into account the number of convolutional layers and the dimensions of the kernel. To evaluate our model, we created multiple scenarios, considering hyperparameters such as the number of filters, the amount of convolutional layers, and the kernel size described before. We conducted binary and multiclass classifications for each situation and subsequently recommended the ideal scenarios that exhibit superior performance. The empirical findings indicate that our suggested approach outperforms previous studies in terms of accuracy, both in binary and multiclass classifications. Nevertheless, the model presented in this article exhibits certain limitations, requiring substantial resources and featuring a rather large number of parameters. significantly study should explore methods for minimizing latency in deep learning-based intrusion detection systems in order to significantly decrease the computational time required.

Acknowledgements

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] Chen, L., et al. *Zyell-nctu nettraffic-1.0: A large-scale dataset for real-world network anomaly detection*. in *2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*. 2021. IEEE.
[2] Fernandes, G., et al., *A comprehensive survey on network anomaly detection.* Telecommunication Systems, 2019. **70**: p. 447-489.
[3] Bhattacharyya, D.K. and J.K. Kalita, *Network anomaly detection: A machine learning perspective*. 2013: Crc Press.
[4] hashim, h.b., *Challenges and Security Vulnerabilities to Impact on Database Systems.* Al-Mustansiriyah Journal of Science, 2018. **29**(2): p. 117-125.
[5] Almulla, K., *Cyber-attack detection in network traffic using machine learning.* 2022.
[6] Ren, X., W. Jiao, and D. Zhou, *Intrusion detection model of weighted navie bayes based on particle swarm optimization algorithm.* Computer Engineering and Applications, 2016. **52**(7): p. 122-126.
[7] Sahu, S.K., et al., *An SVM-based ensemble approach for intrusion detection.* International Journal of Information Technology and Web Engineering (IJITWE), 2019. **14**(1): p. 66-84.
[8] Ahmim, A., et al. *A novel hierarchical intrusion detection system based on decision tree and rules-based models*. in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 2019. IEEE.
[9] Ioannou, C. and V. Vassiliou. *An intrusion detection system for constrained WSN and IoT nodes based on binary logistic regression*. in *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. 2018.
[10] Mishra, S., et al., *Swarm intelligence in anomaly detection systems: an overview.* International Journal of Computers and Applications, 2021. **43**(2): p. 109-118.
[11] Rana, S., *Anomaly Detection in Network Traffic using Machine Learning and Deep Learning Techniques.* Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2019. **10**(2): p. 1063-1067.
[12] Khan, W. and M. Haroon, *An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks.* International Journal of Cognitive Computing in Engineering, 2022. **3**: p. 153-160.
[13] Haqi Al-Tai, M., B.M. Nema, and A. Al-Sherbaz, *Deep Learning for Fake News Detection: Literature Review.* Al-Mustansiriyah Journal of Science, 2023. **34**(2): p. 70-81.
[14] Khan, A.R., et al., *Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions.* Security and Communication Networks, 2022. **2022**.
[15] Xiao, Y., et al., *An intrusion detection model based on feature reduction and convolutional neural networks.* IEEE Access, 2019. **7**: p. 42210-42219.
[16] Yang, H. and F. Wang, *Wireless network intrusion detection based on improved convolutional neural network.* Ieee Access, 2019. **7**: p. 64366-64374.
[17] Lin, P., K. Ye, and C.-Z. Xu. *Dynamic network anomaly detection system by using deep learning techniques*. in *Cloud Computing–CLOUD 2019: 12th International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings 12*. 2019. Springer.
[18] Karatas, G., O. Demir, and O.K. Sahingoz, *Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset.* IEEE access, 2020. **8**: p. 32150-32162.
[19] Ferrag, M.A., et al., *Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study*. Journal of Information Security and Applications, 2020. **50**: p. 102419.

[20] Hu, Z., et al., *A novel wireless network intrusion detection method based on adaptive synthetic sampling and an improved convolutional neural network.* IEEE Access, 2020. **8**: p. 195741-195751.
[21] Jiang, K., et al., *Network intrusion detection combined hybrid sampling with deep hierarchical network.* IEEE access, 2020. **8**: p. 32464-32476.
[22] Jiang, F., et al., *Deep learning based multi-channel intelligent attack detection for data security.* IEEE transactions on Sustainable Computing, 2018. **5**(2): p. 204-212.
[23] Malik, J., et al., *Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in SDN.* IEEE Access, 2020. **8**: p. 134695-134706.
[24] Kim, J., et al., *CNN-based network intrusion detection against denial-of-service attacks.* Electronics, 2020. **9**(6): p. 916.
[25] Mezina, A., R. Burget, and C.M. Travieso-González, *Network anomaly detection with temporal convolutional network and U-Net model.* IEEE Access, 2021. **9**: p. 143608-143622.
[26] Imrana, Y., et al., *A bidirectional LSTM deep learning approach for intrusion detection.* Expert Systems with Applications, 2021. **185**: p. 115524.
[27] Laghrissi, F., et al., *Intrusion detection systems using long short-term memory (LSTM).* Journal of Big Data, 2021. **8**(1): p. 65.
[28] Kumar, S., S. Gupta, and S. Arora, *Research trends in network-based intrusion detection systems: A review.* IEEE Access, 2021. **9**: p. 157761-157779.
[29] Aldhyani, T.H. and H. Alkahtani, *Attacks to automatous vehicles: A deep learning algorithm for cybersecurity.* Sensors, 2022. **22**(1): p. 360.
[30] Hou, T., et al., *A Marine Hydrographic Station Networks Intrusion Detection Method Based on LCVAE and CNN-BiLSTM.* Journal of Marine Science and Engineering, 2023. **11**(1): p. 221.
[31] Song, J., et al., *CSK-CNN: Network Intrusion Detection Model Based on Two-Layer Convolution Neural Network for Handling Imbalanced Dataset.* Information, 2023. **14**(2): p. 130.
[32] Van, N.T. and T.N. Thinh. *An anomaly-based network intrusion detection system using deep learning*. in *2017 international conference on system science and engineering (ICSSE)*. 2017. IEEE.
[33] Ferrag, M.A., et al., *Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks.* Future internet, 2020. **12**(3): p. 44.
[34] Mahmood, H.A., *Network Intrusion Detection System (NIDS) in Cloud Environment based on Hidden Naïve Bayes Multiclass Classifier.* Al-Mustansiriyah Journal of Science, 2018. **28**(2): p. 134 - 142.
[35] Damasevicius, R., et al., *LITNET-2020: An annotated real-world network flow dataset for network intrusion detection.* Electronics, 2020. **9**(5): p. 800.
[36] Labonne, M., *Anomaly-based network intrusion detection using machine learning*. 2020, Institut polytechnique de Paris.
[37] Li, R., et al., *GTF: An Adaptive Network Anomaly Detection Method at the Network Edge.* Security and Communication Networks, 2021. **2021**: p. 1-12.