**Intrusion Detection on UNSW\_NB15 Dataset by Employing Machine Learning and Deep Learning Techniques**

**Contents**

[Introduction 4](#_Toc156225347)

[Research Problem 4](#_Toc156225348)

[Aims 4](#_Toc156225349)

[Objectives 5](#_Toc156225350)

[Research Question 5](#_Toc156225351)

[Literature Review 6](#_Toc156225352)

[Methodology 8](#_Toc156225353)

[Dataset 8](#_Toc156225354)

[Data pre-processing 9](#_Toc156225355)

[Exploratory Data Analysis 10](#_Toc156225356)

[Modelling & Implementation 11](#_Toc156225357)

[Results & Discussion 15](#_Toc156225358)

[Conclusion 16](#_Toc156225359)

[References 18](#_Toc156225360)

**Figures**

[Figure 1: Training Dataset 9](#_Toc156225643)

[Figure 2: Testing Dataset 9](#_Toc156225644)

[Figure 3: Removing Columns 10](#_Toc156225645)

[Figure 4: Label Distribution in Training Dataset 10](#_Toc156225646)

[Figure 5: Label Distribution in Testing Dataset 11](#_Toc156225647)

[Figure 6: ANN Confusion Matrix 12](#_Toc156225648)

[Figure 7: Random Forest Confusion Matrix 12](#_Toc156225649)

[Figure 8: CNN Confusion Matrix 13](#_Toc156225650)

[Figure 9: Naïve Bayes Confusion Matrix 13](#_Toc156225651)

[Figure 10: KNN Confusion Matrix 14](#_Toc156225652)

[Figure 11: Models' Accuracy 15](#_Toc156225653)

[Figure 12: Bar Chart Representation of Models' Accuracy 15](#_Toc156225654)

**Tables**

[Table 1: Classification Report of the Algorithms 12](#_Toc156225686)

**Abstract**

Since the essence of Information Security, intrusion attacks have proven to be most dangerous and difficult to protect against. In this report, intrusion detection has been performed on UNSW-NB15 dataset. UNSW-NB15 dataset available on UNSW Research website as well as on Kaggle also and is used, for model training. The dataset contains a hybrid of real modern activities and synthetic contemporary attack behaviors. Preprocessing is performed on data to convert categorical variables into numerical format. After preprocessing, five machine learning models are trained. The accuracy scores of each algorithm were used to evaluate its performance. With a score of 89.17%, CNN emerged as the best model. Random Forest came in second with an accuracy of 88.37%, and KNN came in third with 85.10% while ANN and Naïve Bayes were fourth and fifth with an accuracy of 76.72% and 74.61% respectively. The results show how important it is to choose an algorithm carefully for intrusion detection, considering the requirements of the application and the balancing act between accuracy and recall.

# Introduction

Attacks on the network infrastructures are the big problem of the network security of today’s world, with the swiftly growing illegal activities in the networking world; the network security becomes a big challenge which is neither hopeless nor solved. It also compromises the usability of data and information as more access of data leads to higher possibilities of vulnerabilities and increases the risks of attacks. It is difficult to protect against intrusion attacks as they are mostly anonymous and most of the times are detected after the damage has been done.

Intrusion attackers intrude the system and hide themselves in the most unpredictable place, taking control of the system or information secretly. It is very sad that hackers always have more effective methods and more dangerous tools against protection. But as we move towards the rapidly innovative times, we have found solutions which help us in protecting against hackers and attackers. Now a days all our activities can be tracked and can be supervised by numerous ways. As most of our activities are being stored in form of logs on backend of the platforms we use. Other than this we always have the option of access control.

## Research Problem

As monitoring activities on a network is very crucial for protection against intrusion attacks, it is a process that should be done very carefully and thoroughly. Plus, you can’t risk information security by trusting the people who monitor or supervise intrusions. Sometimes we may tend to misunderstand a hacker for a trusted user and turn a blind eye to his/her activities on the network or may not think of the deficiency of our system. We require a solution which makes sure that no stone is left unturned while protecting information or a system. An AI based solution should be integrated to overcome the deficiencies in observation done by human.

## Aims

The aim of this research is to make intrusion detection perfect to ensure information security and to create a fearless environment for the user to work in. Through the application of advanced machine learning techniques, we aspire to equip intrusion detection with actionable insights derived from UNSW-NB15 activity data. By integrating a trusted method for monitoring and detection, users can work in fearless environment and pass information securely without the risk of being attacked or hacked.

## Objectives

* Examine current machine learning methods and technologies that are applicable to UNSW-NB15 dataset.
* Formulate a precise research methodology that integrates recognized machine learning techniques.
* Train machine learning models with the chosen training data by applying the suggested technique.
* Utilize assessment methods to determine the efficacy of the model, such as classification reports, confusion matrices, and accuracy scores.

## Research Question

How can different types of intrusions detection can be done with machine learning techniques with a dataset of activity on a network?

**Sub Question 1 (SQ1):** How many types of intrusions are present in the dataset for evaluation?

**Sub Question 2 (SQ2):** What are the challenges and openings in preprocessing and cleaning content information for intrusion detection?

**Sub Question 3 (SQ3):** How do diverse machine learning models perform in classifying best approach for detection?

**Sub Question 4 (SQ4):** What experiences can be determined from the evaluation for further acknowledgment?

# Literature Review

(Ansam Khraisat, 2019) Cybercriminals use social engineering tactics in addition to advanced ways to target computer users. A growing number of cybercriminals are getting more skilled and driven. Cybercriminals have demonstrated their ability to use infrastructure that is resistant to compromise, conceal their identities, isolate themselves from illicit earnings, and mask their conversations. As a result, it becomes more crucial than ever to safeguard computer systems using sophisticated intrusion detection systems that can identify contemporary malware. To effectively design and construct these types of IDS systems, a thorough understanding of the advantages and disadvantages of current IDS research is required.

We have thoroughly reviewed the approaches, varieties, and technologies used in intrusion detection systems in this study, along with their benefits and drawbacks. Many machine learning methods.

(Zeeshan Ahmad, 2021) ML and DL-based network intrusion detection algorithms are extensively reviewed in this study to update new researchers on the field's knowledge, trends, and development. A systematic approach is used to choose AI-based NIDS papers. IDS and its classification schemes are extensively explained in the reviewed literature. Each article's technique, merits and drawbacks in terms of intrusion detection capability and model complexity are then explored. According to this study, DL-based methods are being used to improve NIDS detection accuracy and FAR reduction. About 80% of proposed solutions were DL-based, with AE and DNN being the most popular algorithms. Although DL systems outperform ML-based methods in self-learning and model fitting. These methods are complicated and need a lot of processing and storage power. These difficulties must be addressed to meet NIDS real-time requirements and increase performance. The study found that 60% of proposed approaches were tested using KDD Cup'99 and NSL-KDD datasets due to their comprehensive results. However, these datasets are too old to meet new network assaults, limiting real-time performance of proposed approaches.AI-based NIDS algorithms should be validated with the latest dataset like CSE-CIC-IDS2018 for enhanced intrusion detection accuracy. This study also emphasizes research gaps in enhancing model performance for low-frequency attacks in real-world environments and finding efficient ways to simplify proposed models. Future research could propose an efficient NIDS framework employing simpler DL algorithms and an effective detection method. We will use this knowledge to create a unique, lightweight, and efficient DL-based NIDS to identify network intrusions in future study.

(JABEZ Ja, 2015) In this research, we introduce the Outlier Detection technique for detecting computer network intrusions. Our training model enhances intrusion detection system performance with large datasets and distributed environments. The proposed method was tested with KDD.

Data from the actual world. In contrast to the suggested IDS system, machine learning techniques need significant execution and storage time to detect computer network intrusions. According to this study, the suggested IDS outperforms previous machine learning methods and can detect practically all anomalies in computer networks. This study could be applied to distance computation functions between trained models and testing data in the future. We believe our research can enhance the efficiency of IDS.

PB-DID analyzes and combines conventional flow and TCP information from both data sources. Solving imbalance and over-fitting issues in public data sets involves selecting equal numbers of packets from each category. Using DL technology, we classified non-anomalous, DoS, and DDoS traffic with 96.3% accuracy, encompassing nearly both data sets. Our approach is unique in reducing in half the number of features used to identify malicious traffic and covering two recent benchmarked data sets. Our goal is to enhance feature comparison and selection by utilizing reputable benchmark data sets in the future. New attack categories will be included to address most IoT device risks in classification.

(Mahalakshmi Gopalkrishna, 2021)The suggested work improves intrusion detection efficiency, even if we have many existing IDS, largely built in machine learning algorithms, that fail to prevent freshly generated attacks since they rely on previous data. CNN deep learning is used to construct IDS. We classify UNSW NB15 network intrusion public dataset using CNN algorithm and get 93.5% accuracy. CNN is effective at intrusion detection, and assessment metrics were used to assess model performance.

# Methodology

In this research study a through methodology is used to preprocess the network activity and to evaluate best AI based approach for intrusion detection. First, a dataset is selected on which machine learning models will be trained. For this a dataset available online on UNSW Research website and Kaggle is used. Dataset is loaded from CSV file into a pandas’ data frame, then the structure and distributions of the data is analyzed. A careful data preprocessing step comes next to make sure that the input for machine learning models is of good quality. First, we are going to drop two columns “id” and “attack\_cat”. Then unstructured text data is turned into a standard and better style by using methods like label encoding and min-max scaling. In “service”,” proto” and “state” column it is seen that values are initially given in categorical variables, we have used label encoding to transform them into numerical variables. Further min-max scaling help us change the values to make them understandable for machine learning models. Artificial Neural Network, Convolution Neural Network, K-Nearest Neighbor, Naïve Bayes and Random Forest are some of the machine learning models that are used in the study. After that, models are put through a thorough implementation process on the preprocessed text data. The next step is to evaluate each model's performance in detail. Metrics like accuracy scores, confusion matrices, and classification reports are used to give detailed information about each model's strengths and weaknesses. To import machine learning models, train and evaluate them, Scikit-Learn library is used. For model training and evaluation, an open-source library Scikit-Learn is used. Scikit-learn is an open-source and widely-used Python library for machine learning which includes a range of machine learning algorithms and preprocessing technique. Other than this it also provides functions for data handling and transformation.

## Dataset

Chosen dataset is in CSV format, it is a collection of activity on a network. Dataset is loaded into using the pandas library as a pandas data frame. There are 45 features in dataset, 4 categorical variable columns while 41 numerical variable columns. This dataset has nine types of attacks namely Fuzzers, Analysis, Backdoors, Dos, Exploits, Generic, Reconnaissance, Shellcode and Worms. This helps a lot by providing a variety of attacks for detection and model training. Dataset’s diversity and small scale make it a suitable basis for using machine learning models and gaining insight for securing our networks

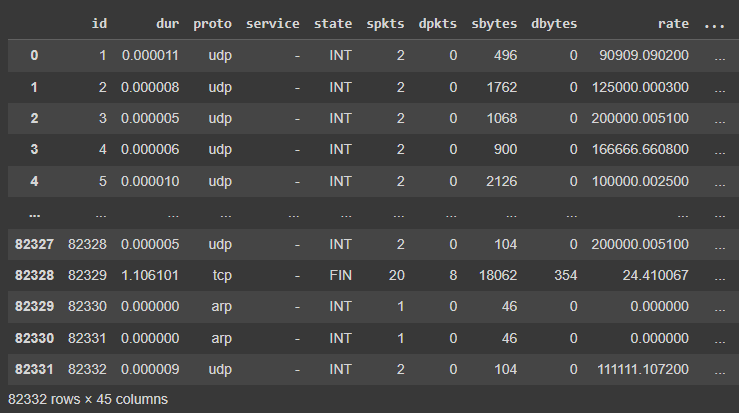


Figure : Training Dataset

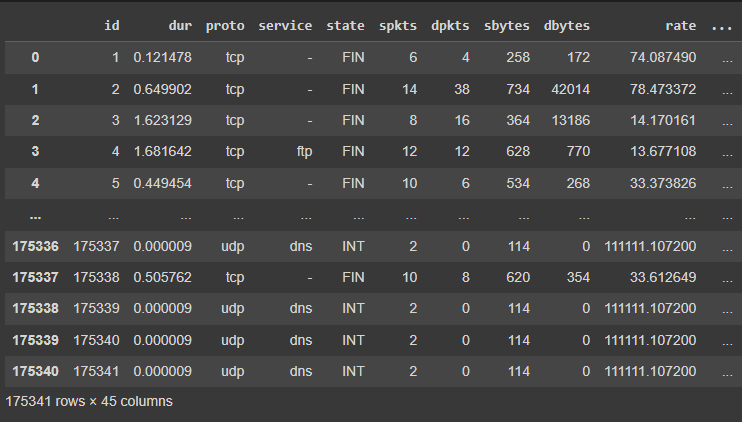
****

Figure : Testing Dataset

## Data pre-processing

During preprocessing following steps are performed:

Two columns are dropped first from both training and testing dataset. Those columns are “id” and “attack\_cat”.

After removing columns, we can see 43 columns are left.

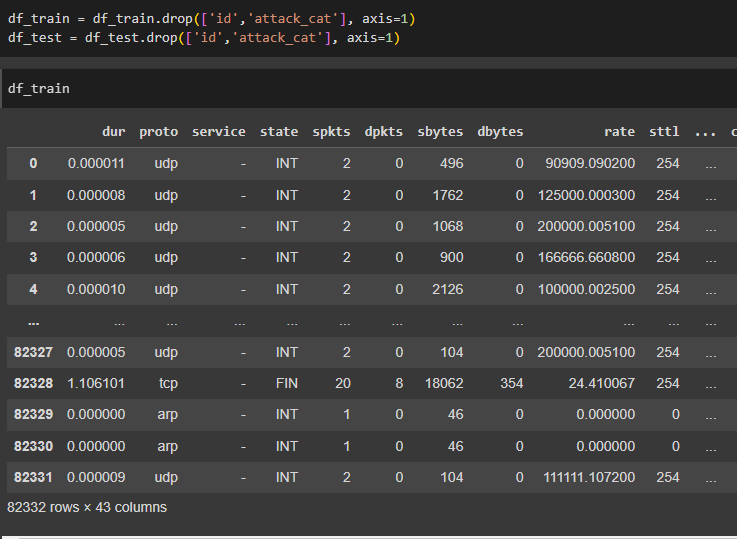


Figure : Removing Columns

For preprocessing categorical variables into numerical variables, label encoding is performed. For further preprocessing we have fit transformed the data using min-max scaler.

## Exploratory Data Analysis

Integrating Exploratory Data Analysis (EDA) into the research technique establishes a basis for making well-informed decisions at every stage of the machine learning process. Through the utilization of visual representations and statistical summaries, researchers can discover trends, anomalies, and significant aspects that influence the overall quality and characteristics of the UNSW-NB15 dataset. This ultimately improves the efficiency of following predictive modeling endeavors.

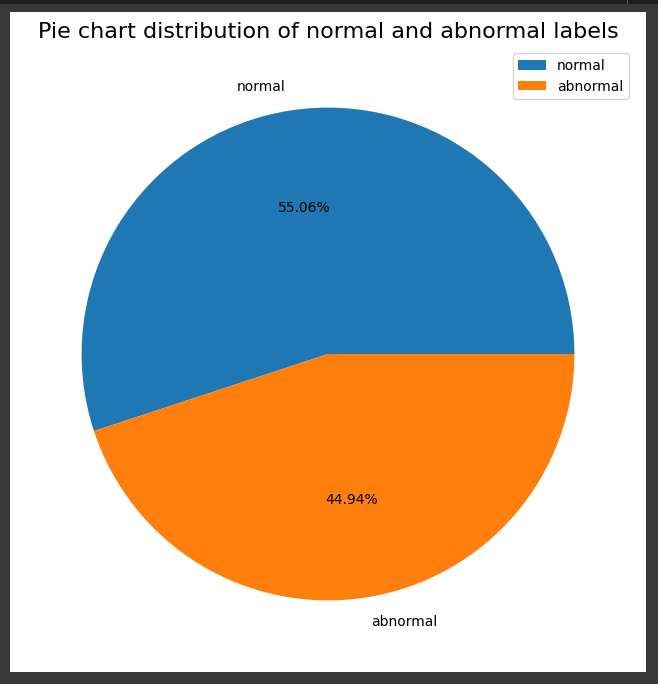


Figure : Label Distribution in Training Dataset

The distribution of activity labels in dataset is reflected by the ratio of positive to negative activities, with 55.06% normal and 44.94% abnormal activities in training dataset.

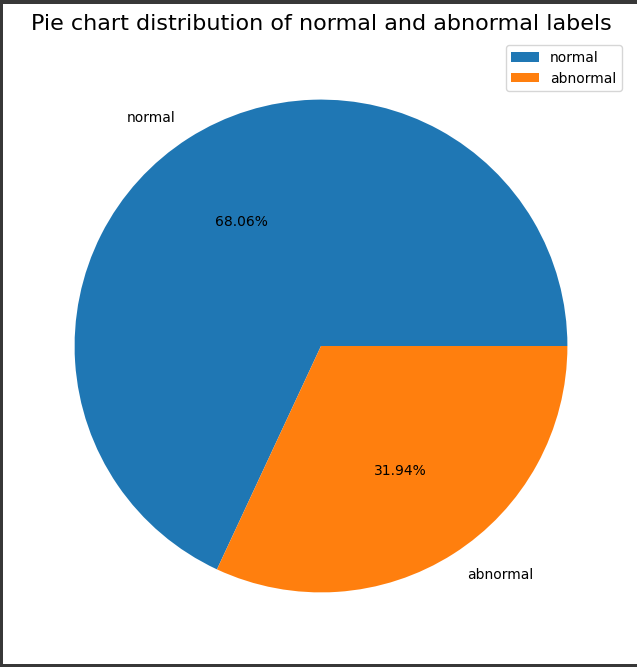


Figure : Label Distribution in Testing Dataset

# Modelling & Implementation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **MODEL** | **ACCURACY** | **NEGATIVE PERCISION** | **POSITIVE PRECISION** | **POSITIVE RECALL** | **POSITIVE F1 SCORE** |
| **ANN** | 83.36% | 0.66 | 0.99 | 0.76 | 0.86 |
| **CNN** | 85.31% | 0.69 | 0.99 | 0.79 | 0.88 |
| **RANDOM FOREST** | 88.63% | 0.75 | 0.99 | 0.84 | 0.91 |
| **KNN** | 85.10% | 0.69 | 0.98 | 0.80 | 0.88 |
| **NAÏVE BAYES** | 74.61% | 0.56 | 0.94 | 0.67 | 0.78 |

Table : Classification Report of the Algorithms

To predict the sentiments of the customers four machine learning algorithms are trained. Different predictive models are trained to get the best predictive model.

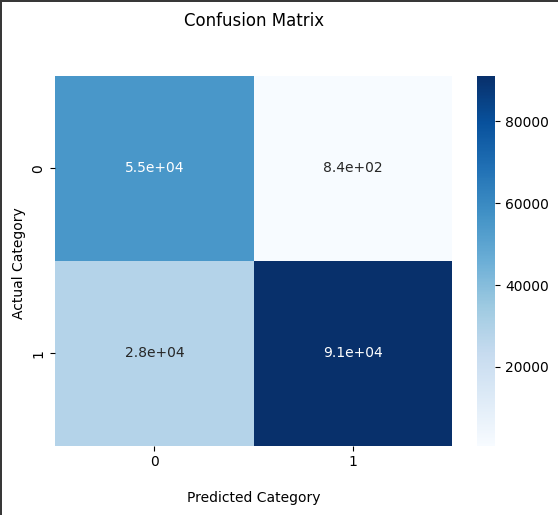


Figure : ANN Confusion Matrix

In Intrusion detection, the Artificial Neural Network model got it right 83.36% of the time. For negative mood, the precision was 0.66, which means it correctly predicted 66% of negative instances, and the recall was 0.99, which means it correctly predicted 99% of real negative instances. It got an F1 score of 0.79 for negative opinion. The accuracy was better for positive mood, at 0.99, with a recall of 0.76 and an F1-score of 0.86. There were 55163 true positives, 837 false positives, 28327 true negatives, and 91014 false negatives in the confusion matrix.

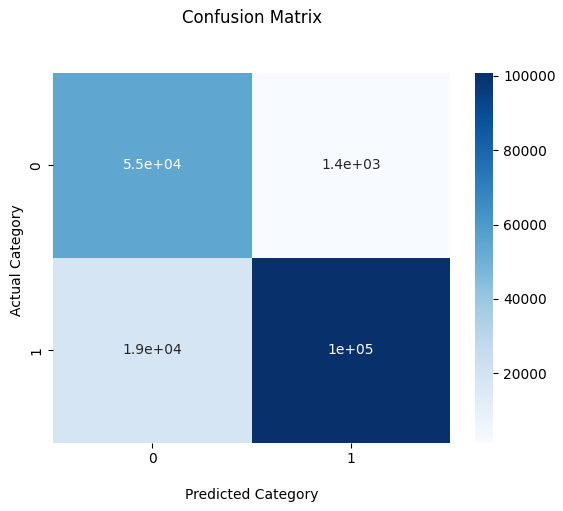


Figure : Random Forest Confusion Matrix

In intrusion detection, the Random Forest model got it right 88.63% of the time. In the case of negative instances, precision score was 0.75, F1-score was 0.85, and the recall was 0.98. For positive instances, the F1-score was 0.91, and the precision was 0.99. The recall was0.84. It showed 54614 true positives, 1386 false positives, 18549 true negatives, and 100792 false negatives.

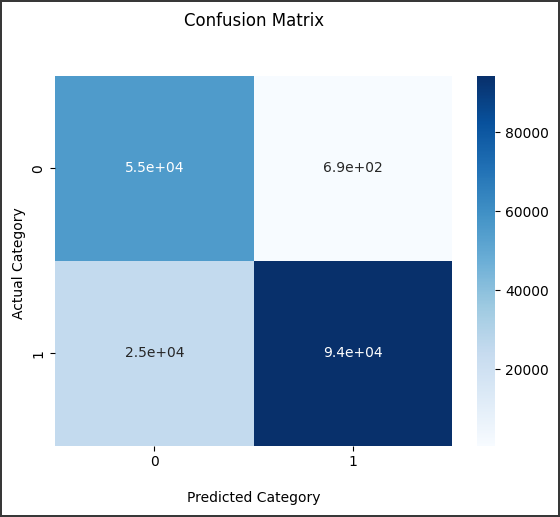


Figure : CNN Confusion Matrix

In intrusion detection, the CNN model got it right 85.31% of the time. For negative instances, the accuracy was 0.69, the recall was 0.99, and the F1-score was 0.81. For positive instances, the accuracy was 0.99, the recall was 0.79, and the F1-score was 0.88. It showed that there were 55312 true negatives, 688 fake positives, 25063 false negatives, and 94278 true positives.

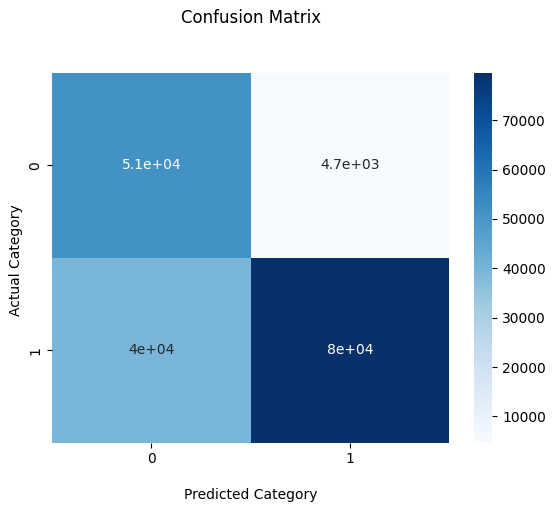


Figure : Naïve Bayes Confusion Matrix

In intrusion detection, the Naïve Bayes model got it right 74.61% of the time. For negative instances, the accuracy was 0.56, the recall was 0.92, and the F1-score was 0.70. For positive instances, the accuracy was 0.94, the recall was 0.67, and the F1-score was 0.78. It showed 51273 true positives, 4727 true negatives, 39782 false positives, and 79559 false negatives.

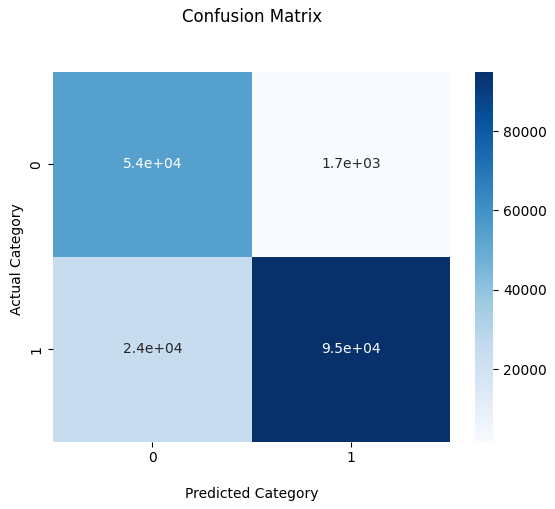


Figure : KNN Confusion Matrix

In intrusion detection, the KNN model got it right 85.10% of the time. For negative instances, the accuracy was 0.69, the recall was 0.97, and the F1-score was 0.81. For positive instances, the accuracy was 0.98, the recall was 0.80, and the F1-score was 0.88. It showed 54282 true positives, 1718 true negatives, 24486 false positives, and 94935 false negatives.

In short, every type has its own pros and cons. All the machine learning models work well for job of recalling negative sentiments. And all the models give a good precision score for positive sentiment while their accuracies may differ from each other a bit. When interpreting, it's important to think about the application's specific goals and the trade-offs between accuracy and recall.

# Results & Discussion

Further, there is an interpretation of the intrusion prediction model results. To implement the model, five machine learning algorithms have been used, "Random Forest (RF), Artificial Neural Network (ANN), Convolution Neural Network (CNN), K-Nearest Neighbor (KNN) and Naïve Bayes." For the training and testing of the model, I have used two different datasets. On the training set I have trained the models and evaluated them using the testing set.

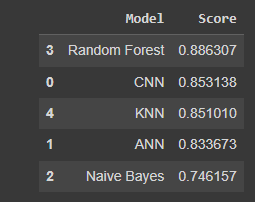


Figure : Models' Accuracy

Figure 11 shows the data frame of model accuracy & performance based on different algorithms or classifiers. We can see Random Forest classifier has shown a better accuracy score than the others. There is a 88.63% accuracy score for the Random Forest classifier, 85.31% accuracy score for the CNN classifier, 85.10% accuracy score for the KNN classifier, 83.36% accuracy score for the ANN classifier and 74.61% accuracy score for Naïve Bayes classifier on the UNSW-NB15 network activity dataset.

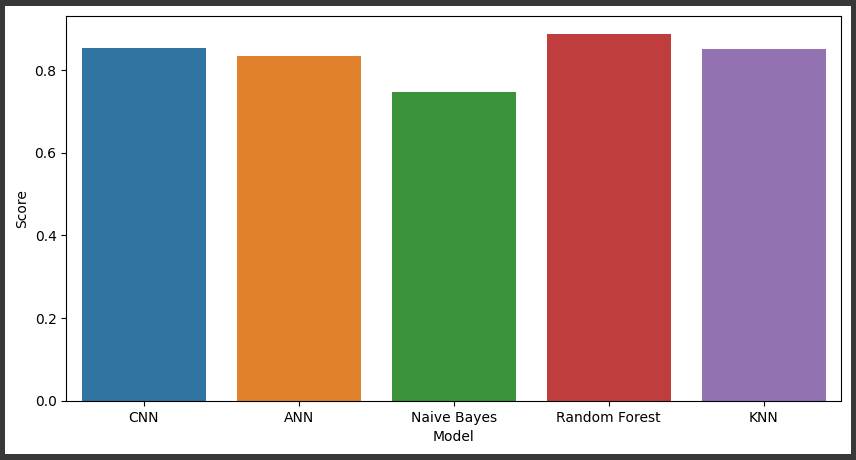


Figure : Bar Chart Representation of Models' Accuracy

The above visualization represents the model accuracy score for each bar plot classifier. It shows Random Forest classifier is the only solution that has provided 88.63% accuracy in the sentiment prediction, and it is the most suitable classifier for such classification.

Based on the above findings & results, it is clear that Random Forest is the best choice to implement the sentiment prediction model. An optimal model with Random Forest takes less execution & prediction time as compared to the other classifiers and provides a more accurate score evaluated by different evaluation metrics.

# Conclusion

The aim of this study was to train a machine learning model, that can classify between positive and negative instances of the network activity. For this classification five machine learning algorithms were used, ANN, CNN, KNN, Random Forest, and Naïve bayes. For the model training I have used a dataset provided online on UNSW-NB15 Research website. First, I have preprocessed the data to drop the columns I needed and changed categorical variables. After that I performed some exploratory data analysis to analyze the data and then used the datasets into testing and training sets. On these datasets, I have trained the model and evaluated it.

With an accuracy score of 88.63%, Random Forest turned out to be the best model. Its reliable and effective performance in intrusion detection tasks was shown by how well it predicted both normal and abnormal activity. CNN model stood second by showing impressive precision and accuracy at 85.31%, confirming its place as a strong option for intrusion detection.

With an accuracy score of 85.10%, KNN had a good balance between precision and recall, which made it even better for jobs that need to detect intrusion. ANN also performed effectively with an accuracy of 83.36%. But the Naïve Bayes model did not do as well as the others. Its accuracy score of 74.61% showed that it might have trouble predicting models as well as the other models.

Based on the findings of the research, Random Forest is the best model to perform intrusion detection. (Ansam Khraisat, 2019)

In the future, possible changes could include finetuning the hyperparameters even more, engineering features, or looking into more advanced models to make the whole thing run better. In addition, knowing the specific needs of the sentiment analysis application will help with choosing the best algorithm for correct sentiment classification in the future.

# References

Akanksha Halde, A. U. (2022). SENTIMENT ANALYSIS ON AMAZON PRODUCT REVIEWS. *International Research Journal of Modernization in Engineering Technology and Science*.

Alroobaea, R. (2022). Sentiment Analysis on Amazon Product Reviews. *International Journal of Advanced Computer Science and Applications*.

Ansam Khraisat, I. G. (2019, July 17). *Cyber Security,SpringerOpen*. Retrieved from SpringerOpen: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7

JABEZ Ja, D. M. (2015, April 19). *Science Direct*. Retrieved from ScienceDirect.com: https://www.sciencedirect.com/science/article/pii/S1877050915007000

Mahalakshmi Gopalkrishna, U. E. (2021, November). *ResearchGate*. Retrieved from researchgate.net: https://www.researchgate.net/publication/367821966\_Intrusion\_Detection\_System\_Using\_Convolutional\_Neural\_Network\_on\_UNSW\_NB15\_Dataset

Maurya, S., & Pratap, V. (2022). Sentiment Analysis on Amazon Product Reviews. *International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON).*

Medikonda, S. (2021). AMAZON PRODUCT REVIEW SENTIMENT ANALYSIS USING MACHINE LEARNING. *International Research Journal of Computer Science*.

MUHAMMAD ZEESHAN1(Senior Member, Q. R. (2021). *paperswithcode*. Retrieved from paperswithcode.com: https://paperswithcode.com/paper/protocol-based-deep-intrusion-detection-for

SANA NABIL, J. E. (2021). SENTIMENT ANALYSIS OF AMAZON’S REVIEWS USING MACHINE LEARNING ALGORITHMS. *Journal of Theoretical and Applied Information Technology*.

Tanjim Ul Haque, F. M. (2018). *Sentiment analysis on large scale Amazon product reviews.*

Zeeshan Ahmad, A. S. (2021, January). *ResearchGate*. Retrieved from ResearchGate.net: https://www.researchgate.net/publication/344726867\_Network\_intrusion\_detection\_system\_A\_systematic\_study\_of\_machine\_learning\_and\_deep\_learning\_approaches