BİTLİS EREN ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

ISSN: 2147-3129 / e-ISSN: 2147-3188

Article Type : Research Article
Received : January 18, 2025
Revised : February 19, 2025
Accepted : March 10, 2025
DOI : 10.17798/bitlisfen.1622548

Year : 2025
Volume : 14
Issue : 1
Pages : 597-609

CLASSIFICATION OF MALICIOUS NETWORK DATASET WITH RESIDUAL CNN

Mücahit KARADUMAN [1], **Sercan YALÇIN [2,*]**, Muhammed YILDIRIM [3]

[1] *Malatya Turgut Özal University, Computer Engineering Department, Malatya, Türkiye*

[2] *Adıyaman Eren University, Mechanical Engineering Department, Adıyaman, Türkiye*

[3] *Malatya Turgut Özal University University, Mechanical Engineering Department, Malatya, Türkiye*

**** Corresponding Author:*** *svancin@adiyaman.edu.tr*

ABSTRACT

This paper proposes a Residual Convolutional Neural Network (CNN) based model for malicious traffic detection. Network security is becoming increasingly important every day as the digital world develops. It aims to classify the data labeled as benign and malicious in the ready dataset. In the proposed model, first of all, all the information in the dataset is digitized. Then, it is normalized to the range of 0-1 and made ready as an input to the proposed architecture. It is aimed to classify the information in this two-class dataset with the proposed Residual Convolutional Neural Network (CNN) architecture. The accuracy rate obtained after the training and testing stages of the model is 94.9%. This accuracy rate shows that the proposed model successfully results in the detection of malicious packets in network attacks and can be used for network security.

Keywords: Network security, Residual CNN, Malicious packet detection, Classification.

1 INTRODUCTION

The development of Internet networks brings many problems along with the increasing communication methods provided over these networks. Security threats for individuals, institutions, and states are reaching serious dimensions with the increasing digitalization. The basic problems of computer networks include secure transfer, data protection, and performance.

Computer networks contain many communication devices. The most basic of these devices are routers [1], switches [2], and personal use devices. The most undesirable situation is for attackers to connect to computer networks and launch attacks.

Information security is important for individuals' privacy, protection of their private information and feeling safe, while it is of great importance for states in terms of national security, strategic information and protection of critical infrastructures. Ensuring data security is based on confidentiality, integrity and accessibility. Confidentiality is possible only by guaranteeing access to authorized persons. Data integrity is possible by guaranteeing its originality and proving that it has not been changed by unauthorized persons. Ensuring access at the desired time and speed is also among the important elements. Violation of these rules can cause great material and moral losses and security gaps. The development, expansion and widespread use of networks bring about an increase in attacks. These attacks are carried out for reasons such as stopping system operations, stealing information and preventing communication. The types of attacks are given in Table 1. Distributed Denial of Service (DDoS) attacks are attacks carried out to render networks inoperable by creating high network traffic [3]. Man-in-the-Middle (MitM) attacks are attacks carried out to secretly capture, monitor or change the communication of two parties in communication [4]. Phishing Attacks are attacks that are created by sharing misleading information and documents to deceive people and steal their personal information [5]. In attacks made with SQL Injections, the attacker adds unauthorized and malicious SQL query codes to the codes and attacks are made to access the database [6]. The aim is to seize the system and obtain information.

Table 1. Network attack types and characteristics.

Attack Types	**Features**
DDoS	It sends high traffic to the network from many sources, making services unavailable.
MitM	It is a way of intercepting the communication between two parties and monitoring and changing the information.
Phishing Attacks	It means obtaining personal information by misleading users.
SQL Injections	It is done to gain unauthorized access to the database with malicious SQL codes.

Data packets on the network are the primary targets for attackers. In case of a security breach, attacks such as packet sniffing, packet forwarding, packet replay and packet poisoning are carried out. These attacks generally monitor network traffic, collect sensitive information, unencrypted information is easily captured, network traffic is directed to the wrong place, data packets can be sent repeatedly to deceive the system and malicious network packets can be added to manipulate the system and disrupt its operation. All these attacks reveal the importance of network security. Detection of attacks is possible both by conscious users and by developing intelligent systems. When the studies on computer networks and attack types and their detection are examined, it is seen that many detection studies have been carried out with machine learning methods. When the detection studies for DDoS attacks are examined, it is seen that while Support Vector Machines (SVM) architecture is used for detection [3], [7], [8], [9], deep learning architectures are used for detection in CNN models [10], [11], [12], [13], [14]. Again, in the detection studies conducted for MitM attacks, it is seen that SVM [15], K-Nearest Neighbors (KNN) [16] and CNN [17] models are used and successful results are obtained. There are many studies in the literature on phishing attack detection and when these studies are examined, there are studies with different models of SVM [18], KNN [19] and CNN [20], [21] architectures. It is seen that machine learning methods are used in SQL injection attacks [6], [22], [23], [24], [25], [26]. It is seen that these studies have intensified in recent years and successful results are obtained. In this study, a study is made on determining whether the packets transmitted during communication in a network traffic are secure.

There are studies on the subject in the literature. Shombot et al., in their study to predict phishing attacks, created a graphical user interface to detect whether websites are phishing or not. They conducted experiments with different machine learning methods in the study. After the preprocessing steps, the highest accuracy of 84% was achieved in the polynomial SVM classifier [18].

Irsan et al. used a dataset consisting of 10,000 data for phishing detection. In this study, they compared KNN and decision trees. Data preprocessing was first done in the study, and then models were trained and tested. They stated that the KNN classifier (accuracy %95) was more successful than decision trees (accuracy %93) in the dataset used for phishing detection [19].

Bezkorovalnyi et al. stated that they analyzed modern methods to detect phishing emails. The study highlighted that deep learning models can extract valuable features without applying a preprocessing step to the data. In this study, the advantages and disadvantages of different methods are included [20].

Gupta et al. stated that information security and privacy caused by phishing attacks pose a serious risk. In the relevant study, they used the Cuckoo Search algorithm to adjust the hyperparameters of the proposed CNN model. The accuracy value obtained in this study was 90%. In this paper, hyperparameter optimization comes to the fore [21].

Kocyigit et al. used genetic algorithms and classifiers for phishing detection. The selection of important features was performed using genetic algorithms. Different ablation results were included in the study. When the features selected using genetic algorithms were classified in the classifiers, the highest success was achieved with 92.93% in the Random Forest classifier [27].

Mankar et al. emphasized that malicious URLs cause significant financial losses. Four different models were used in the study. At the end of the study, they stated that decision trees and random forest models achieved an accuracy rate of 91%. This study obtained lower accuracy values in KNN and Naive Bayes models [28].

A deep learning based model is proposed in the study. The proposed deep learning model is a model with residual connections and is a new approach to classifying packets in the network. The formalization processes performed from the dataset also include innovation in digitizing the data received in the network. The digitization and normalization of both the texts in the data and the information in all other columns, including IP addresses, ensures that all parameters in the network are taken into account in the classification phase.

In this study, the details of the dataset used are given in section 2. In addition, the details about the proposed method and all the success metrics used are included in this section. In section 3, examples from the units in the used dataset are given, and then the confusion metric and performance metrics showing the results of the proposed model are given. In the last section, the evaluations and results are interpreted, and suggestions for the future are made.

2 SYSTEM THEORY

2.1 Dataset

Data packets in computer networks can be modified by attackers and made harmful. Distinguishing and filtering these malicious and normal packets from each other is of great importance in terms of information and network security. In the dataset prepared for this purpose by Saadoon and Behadili (2024) [29], the transmitted data packets are recorded in two classes as benign and malicious. 9 features are kept for each packet in the dataset. These features are Protocol(P), remote_ip(Ri), remote_port(Rp), local_ip(Li), local_port(Lp), md5_hash(Mh), sha512_hash(Sh), Length(L) and data_hex(Dh). Malicious network dataset features are given in Figure 1. In order to obtain these features, they collected the packets using the honey trap method placed with Honeytrap in the system they created.

The features used for the dataset are protocols used in network communication such as Protocol Hyper-Text Transfer Protocol (HTTP), File Transfer Protocol (FTP) or Secure Shell (SSH). remote_ip is the IP address of the system from which the remote connection is initiated (attacker) and remote_port is the port number of the same system. local_ip is the IP address of the local system and the port of this system is called local_port. md5_hash is the payload hash used to both identify and compare files and data. sha512_hash is the SHA-512 hash obtained for the payload and is kept as a secure identification for the file and data. Length represents the length of the payload in bytes. data_hex is the hexadecimal representation of the raw payload.

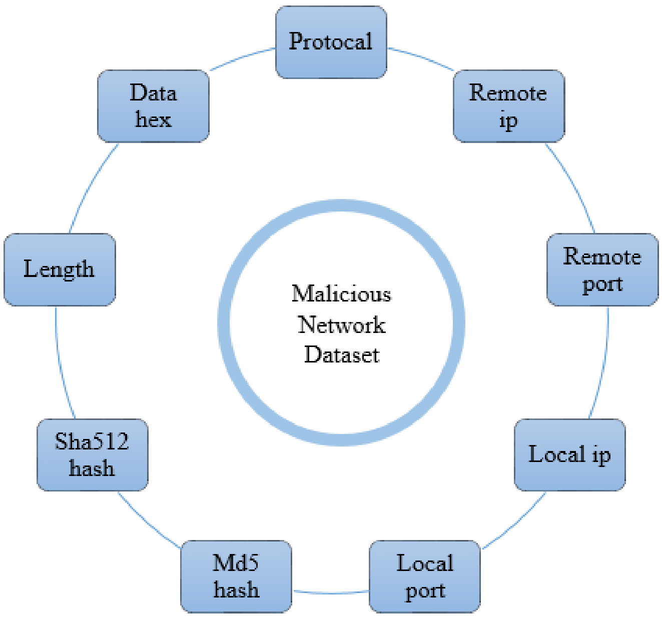

Figure1. Malicious network dataset features.

2.2 The proposed method

The use of artificial intelligence methods to detect attacks on computer networks is important in terms of ensuring the security and automation of systems. Residual networks allow deeper networks to be trained efficiently by reducing the vanishing gradient problem encountered in the training of deep neural networks. While traditional deep networks may experience a learning process hindered by the vanishing gradients as the network gets deeper, skip connections alleviate this problem and facilitate the gradient flow during backpropagation. This structure improves training by accelerating learning and allowing deep networks to generalize better. Residual blocks preserve parameter efficiency and increase accuracy rates without increasing the depth of the model using identity mapping. The general structure of the residual CNN-based model developed for the classification of data in the dataset is given in Figure 2. In the proposed model, a ready-made dataset is used first. Transformation and normalization processes are applied to bring the features in this dataset to a usable format in the deep learning model.

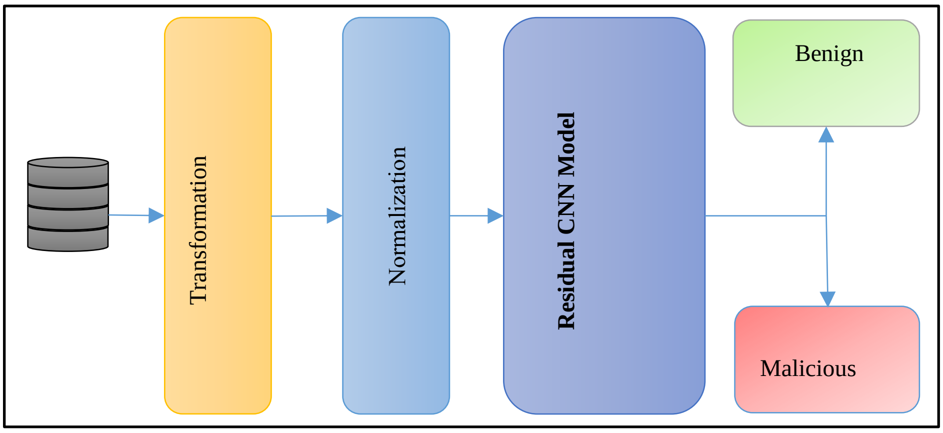

Figure 2. The proposed method.

In the transformation step, firstly the hash and hex properties are analyzed. The formulas used for these analyses are given in Equations 1, 2, and 3.

$$Total_{hash} = \begin{cases} \sum_{i=1}^{n} ord(c_i), & if\ x\ is\ a\ string \\ 0\,, & otherwise \end{cases} \tag{1}$$

In Equation 1, x represents a hash string, n represents the length of the string, c_i represents the ith character of the string, and ord calculates the ASCII value of the given character.

$$Total_{hex} = \begin{cases} \sum_{i=1}^{n} int(x[i\colon i+2], 16), & if\ x\ is\ a\ string \\ 0\,, & otherwise \end{cases} \tag{2}$$

In Equation 3, x represents a hex string, n represents the total number of binary in the hexadecimal string, $i\colon i+2$ represents the ith 2-character group of the string, $int(x[2i-2\colon 2i]$,16) calculates the decimal equivalent of the 16 data.

$$Mean_{hex} = \begin{cases} \dfrac{\sum_{i=1}^{n} int(x[i\colon i+2], 16)}{n}, & if\ x\ is\ a\ string\ and\ n > 0 \\ 0\,, & otherwise \end{cases} \tag{3}$$

Equation 4 is used to convert IP addresses into numerical form.

$$Num_{IP} = (o_1 \cdot 256^3) + (o_2 \cdot 256^2) + (o_3 \cdot 256^1) + (o_4 \cdot 256^0) \tag{4}$$

The Equation 4 calculates the numerical equivalent of the IP address and represents each octet of those values. Then, the normalization step is started. In the normalization step, the values are normalized to the range of 0-1 using Equation 5.

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{5}$$

In Equation 5, x is the data point to be normalized, x_{min} is the smallest value of the dataset, x_{max} is the largest value of the dataset, and x' is the normalized value. After this stage, the data is divided and given as input to the residual CNN model. The normalized dataset is divided into two parts as training and testing. While 80% of the data is separated for training, 20% of the data is separated for testing.

The residual CNN architecture is created and the data classification step is passed. In this step, first the architecture is designed in a way that the One-dimensional Convolution Layer (Conv1D) process will be applied. Then the maxpooling step is performed and then the residual connection is added in the dropout step. With this connection, a shortcut is created and the dropout and Conv1D steps are combined. This step is usually added to accelerate learning and reduce gradient loss problems. The Residual CNN architecture created for the proposed model is given in Figure 3. The model parameters were determined as learning rate 0.001, epoch number was used as 100 and batch size was used as 32. Adam was also preferred as the optimization algorithm.

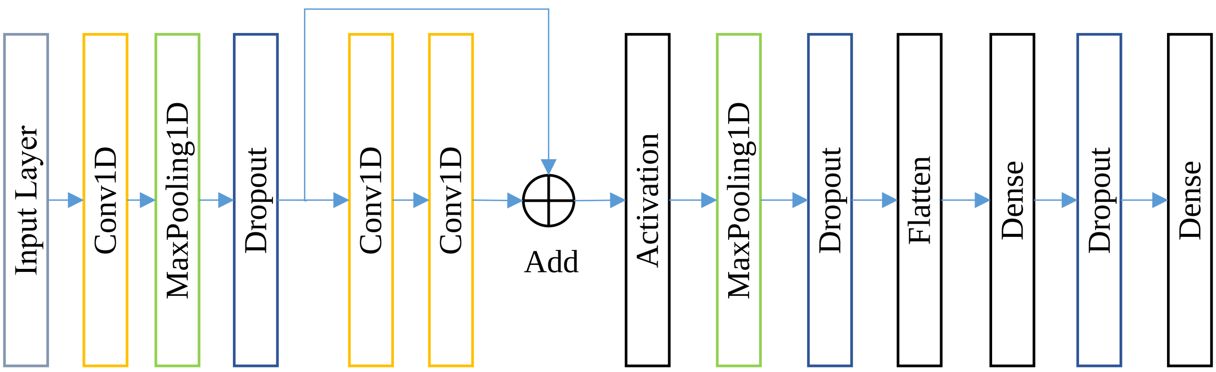

Figure3. Structure of the Residual CNN model.

Table 2. Performance metrics.

Performance Metric	**Formula**
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$
Precision	$\frac{TP}{TP + FP}$
Recall	$\frac{TP}{TP + FN}$
Specificity	$\frac{TN}{TN + FP}$
F1-Score	$2 \cdot \frac{(\text{Precission} \cdot \text{Recall})}{(\text{Precission} + \text{Recall})}$
MCC	$\frac{(TP \cdot TN) - (FP \cdot FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$
Balanced Accuracy	$\frac{\text{Recall(Sensitivity)} + \text{Specificity}}{2}$

The success of the studies is possible with the analysis of the classification results. With these analyses, performance metrics are calculated, and the rate of correct predictions of the model, the rates of incorrect and missing classifications are determined. Thus, the working accuracies for different classes can be determined. Performance metrics are calculated with the values of TP (True Positive), TN (True Negative), FP (False Positive), FN (False Negative). In addition to the basic criteria Accuracy, Precision and Recall, the imbalance between classes is determined with Specificity. In addition, criteria such as Balanced Accuracy and MCC (Matthews Correlation Coefficient) are used in performance analysis. The calculation methods of these performance metrics are given in Table 2.

3 EXPERIMENTAL RESULTS

The malicious network dataset consists of a total of 27978 records. Half of these records contain malicious data and the other half contain benign data. Some records in the dataset are given in Table 3.

The data in the table first passes through the transformation step and all the data is calculated as numerical values. Sums and averages are calculated for Hash and Hex values. Digitization operations are performed for IP addresses. After the digitization step is completed, the normalization step is passed and all digitized data is normalized to the 0-1 range. After this step, the preprocessed data were classified using four different classifiers accepted in the literature to compare the proposed model's performance. These models are KNN, SVM, Naive

Bayes (NB) [30], and Logistic Regression (LR) [31]. In the confusion matrix, 0 represents Benign data, while 1 represents Malicious data. The confusion matrices obtained from these classifiers are presented in Figure 4

Table 3. Some data from dataset.

P	Ri	Rp	Li	Lp	Mh	Sh	L	Dh	Class
tcp	80.75.212.9	42196	165.227.180.71	8697	f7f3a1 b1a764 82b3d2 e3b5b5 b06f07 2a	82e7da3fa6cbd0c bc51670637a99b8 701a974c9723515 fb146c36acd05cc a8527e7019a2030 426cfcc150a6b50 de92753efa159fb 978e29ca570a25f ecc23586	105	434f4e4e454354207777772e676f6f676c652e636f6 d3a343433204854545 02f312e310d0a486f73743a2 07777772e676f6f676c652e636f6d0d0a557365722d 4167656e743a204d6f7a696c6c612f352e300d0a436 f6e6e656374696f6e3a20636c6f73650d0a0d0a	benign
tcp	192.155.90.220	62806	165.227.180.71	8098	4643f0 885b73 3a87ca 767467 4d4bfe d5	a1893f0d5155e3e 6e5dbda0c0afa2c b20666d0fb14791 3e927b50b75c4af 9ab74db54d05083 f5a89023a93868f 87a8f1721c16838 044382003f0792d a9f08a2a	239	16030100ea010000e60303c11726e29b15ca160dc1 39358664ae3a462be91f05a769ed31afb2284195033 f20d34616321b8909d6bc0043975afee318ba161c3 3c3d63b1ae9f4f23d5289c1790026c02bc02fc02cc0 30cca9cca8c009c013c00ac014009c009d002f0035c 012000a130113021303010000770005000501000 0 0000000a000a0008001d00170018001900 0b00020 100000d001a0018080404030807080508060401 05 01060105030603020102 03ff010001000012000000 2b0005040304030300330026002400 1d0020de063 782f7afd56a605fceb4c3f52f82af9ee40d9af817ee15 ed5b700c6f4c22	malicious

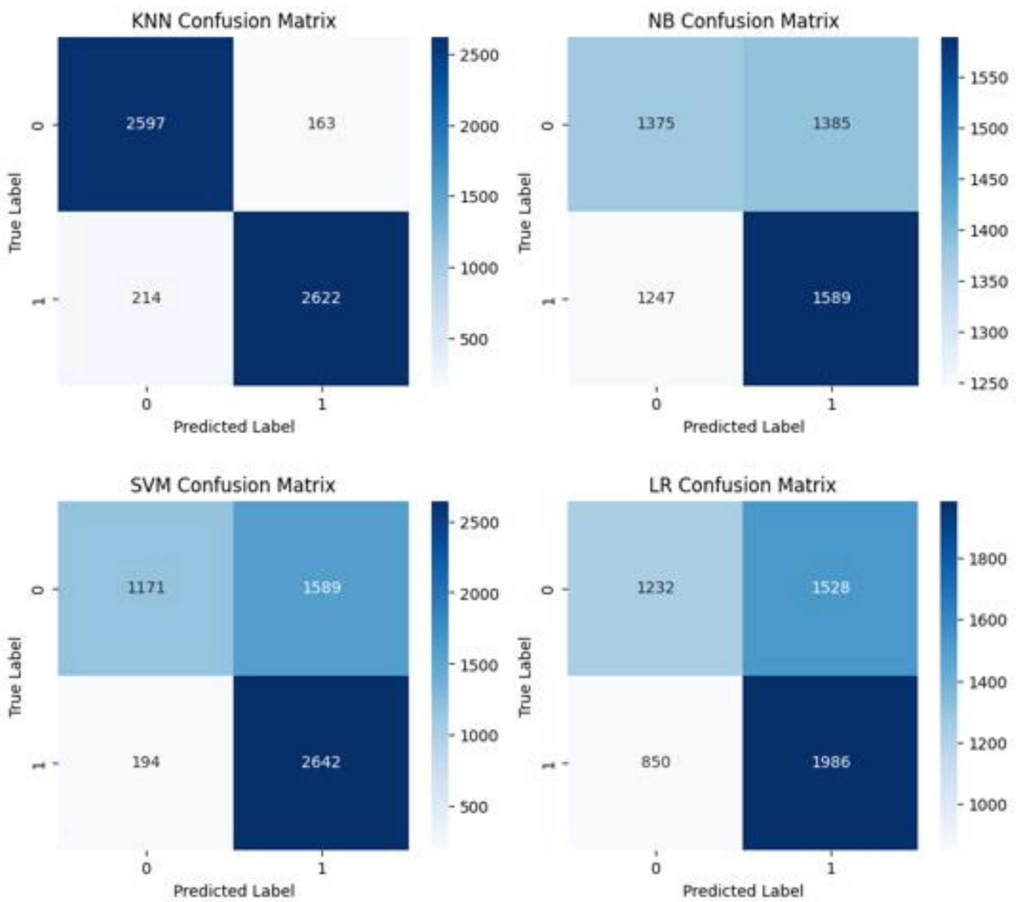

Figure 4. Confusion matrix of Classifiers.

When the confusion matrices presented in Figure 4 are examined, it is seen that the most successful classifier is KNN. The values that the KNN classifier incorrectly predicted are close to each other. The KNN classifier predicted 163 images belonging to the benign class as malicious. It predicted 214 images belonging to the malicious class as benign. It is undesirable for false negative values to be high. Because the model predicts the malicious data as benign.

After this step, the model is trained for classification by entering 100 epochs and 32 batch size values with the Residual CNN model. 80% of the dataset is used for training. The training accuracy obtained after the training of the model is 94.57%. Then, the test step of the model is performed with the test data. The remaining 20% of the data is used at this stage. The test accuracy is calculated as 94.9%.

The confusion matrix of the proposed model is given in Figure 5. In the confusion matrix, 0 represents Benign data, while 1 represents Malicious data. When the values in the confusion matrix are examined, it is seen that the Benign correct detection rate TN is recognized with a high value of 2592 and the FP with a relatively low value of 168. Similarly, while the Malicious correct prediction TP has a high value of 2717, it is seen that the FN has a low value of 119. When the confusion matrices of the classifiers accepted in the literature are examined in Figure 5, it is seen that the FN value is 214 in the KNN classifier, 1247 in NB, 194 in SVM, and 850 in LR. In the proposed model, this value is 119. The FN value in the proposed model is much lower than that of others.

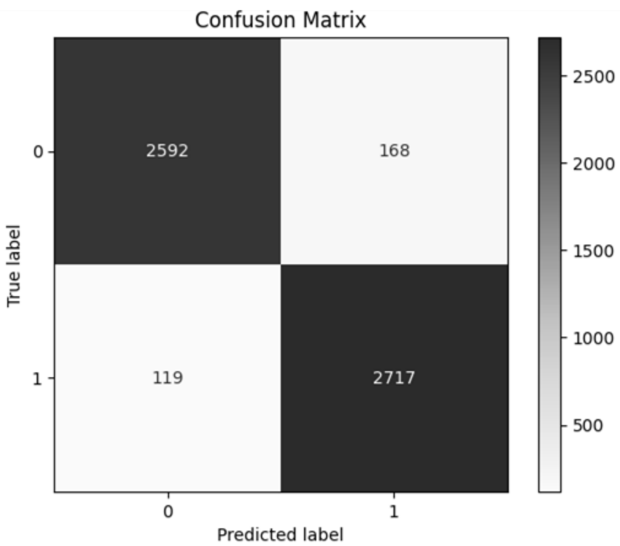

Figure 5. Confusion matrix of Proposed Model

As a result of all these evaluations, it is seen that the proposed model has a high rate of correct prediction in both classes and exhibits a good performance. While the FP and FN rates support the good performance of the model in the low probability, it also increases the general accuracy of the model and the Balanced Accuracy and Specificity values, which are the balance indicators between the classes, by increasing the indicators such as Precision and Recall. Table 4 provides the performance metrics of the models used to obtain the application results in the study.

Table 4. Performance metrics of models (%).

	Accuracy	**Precision**	**Recall**	**Specificity**	**F1**	**MCC**	**Balanced Accuracy**
KNN	93.26	93.27	93.26	94.09	93.26	0.86	93.27
NB	52.97	52.94	52.97	49.82	52.92	0.06	52.92
SVM	68.14	73.96	68.14	42.43	65.90	0.41	67.79
LR	57.51	57.83	57.51	44.64	56.80	0.15	57.33
Proposed Model	94.90	94.20	95.80	93.90	95.00	0.90	94.90

When Table 4 is examined, it is seen that the highest accuracy value of 94.90% is obtained in our proposed Residual CNN model. This is predicted by KNN, SVM, LR, and NB classifiers, respectively.

4 CONCLUSION

Thanks to the spread of internet networks and digitalization, information security and privacy issues have come to the forefront, and attacks to seize or damage this information are increasing daily. Detection and prevention of these attacks will prevent possible material and moral losses. For this purpose, classification was performed with a ready-made dataset belonging to the MitM attack type in this study. The data was first transformed and digitized in the study, and normalization was applied. After these processes, the developed Residual CNN architecture performed the classification process. It is seen that the packets were correctly classified with a 94.9% accuracy rate in the classification step. This study reveals that the Residual CNN architecture, which is a deep learning method in the detecting network attacks, detects malicious packets with a high accuracy rate and can be used for network security. In this way, it is seen that good points will be reached in terms of protecting network security and data integrity by utilizing deep learning architectures to prevent data loss, material losses, and personal information theft.

Conflict of Interest Statement

There is no conflict of interest between the authors.

Statement of Research and Publication Ethics

The study is complied with research and publication ethics.

Artificial Intelligence (AI) Contribution Statement

This manuscript was entirely written, edited, analyzed, and prepared without the assistance of any artificial intelligence (AI) tools. All content, including text, data analysis, and figures, was solely generated by the authors.

Contributions of the Authors

Mücahit Karaduman contributed to the experimental studies, data interpretation, and the preparation of the manuscript. Sercan Yalçın contributed to the experimental studies and the preparation of the manuscript. Muhammed Yıldırım contributed to the experimental studies.

REFERENCES

[1] Aweya J. IP router architectures: an overview. Int. J. Commun. Syst. 2001; 14(5); 447–475.

[2] Femenias G, Lassoued N, Riera-Palou F. Access point switch ON/OFF strategies for green cell-free massive MIMO networking. IEEE access 2020; 8: 21788–21803.

[3] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput. Commun. Rev. 2004, 34(2): 39–53.

[4] Pingle B, Mairaj A, Javaid A Y. Real-world man-in-the-middle (MITM) attack implementation using open source tools for instructional use. in 2018 IEEE International Conference on Electro/Information Technology (EIT), 2018, pp. 192–197.

[5] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *2016 international conference on computing, communication and automation (ICCCA)*, 2016, pp. 537–540.

[6] R. Rawat and S. K. Shrivastav, "SQL injection attack detection using SVM," *Int. J. Comput. Appl.*, vol. 42, no. 13, pp. 1–4, 2012.

[7] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," *Expert Syst. Appl.*, vol. 34, no. 3, pp. 1659–1665, 2008.

[8] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software defined network," *Secur. Commun. Networks*, vol. 2018, no. 1, p. 9804061, 2018.

[9] U. Ince and G. Karaduman, "Classification of Distributed Denial of Service Attacks Using Machine Learning Methods," *NATURENGS*, vol. 5, no. 1, pp. 15–20, 2024.

[10] M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison," *Bull. Electr. Eng. Informatics*, vol. 12, no. 2, pp. 930–939, 2023.

[11] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via Convolutional Neural Network (CNN)," in *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, 2019, pp. 233–238.

[12] A. A. Najar, M. N. Sugali, F. R. Lone, and A. Nazir, "A novel CNN-based approach for detection and classification of DDoS attacks," *Concurr. Comput. Pract. Exp.*, vol. 36, no. 19, p. e8157, 2024.

[13] A. A. Najar and S. M. Naik, "Cyber-secure SDN: A CNN-based approach for efficient detection and mitigation of DDoS attacks," *Comput. \& Secur.*, vol. 139, p. 103716, 2024.

[14] C. Padmavathy *et al.*, "1D CNN Based Model for Detection of DDoS Attack," in *2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*, 2024, pp. 1–6.

[15] A. Kumar, I. Sharma, S. Mittal, and others, "Enhancing Security through a Machine Learning Approach to Mitigate Man-in-the-Middle Attacks," in *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, 2024, pp. 1–6.

[16] K. V. Rao, B. R. Akshaya, G. G. Satvik, B. Rohith, and G. C. B. Lahari, "Machine Learning based Man-in-the-Middle Attack Prediction," in *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2024, pp. 1393–1399.

[17] M. Iddrisu, K. Takyi, R.-M. O. M. Gyening, K. O. Peasah, L. A. Banning, and K. Owusu-Agyemang, "An improved man-in-the-middle (MITM) attack detections using convolutional neural networks," *Multidiscip. Sci. J.*, vol. 7, no. 3, p. 2025129, 2025.

[18] E. S. Shombot, G. Dusserre, R. Bestak, and N. B. Ahmed, "An application for predicting phishing attacks: A case of implementing a support vector machine learning model," *Cyber Secur. Appl.*, vol. 2, p. 100036, 2024.

[19] M. Irsan, F. Febriana, H. H. Nuha, and H. R. P. Sailellah, "Phishing Detection on URL Data Using K-Nearest Neighbors Method," in *2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2024, pp. 792–797.

[20] P. R. Uyyala, "Phishing email detection using CNN," *J. Eng. Technol. Manag.*, vol. 72, pp. 1046–1051, 2024.

[21] B. B. Gupta, A. Gaurav, R. W. Attar, and V. Arya, "A Novel Cuckoo Search-Based Optimized Deep CNN Model for Phishing Attack Detection in IoT Environment," 2024.

[22] R. D. N. Shakya, D. N. S. Dharmaratne, and M. Sandirigama, "Detection of SQL Injection Attacks Using Machine Learning Techniques," in *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, 2024, pp. 1–6.

[23] H. C. Altunay, "Detection of SQL Injection Attacks Using Machine Learning Algorithms Based on NLP-Based Feature Extraction," in *2024 9th International Conference on Computer Science and Engineering (UBMK)*, 2024, pp. 468–472.

[24] M. Thilakraj, S. Anupriya, M. M. Cibi, and A. Divya, "Detection of SQL Injection Attacks," in *2024 International Conference on Inventive Computation Technologies (ICICT)*, 2024, pp. 1515–1520.

[25] W. Zhao, J. You, and Q. Chen, "SQL Injection Attack Detection Based on Text-CNN," in *Proceedings of the 2024 International Conference on Generative Artificial Intelligence and Information Security*, 2024, pp. 292–296.

[26] M. Shahbaz, G. Mumtaz, S. Zubair, and M. Rehman, "Evaluating CNN Effectiveness in SQL Injection Attack Detection," *J. Comput. \& Biomed. Informatics*, vol. 7, no. 02, 2024.

[27] Kocyigit, E., Korkmaz, M., Sahingoz, O. K., & Diri, B. (2024). Enhanced feature selection using genetic algorithm for machine-learning-based phishing URL detection. Applied sciences, 14(14), 6081.

[28] Mankar, N. P., Sakunde, P. E., Zurange, S., Date, A., Borate, V., & Mali, Y. K. (2024, April). Comparative Evaluation of Machine Learning Models for Malicious URL Detection. In 2024 MIT Art, Design and Technology School of Computing International Conference (MITADTSoCiCon) (pp. 1-7). IEEE.

[29] M. S. Saadoon and S. F. Behadili, "Malicious network dataset," 2024, *Zenodo*. doi: 10.5281/ZENODO.14559922.

[30] Kohavi, R. (1996, August). Scaling up the accuracy of naive-bayes classifiers: A decision-tree hybrid. In Kdd (Vol. 96, pp. 202-207).

[31] Hosmer Jr, D. W., Lemeshow, S., & Sturdivant, R. X. (2013). Applied logistic regression. John Wiley & Sons.