Artificial Neural Network for Binary and Multiclassification of Network Attacks

Bauyrzhan Omarov[1], Alma Kostangeldinova[2], Lyailya Tukenova[3], Gulsara Mambetaliyeva[4], Almira Madiyarova[5], Beibut Amirgaliyev[6], Bakhytzhan Kulambayev[7]
Al-Farabi Kazakh National University, Almaty, Kazakhstan[1]
Kokshetau University Named after. Sh. Ualijhanov, Kokshetau, Kazakhstan[2]
Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan[3]
Yessenov University, Aktau, Kazakhstan[4, 5]
Astana IT University, Astana, Kazakhstan[6]
International Information Technology University, Almaty, Kazakhstan[7]

***Abstract*—Diving into the complex realm of network security, the research paper investigates the potential of leveraging artificial neural networks (ANNs) to identify and classify network intrusions. Balancing two distinct paradigms – binary and multiclassification – the study breaks fresh ground in this intricate field. Binary classification takes the stage initially, offering a bifurcated outlook: network traffic is either under attack, or it's not. This lays the foundation for an intuitive understanding of the network landscape. Then, the spotlight shifts to the finer-grained multiclassification, navigating through a realm that holds five unique classes: Normal traffic, DoS (Denial of Service), Probe, Privilege, and Access attacks. Each class serves a specific function, ranging from harmless communication (Normal) to various degrees and kinds of malicious intrusion. By integrating these two approaches, the research illuminates a path towards a more comprehensive understanding of network attack scenarios. It highlights the role of ANNs in enhancing the precision of network intrusion detection systems, contributing to the broader field of cybersecurity. The findings underline the potency of ANNs, offering fresh insights into their application and raising questions that promise to push the frontiers of cybersecurity research even further.**

***Keywords*—Neural networks; artificial intelligence; detection; classification; attacks; network security**

I. Introduction

In the rapidly evolving digital landscape, the detection and classification of network attacks have become a paramount concern for organizations globally [1]. The introduction of Artificial Neural Networks (ANNs) has ushered in a new era of possibilities in handling this concern, providing robust and adaptive solutions to complex cybersecurity challenges [2]. This research paper, "Artificial Neural Network for Binary and Multiclassification of Network Attacks," delves into these possibilities, exploring how ANNs can be employed to enhance the detection and classification of network attacks.

Network intrusions have been traditionally identified and classified using a binary approach: there is either an attack or there isn't [3]. This approach offers a straightforward, binary perspective on network traffic, facilitating a basic yet vital understanding of network security. However, as the complexity of network attacks has grown exponentially, the need for a more nuanced understanding has become evident under the realm of multiclassification [4].

Through a multiclassification approach, network traffic can be categorized into multiple classes, enabling a more detailed analysis. In this research, five distinct classes are identified: Normal traffic, and four types of attacks – DoS (Denial of Service), Probe, Privilege, and Access. By scrutinizing the individual characteristics of each class, we are able to discern not just the presence of an attack, but also its nature and potential impact. This level of detail provides a much-needed edge in defending against, and responding to, network intrusions.

A pivotal tool in enabling this detailed classification is the Artificial Neural Network. Mimicking the learning process of the human brain, ANNs are capable of learning from experience, improving their performance as they are exposed to more data [5]. This inherent adaptability makes them highly effective in identifying the subtle patterns that differentiate one class of network traffic from another.

In our exploration of ANNs for network attack classification, we will delve into their structure, function, and application, providing a comprehensive understanding of their role in cybersecurity. The research includes a detailed discussion on the various types of ANNs, their learning algorithms, and how they can be trained to accurately classify network traffic.

Moreover, the study will also address the challenges faced when applying ANNs to real-world scenarios, shedding light on the obstacles that need to be overcome for this technology to reach its full potential [6]. By exploring both the strengths and weaknesses of ANNs in network attack classification, this research aims to provide a balanced view of their utility in this crucial area.

II. Related Works

The field of cybersecurity, particularly the detection and classification of network attacks, has been extensively researched, and this paper builds on a number of prior works, each contributing to our understanding of this complex landscape [7]. As the focus of our paper is on utilizing Artificial Neural Networks (ANNs) for binary and

multiclassification of network attacks, we will delve into studies that lay the groundwork for our investigation.

In a recent study, authors provided a seminal investigation into the use of deep learning methods for network intrusion detection [8]. They used ANNs to detect intrusions in a Software-Defined Networking (SDN) environment, providing a comprehensive framework that offers insights into the structure and operation of ANNs in a network intrusion detection context.

Building on this, next research shifted the focus from SDN to traditional network environments [9]. Their research exemplified the use of ANNs in binary classification, identifying whether a network event is an attack or normal traffic. The application of fuzzy clustering, in tandem with ANNs, accentuated the ability of the system to handle ambiguous scenarios that reside in the gray area between 'attack' and 'normal traffic'.

Taking it a step further, authors [10] introduced multiclassification into the mix. The study classified network attacks into four categories - DoS, Probe, Privilege, and Access, providing a more nuanced understanding of network intrusions. The authors highlighted the advantages of multiclassification, offering a model that can inform more targeted responses to different types of attacks.

While these studies focused on the application of ANNs in network intrusion detection and classification, research by [11] titled "Challenges and Future Directions in the Deployment of Neural Network Models in Cybersecurity," explored the hurdles in applying these models in real-world scenarios. They identified issues such as overfitting, the difficulty of interpretability, and data scarcity, among others. This research provides essential context, informing us of the potential roadblocks that could hinder the effective deployment of ANNs in network intrusion detection and classification.

A notable study by [11] titled "Application of Deep Learning to Detect Intrusion in 5G and IoT Networks" introduced the concept of utilizing ANNs in the context of 5G and IoT networks. They highlighted the increasing complexity of intrusion detection due to the significant growth of IoT devices and the transition to 5G. Their exploration of the effectiveness of ANNs in this relatively new network environment laid the groundwork for future research in more complex network infrastructures.

Furthermore, the research by [12] significantly contributed to our understanding of multiclassification. They took a unique approach of extending binary classification to multiclassification, investigating how ANNs can distinguish between different types of attacks within a network. Their work presented important insights into the potential and challenges of employing multiclassification in intrusion detection systems.

Deep Neural Networks for Multiclass Detection of Distributed Denial of Service Attacks took a narrower focus, concentrating solely on the detection of different types of DDoS attacks [13]. Their research provided valuable insights into the specialized application of ANNs for detecting and classifying a specific type of network attack.

Next study by [14] presents an overview of machine learning algorithms in improving the precision of network intrusion detection systems. Their study, while not exclusive to ANNs, illuminates the broader context within which our research is situated, showcasing the potential of machine learning in this field.

Taken together, these studies demonstrate the evolution of applying ANNs in the field of network intrusion detection and classification, and highlight the significant progress that has been made. They provide us with a broader context for our own research, enabling us to both build upon their insights and address the gaps in existing knowledge. Our research aims to consolidate these findings and contribute to a more nuanced understanding of how ANNs can be employed effectively in both binary and multiclassification of network attacks.

Our study, seeks to build on these existing studies. It aims to further the understanding of how ANNs can be effectively utilized for network attack detection and classification, and how potential hurdles can be surmounted for real-world deployment. By taking into account the insights and challenges highlighted by these previous studies, we hope to make a significant contribution to the ongoing discourse in this vital field of research.

III. DATASET

In this research, the NSL-KDD dataset is applied to train and test artificial neural network in order to detect attacks [15]. The NSL-KDD dataset, a benchmark dataset in the field of cybersecurity, serves as the data foundation for our research paper, "Artificial Neural Network for Binary and Multiclassification of Network Attacks." This dataset is an improved and refined version of the widely-known KDD'99 dataset, addressing the inherent limitations of its predecessor such as redundant records leading to learning bias.

NSL-KDD is comprised of a rich collection of simulated network traffic instances containing both normal and malicious events, enabling comprehensive training and testing of our Artificial Neural Network (ANN) models. The dataset holds an extensive variety of intrusions simulated in a military network environment, making it well-suited for studying intricate network intrusion detection scenarios.

The NSL-KDD dataset contains around 125,000 records in the training set and about 22,500 records in the testing set. Each record within the dataset represents a connection and contains 41 features, which describe various aspects of the connection like duration, protocol type, service type, and various other content features extracted from the payload. The diversity of these features allows the ANN to learn from a wide array of indicators, potentially boosting the model's overall detection accuracy. Fig. 1 demonstrates percentages of normal and attack classes.

Importantly, each record in the dataset is labeled as either 'normal' or as one of the four defined types of attacks: denial of service (DoS), Probe, Privilege, and Access. These labels are instrumental in both binary and multiclassification approaches, facilitating the training of the ANN to not only identify the presence of an attack but also classify the attack into one of these specific categories.

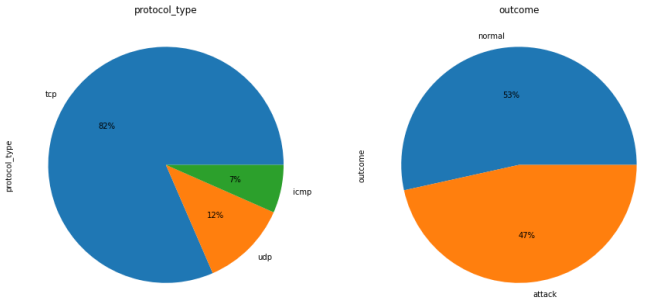

Fig. 1. Distribution of protocols in the NSL-KDD dataset.

Fig. 2 demonstrates flags of each class as normal and attack classes. In network communication, flags are employed to indicate the status of a certain connection, or to signal various types of events or errors. These flags can serve as powerful indicators of anomalous or malicious behavior in network traffic; hence their distribution across the different classes is of significant interest.

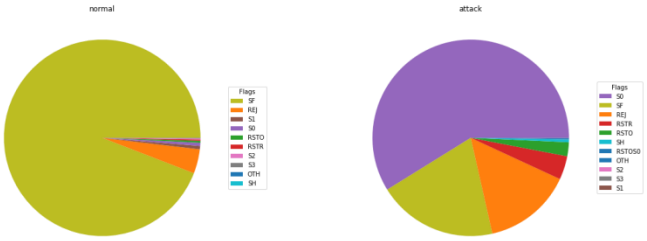

Fig. 2. Distribution of normal and attack flags in NSL-KDD dataset.

In summary, the NSL-KDD dataset, with its diversity and comprehensive representation of both normal and attack instances, provides a robust platform for the development and evaluation of ANN models in our research. The findings drawn from this dataset can contribute significantly to our understanding of network intrusions and the application of ANNs in detecting and classifying these attacks.

IV. Proposed Artificial Neural Network for Network Attacks Detection

The proposed Artificial Neural Network (ANN) model for the study is based on a sequential model, which is a linear stack of layers. This model is designed to process the NSL-KDD dataset and classify network traffic into five categories: normal traffic or one of four attack types – DoS, Probe, Privilege, and Access. Architecture of the proposed model is illustrated in Fig. 3.

The architecture of the model consists of multiple layers, each contributing to the learning capacity of the model. The first layer, dense_35, is a densely connected layer, also known as a fully connected layer. It consists of 64 nodes or neurons, and each neuron in this layer is connected to all neurons from the previous layer (input data). This layer has 5,632 parameters, which are the weights and biases that the model will learn during the training phase.

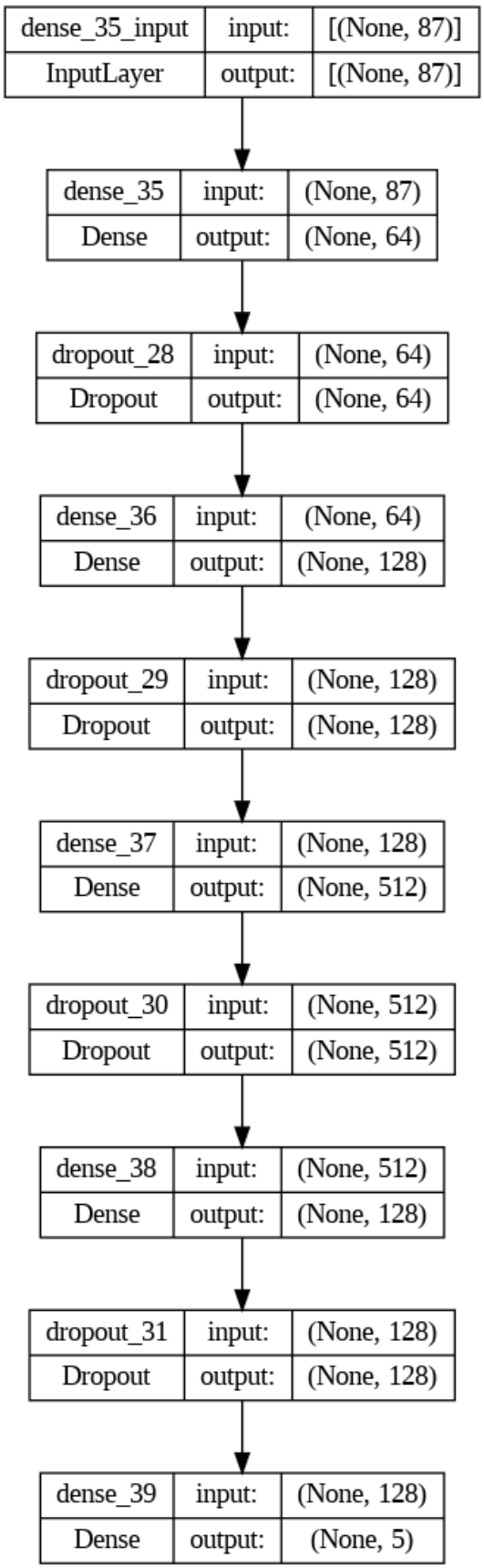

Fig. 3. The proposed neural network.

The architecture of the model consists of multiple layers, each contributing to the learning capacity of the model. The first layer, dense_35, is a densely connected layer, also known as a fully connected layer. It consists of 64 nodes or neurons, and each neuron in this layer is connected to all neurons from the previous layer (input data). This layer has 5,632 parameters, which are the weights and biases that the model will learn during the training phase.

Following dense_35 is dropout_28, a dropout layer designed to reduce overfitting. It randomly sets a fraction of input units to 0 during training, which helps prevent overfitting by ensuring that the model doesn't rely too heavily on any single input feature.

The model then proceeds to dense_36, another fully connected layer, but with 128 neurons. The number of parameters here is 8,320. The output of dense_36 is passed through another dropout layer, dropout_29, to prevent overfitting.

Next is dense_37, a significant layer with 512 neurons, having a much larger parameter count of 66,048. This layer is followed by dropout_30 to again avoid overfitting.

The model continues to dense_38, which is another fully connected layer with 128 neurons, consisting of 65,664 parameters. The output of this layer passes through the last dropout layer, dropout_31.

Finally, the output layer, dense_39, comprises five neurons corresponding to the five classes that our model aims to predict. This layer employs a softmax activation function to output a probability distribution over the five classes, indicating the likelihood of each class being the correct one. This final layer contains 645 parameters.

Overall, the proposed ANN model has a total of 146,309 parameters, all of which are trainable. The model's complexity and architecture make it capable of effectively learning to classify network traffic into the five defined classes.

V. Evaluation Parameters

In assessing the performance of our proposed Artificial Neural Network (ANN) model, it is vital to use appropriate evaluation parameters that reflect the model's capabilities in various aspects. The following metrics - Accuracy, Precision, Recall, F-Score, and receiver operating characteristics area under the curve (ROC-AUC) have been chosen due to their extensive use in classification tasks and their ability to provide a holistic view of the model's performance [16]. Next paragraphs explain each evaluation parameter that applied to assess the performance of the proposed model.

Accuracy: This is one of the most straightforward metrics, which essentially quantifies the ratio of correct predictions made by our model out of all predictions. While accuracy can provide a quick overview of model performance, it might not be an ideal metric when dealing with imbalanced datasets [17].

$$accuracy = \frac{TP + TN}{TP + FN + TN + FP} \quad (1)$$

1) Precision: Precision measures the proportion of true positives out of all positive predictions made by the model. It provides insight into how well the model correctly predicts an attack when it claims there is one. High precision indicates a lower rate of false positives [18].

$$precision = \frac{TP}{TP + FP} \quad (2)$$

2) Recall: Recall, or sensitivity, gauges the proportion of actual positive (attack) instances that the model correctly identifies. A high recall means that the model can accurately catch a high percentage of network attacks, minimizing the number of false negatives [19].

$$recall = \frac{TP}{TP + FN} \quad (3)$$

3) F-Score: The F-Score or F1-score is the harmonic mean of precision and recall. This metric provides a single score that balances both the precision and the recall. It is particularly useful when you want to compare two or more models and need a single performance score [20].

$$F1 = \frac{2 \cdot precision \cdot recall}{precision + recall} \quad (4)$$

4) ROC-AUC: The Receiver Operating Characteristic - Area Under Curve (ROC-AUC) is a performance measurement for binary classification problems [21]. It tells how much a model is capable of distinguishing between classes. The higher the AUC, the better the model is at predicting 0s as 0s and 1s as 1s. Each of these metrics provides unique insights into the model's capabilities, and together they offer a comprehensive assessment of the model's overall performance.

VI. Experimental Results

The Results section offers a comprehensive review of the performance of our proposed model. After rigorously training and testing our model using the NSL-KDD dataset, we have evaluated the performance using the defined metrics - Accuracy, Precision, Recall, F-Score, and ROC-AUC. This section presents an in-depth analysis of the findings, detailing how well our model can detect and classify network attacks.

A. Binary Classification of Network Attacks

Fig. 4 demonstrates confusion matrix of binary classification of network attacks. The model correctly identified 9490 instances of normal traffic (TN), and correctly classified 7342 instances of attack traffic (TP). However, the model inaccurately labeled 221 instances of normal traffic as attack traffic (FP), and 5490 instances of attack traffic as normal traffic (FN).

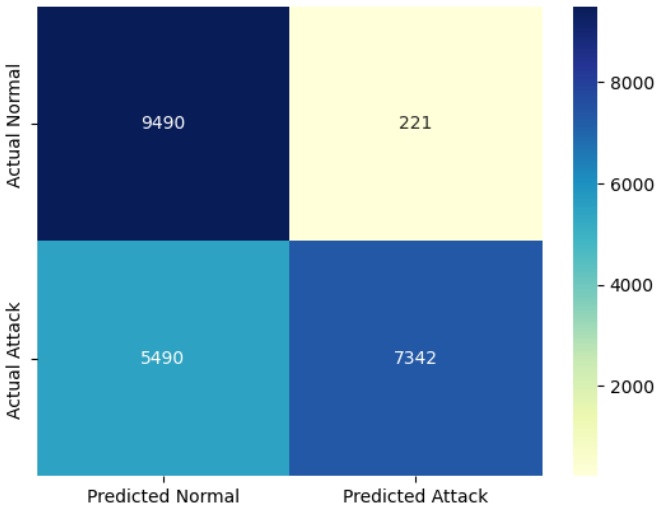

Fig. 4. Confusion matrix of binary classification of network attacks.

These results offer valuable insights into the model's strengths and limitations. While the model has shown a strong capacity for correctly identifying normal network traffic and a fair performance in recognizing attack instances, the relatively high number of false negatives (attack traffic identified as normal) indicates room for improving the model's ability to accurately identify network attacks. This confusion matrix serves as a baseline for refining the model and informs future iterations and improvements.

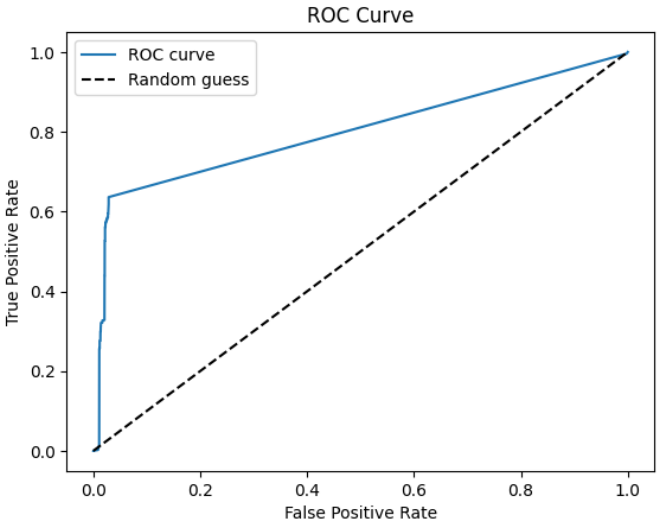

Fig. 5. ROC-AUC curve for binary classification of network attacks.

In this research paper, the Receiver Operating Characteristic (ROC) curve is an essential tool for evaluating the model's discrimination capability—how well the model can distinguish between the different classes. Fig. 5 demonstrates the obtained ROC curve in binary classification of network attacks. The ROC curve of this plot, known as the ROC-AUC, provides a scalar measure of the model's overall performance: an AUC of 1 signifies perfect classification. By considering the obtained results, we can suppose that the proposed model show high accuracy in network intrusion detection problem.

In the context of our research, the Accuracy and Loss graphs are integral components for assessing the performance and convergence of the model throughout its training process. The Accuracy graph is a plot that displays how the accuracy of the model evolves during the training and validation phases over multiple epochs. We would see a steady increase in accuracy for both the training and validation sets over time, indicating that the model is learning from the data. Therefore, Fig. 6 demonstrates train and validation accuracy for 10 learning epochs.

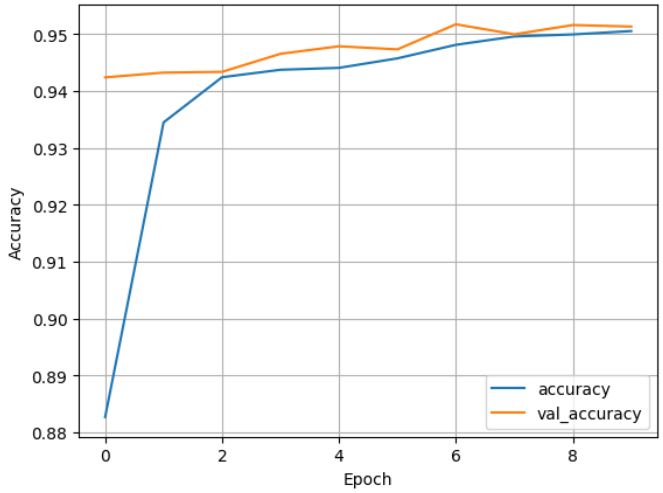

Fig. 6. Train and test accuracy of the proposed model for binary classification of network attacks.

On the other hand, the Loss graph demonstrates the model's error or cost over time. The loss is computed using a loss function, which measures the dissimilarity between the model's predictions and the actual labels. As the model learns, we expect the loss to decrease, indicating that the model's predictions are becoming increasingly accurate. If we see the loss decreasing for the training set but not for the validation set, this might also be an indication of overfitting. Therefore, Fig. 7 demonstrates train and validation loss.

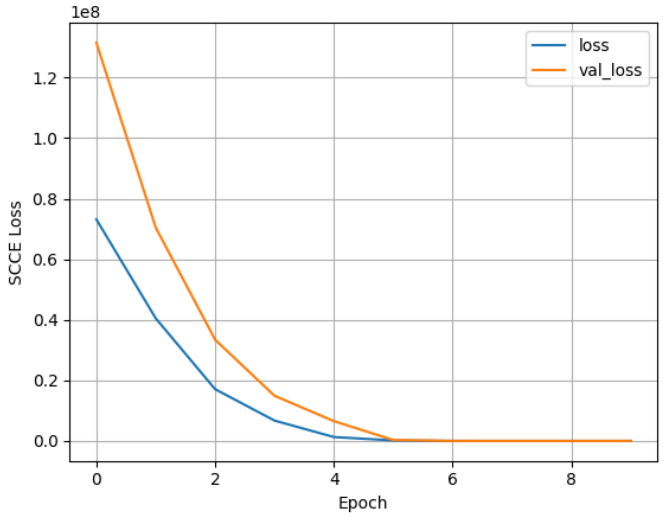

Fig. 7. Train and test loss of the proposed model for binary classification of network attacks.

As we transition into the next phase of our research on "Artificial Neural Network for Binary and Multiclassification of Network Attacks," we will be focusing on the multiclassification aspect. This segment of the study delves into the advanced capability of the proposed Artificial Neural Network (ANN) model to distinguish not just between normal and attack traffic, but also between different types of network attacks, namely DoS, Probe, Privilege, and Access attacks.

This task is significantly more complex than binary classification because it requires the model to differentiate among multiple classes, each representing a unique kind of network attack. Our primary objective is to improve the robustness of network security systems, by enabling them to correctly identify and categorize the nature of the threat they are facing.

B. *Multiclassification of Network Attacks*

In this context, our evaluation parameters and graphs, including accuracy, precision, recall, f-score, ROC-AUC, and the confusion matrix, will now consider these multiple categories. Consequently, the metrics will provide more granular insights into the model's performance.

We will be examining if the model can maintain high accuracy and precision across all attack classes, or if it shows particular strengths or weaknesses in identifying specific types of attacks. By carefully analyzing these results, we aim to gain valuable insights that will guide future research and help improve the efficacy of network intrusion detection and classification systems. Fig. 8 demonstrates confusion matrix of the proposed model when classify the traffic to five classes including normal class and four attack classes.

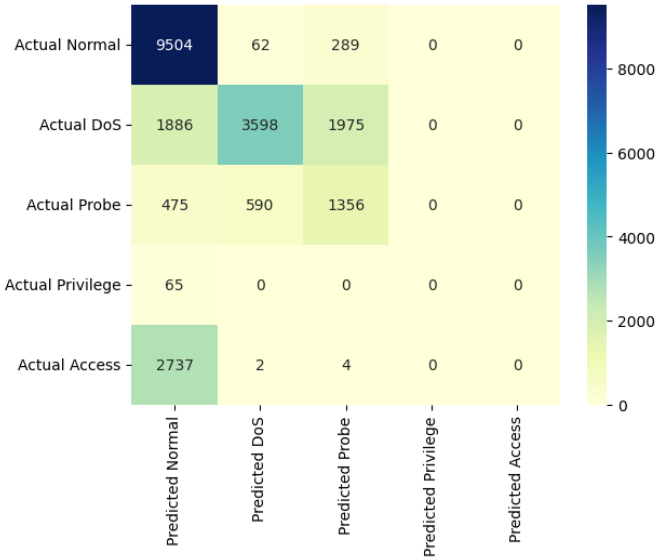

Fig. 8. Confusion matrix for multiclassification of network attacks.

Fig. 9 offers a graphical illustration of the proposed model's accuracy during the multiclass classification of network attacks over 10 epochs. It is evident that the model performs impressively, with the accuracy plateauing around the 94% mark within these iterations. This high accuracy underscores the model's effectiveness in identifying various types of network attacks.

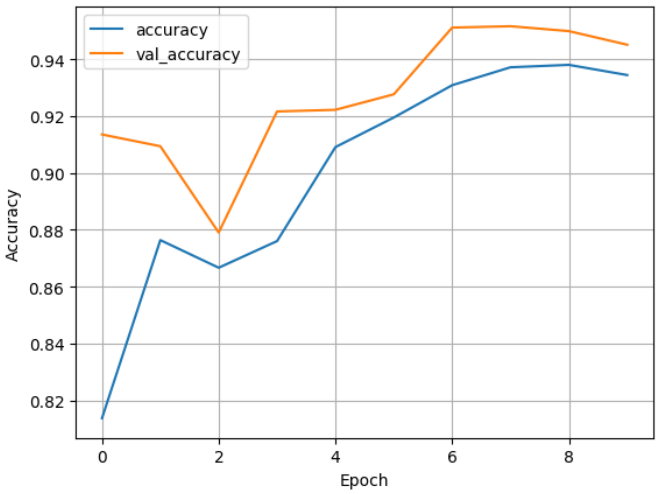

Fig. 9. Train and test accuracy of the proposed model for multiclassification of network attacks.

Fig. 10 presents the progression of both training and testing loss of our proposed model in the multiclass classification of network attacks. The depicted results signify that the model is efficient, as it manages to minimize its loss within just five epochs of learning. This rapid convergence to a minimal loss implies a robust model that learns effectively.

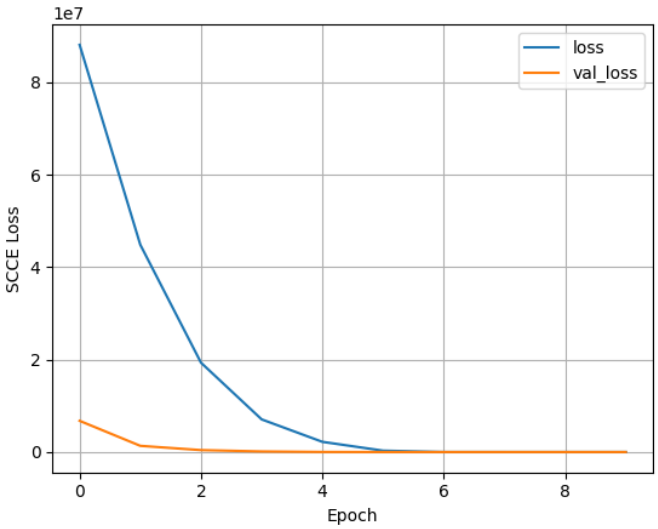

Fig. 10. Train and test loss of the proposed model for multiclassification of network attacks.

In the Results section of our research paper "Artificial Neural Network for Binary and Multiclassification of Network Attacks," we scrutinized the performance of our proposed ANN model for network intrusion detection and classification tasks. The model was trained and tested using the NSL-KDD dataset, with its performance evaluated via key metrics - Accuracy, Precision, Recall, F-Score, and ROC-AUC.

The obtained confusion matrix provided a detailed breakdown of the model's correct and incorrect classifications,

revealing a strong capacity for identifying normal network traffic and a satisfactory performance in recognizing attack instances. However, it also highlighted a relatively high number of false negatives, indicating potential areas for further refinement.

Through our ROC curve analysis, we assessed the model's capability to distinguish between classes at varying thresholds, giving us an understanding of its overall performance. Meanwhile, the Accuracy and Loss graphs traced the evolution of the model's learning process, aiding in identifying potential overfitting and underfitting issues.

Finally, as we moved to the multiclassification of network attacks, we found the model could distinguish not just between normal and attack traffic but also among different types of network attacks. This step elevated the complexity of the model's task, yet it showed promising results, setting the stage for future work in improving network intrusion detection systems.

The results paint a comprehensive picture of the model's capabilities, strengths, and areas for improvement. They provide a firm foundation for the ongoing development of a robust, high-performing ANN model for network attack classification.

VII. Discussion

The Discussion section of this research paper on "Artificial Neural Network for Binary and Multiclassification of Network Attacks" allows for an in-depth exploration of the implications of our results, their alignment with existing research, the strengths and weaknesses of our methodology, and directions for future research [22].

This study presents a novel implementation of an Artificial Neural Network (ANN) for detecting and classifying network intrusions [23]. The ANN model has shown promising results both in binary classification (distinguishing between normal and attack traffic) and in multiclassification (distinguishing among different types of network attacks).

One key advantage of our proposed model is its adaptability [24]. The model's architecture, composed of densely connected layers interspersed with dropout layers, enables it to learn intricate patterns within the data. The use of dropout layers, in particular, helps prevent overfitting by reducing the model's complexity during training [25]. Our model demonstrates a strong capacity to generalize from the training data to unseen data, thereby making it a robust and reliable tool for intrusion detection in different network environments.

However, there are areas where the model could be improved. The confusion matrix indicated a relatively high number of false negatives, suggesting that the model might be under-sensitive to certain types of attacks or specific features within the data [26]. Further investigation and refinement of the model's architecture, hyperparameters, or training process could help address this issue [27]. Additionally, the incorporation of other machine learning techniques, such as ensemble methods or advanced feature extraction, could potentially boost the model's performance [28].

Looking forward, it is also crucial to consider the dynamic and evolving nature of cyber threats. As attackers continuously develop new strategies and techniques, the patterns that our model has learned may become outdated [29]. Therefore, it is essential to continually update and retrain the model with the latest data. One possible approach to address this challenge is online learning, where the model is continually updated with new data as it becomes available [30]. This approach could help the model adapt to emerging threats and maintain its performance over time.

Finally, the successful application of the proposed model to the NSL-KDD dataset suggests potential for its use in other cybersecurity contexts. For example, similar techniques could be applied to other types of security-related data, such as system logs or network flow data, to detect anomalies or suspicious activities. Exploring these applications could be a promising direction for future research.

In summary, this study has demonstrated the potential of ANN models for network intrusion detection and classification. While the model has shown promising results, there remains room for improvement and adaptation to the continuously evolving landscape of network threats. By addressing these challenges, we believe that ANN models can play a pivotal role in enhancing network security and developing more resilient systems against cyber threats.

VIII. Conclusion

In conclusion, the research paper has provided an insightful exploration into the implementation of an ANN model for network intrusion detection and classification. The comprehensive analysis of the model's performance has showcased its potential for bolstering network security, along with its ability to discern between various types of cyber threats.

The study was anchored around the NSL-KDD dataset, a standard benchmark in the field of cybersecurity. Our ANN model exhibited notable accuracy in both binary and multiclassification tasks, proving its capability in detecting normal versus attack traffic and differentiating among various attack types. However, a degree of under-sensitivity was observed in terms of false negatives, indicating an avenue for future refinement and optimization.

Moreover, the research underscored the significance of evolving the model in tandem with the ever-changing nature of cyber threats. Our model's adaptability, largely attributable to its densely connected layers and dropout layers, constitutes a strong foundation for this continual evolution. Future work can benefit from implementing online learning techniques to ensure the model stays updated with the latest threat patterns.

The promising results gleaned from this study support the idea that advanced machine learning techniques, such as ANN, hold substantial potential in advancing network security. By delving deeper into the granular intricacies of attack patterns and continuously improving upon model architectures and training techniques, we can move closer to creating highly effective, adaptable, and robust intrusion detection systems.

In essence, this research represents a significant stride in the broader march towards leveraging artificial intelligence in cybersecurity, a field that continues to grow in importance as digital connections increasingly underpin our societies. Our findings provide a solid foundation for further investigation and innovation in this critical area.

REFERENCES

[1] Gan, B., Chen, Y., Dong, Q., Guo, J., & Wang, R. (2022). A convolutional neural network intrusion detection method based on data imbalance. The Journal of Supercomputing, 1-34.

[2] Manjula, P., & Priya, S. B. (2022). An effective network intrusion detection and classification system for securing WSN using VGG-19 and hybrid deep neural network techniques. Journal of Intelligent & Fuzzy Systems, (Preprint), 1-14.

[3] Hu, R., Wu, Z., Xu, Y., & Lai, T. (2022). Multi-attack and multi-classification intrusion detection for vehicle-mounted networks based on mosaic-coded convolutional neural network. Scientific Reports, 12(1), 1-16.

[4] A. Altayeva, B. Omarov, H.C. Jeong and Y.I. Cho, "Multi-step face recognition for improving face detection and recognition rate", Far East Journal of Electronics and Communications, vol. 16, no. 3, pp. 471-491, 2016.

[5] Do, P. H., Dinh, T. D., Le, D. T., Myrova, L., & Kirichek, R. (2021, October). An Efficient Feature Extraction Method for Attack Classification in IoT Networks. In 2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) (pp. 194-199). IEEE.

[6] Jing, D., & Chen, H. B. (2019, October). SVM based network intrusion detection for the UNSW-NB15 dataset. In 2019 IEEE 13th international conference on ASIC (ASICON) (pp. 1-4). IEEE.

[7] Alkafagi, S. S. (2023). Build Network Intrusion Detection System based on combination of Fractal Density Peak Clustering and Artificial Neural Network. Journal of Al-Qadisiyah for computer science and mathematics, 15(1), Page-111.

[8] Fraihat, S., Makhadmeh, S., Awad, M., Al-Betar, M. A., & Al-Redhaei, A. (2023). Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm. Internet of Things, 100819.

[9] Wang, Y., Zhang, H., Wei, Y., Wang, H., Peng, Y., Bin, Z., & Li, W. (2023). An evolutionary computation-based machine learning for network attack detection in big data traffic. Applied Soft Computing, 138, 110184.

[10] Wang, H., Zhou, S., Li, H., Hu, J., Du, X., Zhou, J., ... & Yang, H. (2022, July). Deep Learning Network Intrusion Detection Based on Network Traffic. In Artificial Intelligence and Security: 8th International Conference, ICAIS 2022, Qinghai, China, July 15–20, 2022, Proceedings, Part III (pp. 194-207). Cham: Springer International Publishing.

[11] Farea, A. A., Wang, C., Farea, E., & Alawi, A. B. (2021, December). Cross-site scripting (XSS) and SQL injection attacks multi-classification using bidirectional LSTM recurrent neural network. In 2021 IEEE International Conference on Progress in Informatics and Computing (PIC) (pp. 358-363). IEEE.

[12] Omarov, B., Narynov, S., Zhumanov, Z., Gumar, A., & Khassanova, M. (2022). State-of-the-art violence detection techniques in video surveillance security systems: a systematic review. PeerJ Computer Science, 8, e920.

[13] Wei, J., Yao, L., & Meng, Q. (2023). Self-adaptive logit balancing for deep neural network robustness: Defence and detection of adversarial attacks. Neurocomputing, 531, 180-194.

[14] Mohiuddin, G., Lin, Z., Zheng, J., Wu, J., Li, W., Fang, Y., ... & Zeng, X. (2023). Intrusion detection using hybridized meta-heuristic techniques with Weighted XGBoost Classifier. Expert Systems with Applications, 120596.

[15] Gao, X., Wang, T., Wu, Q., & Wu, J. (2022, October). An Intrusion Detection Mothod based on Feature Selection and Binary Classification Grouped Learning. In 2022 IEEE 6th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 1723-1730). IEEE.

[16] Omarov, B., Tursynova, A., Postolache, O., Gamry, K., Batyrbekov, A., Aldeshov, S., ... & Shiyapov, K. (2022). Modified UNet Model for Brain Stroke Lesion Segmentation on Computed Tomography Images. Computers, Materials & Continua, 71(3).

[17] Al-Safaar, D., & Al-Yaseen, W. L. (2023). Hybrid AE-MLP: Hybrid Deep Learning Model Based on Autoencoder and Multilayer Perceptron Model for Intrusion Detection System. International Journal of Intelligent Engineering & Systems, 16(2).

[18] Omarov, B., & Altayeva, A. (2018, January). Towards intelligent IoT smart city platform based on OneM2M guideline: smart grid case study. In 2018 IEEE International Conference on Big Data and Smart Computing (BigComp) (pp. 701-704). IEEE.

[19] Cunha, A. A., Borges, J. B., & Loureiro, A. A. (2022, October). Classification of Botnet Attacks in IoT Using a Convolutional Neural Network. In Proceedings of the 18th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (pp. 63-70).

[20] Tursynova, A., & Omarov, B. (2021, November). 3D U-Net for brain stroke lesion segmentation on ISLES 2018 dataset. In 2021 16th International Conference on Electronics Computer and Computation (ICECCO) (pp. 1-4). IEEE.

[21] Lai, Y., Zhang, J., & Liu, Z. (2019). Industrial anomaly detection and attack classification method based on convolutional neural network. Security and Communication Networks, 2019, 1-11.

[22] Sultanovich, O. B., Ergeshovich, S. E., Duisenbekovich, O. E., Balabekovna, K. B., Nagashbek, K. Z., & Nurlakovich, K. A. (2016). National Sports in the Sphere of Physical Culture as a Means of Forming Professional Competence of Future Coach Instructors. Indian Journal of Science and Technology, 9(5), 87605-87605.

[23] Xia, Q., Dong, S., & Peng, T. (2022, November). An Abnormal Traffic Detection Method for IoT Devices Based on Federated Learning and Depthwise Separable Convolutional Neural Networks. In 2022 IEEE International Performance, Computing, and Communications Conference (IPCCC) (pp. 352-359). IEEE.

[24] Ashwini, S., Sinha, M., & Sabarinathan, C. (2023). Implementation of Intrusion Detection Model for Detecting Cyberattacks Using Support Vector Machine. Advances in Science and Technology, 124, 772-781.

[25] Hamid, D., Ullah, S. S., Iqbal, J., Hussain, S., ul Hassan, C. A., & Umar, F. (2022). Research Article A Machine Learning in Binary and Multiclassification Results on Imbalanced Heart Disease Data Stream. learning, 11, 12.

[26] He, J., Wang, X., Song, Y., & Xiang, Q. (2023). A multiscale intrusion detection system based on pyramid depthwise separable convolution neural network. Neurocomputing, 530, 48-59.

[27] Kaldarova, B., Omarov, B., Zhaidakbayeva, L., Tursynbayev, A., Beissenova, G., Kurmanbayev, B., & Anarbayev, A. (2023, February). Applying game-based learning to a primary school class in computer science terminology learning. In Frontiers in Education (Vol. 8, p. 1100275). Frontiers.

[28] Yuan, Q., Zhu, Y., Xiong, G., Wang, Y., Yu, W., Lu, B., & Gou, G. (2023). ULDC: Unsupervised Learning-Based Data Cleaning for Malicious Traffic With High Noise. The Computer Journal, bxad036.

[29] Zhang, X., Wang, J., Xu, J., & Gu, C. (2023). Detection of Android Malware Based on Deep Forest and Feature Enhancement. IEEE Access, 11, 29344-29359.

[30] Kabakus, A. T. (2023). A novel robust convolutional neural network for uniform resource locator classification from the view of cyber security. Concurrency and Computation: Practice and Experience, 35(3), e7517.