The Role of AI in Network Security

Duru Çapar
Dokuz Eylül University
Computer Engineering Department
Izmir, Türkiye
duru.capar@ogr.deu.edu.tr

Abstract- In this paper, we will be discussing about the role of AI in network security. As you know, Artifical Intalligance has been rapidly involving our daily day lives and it is also widely used in technology.

1. INTRODUCTION

The fact that technology, which is the reality of our age, is developing day by day is known by everyone. With this development, the threat of cybersecurity has become even more serious and complex with the existence of Internet-connected systems in every area of our lives.

Traditional security mechanisms such as firewalls and antivirus software, which have been used for a long time, have become insufficient to combat developing cyber attacks that utilize automation, obscuration and advanced evasion techniques, and the "Artificial Intelligence" technology, which has developed incredibly in the last few years, has also begun to be used in cybersecurity.

AI has become a crucial asset in cybersecurity, enhancing threat detection, incident response, and overall network protection.

By leveraging machine learning, deep learning, and natural language processing [1], AI-powered cybersecurity solutions can process vast amounts of data, detect anomalies, and anticipate potential threats in real time.

However, although this situation is positive for cybersecurity, it also paves the way for various cyberattacks such as AI-supported cyberattacks.

Today, many countries, especially the USA, China and Russia, are developing AI-supported military systems. However, since AIs are developed by private companies, there is not enough government regulation.

Regarding the use of Artificial Intelligence in military and cybersecurity:

A) Weaponization of AI

If AI technology is used in military operations, it can make traditional weapon systems more efficient. However, the combination of nuclear weapons, chemical and biological weapons with AI can lead to undesirable results.

AI takes shape according to the data it is fed. Manipulation with malicious data can divert the technology it is used in from its purpose, as in the example of Microsoft's Tay Bot [2].

B) Weaponized AI in Cyberspace

With AI, automated cyber attacks that do not require human intervention can be created. AI-supported malware can identify and exploit security vulnerabilities in systems.

As can be seen, although AI's positive contribution to cybersecurity is high, AI-supported attacks harm both individuals and states by performing large-scale manipulations.

In conclusion, this article examines how AI can be used in cybersecurity in two ways: as a tool to improve security and as a method to launch more advanced cyberattacks. It examines how AI helps detect, predict, and respond to threats, as well as how attackers use AI to create smarter and more dangerous threats.

2. RELATED WORKS

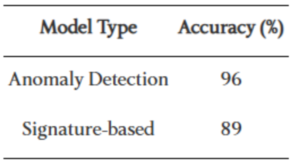
If AI can control the internet news network, it can be used to manipulate people’s thoughts and even to start war. The concept that caused AI to be much powerful as it is right now is the Singularity. Singularity is a hypothetical future where technology growth is out of control and irreversible [5].

A) MALWARE

Along with AI, malware has been developed that can bypass the antivirus program.

B) MACHINE LEARNING FOR CYBERSECURİTY

Anomaly detection methods are better at detecting zero-day attacks than signature-based models. Studies have shown that ML models can detect unseen threats with high accuracy when trained on a sufficiently diverse and large dataset.



Model Type	Accuracy (%)
Anomaly Detection	96
Signature-based	89

Figure 2.1 Comparison of Anomaly-based detection and Signature-based Detection [4].

C) DEEP LEARNING IN NETWORK SECURITY

The application of neural networks in identifying complex cyber threats has been studied in depth. It has been emphasized that Convolutional Neural Networks are effective in analyzing traffic patterns to detect attacks, even if there are activities aimed at blocking normal traffic.

D) IOT SECURRITY WITH ML

IoT is widely used in every aspect of our lives. Therefore, the security concerns associated with it have also increased rapidly. It has been discovered that ML algorithms can greatly reduce the security vulnerability in IoT networks.

E) AUTOMATED RESPONSE MECHANISMS

Automation of not only detection but also threat reduction is very important. The way ML models work with active response systems has also been investigated. Models are not limited to threat detection, taking preventive measures to neutralize threats without human intervention.

3. RESEARCH METHODOLOGY AND ARCHITECTURE

In this section, we will focus on the research methodology and project architecture. The project is about making predictions with the XGBoost machine learning model using the "UNSW-NB 15" dataset. The dataset contains 49 features and nine different types of attacks.

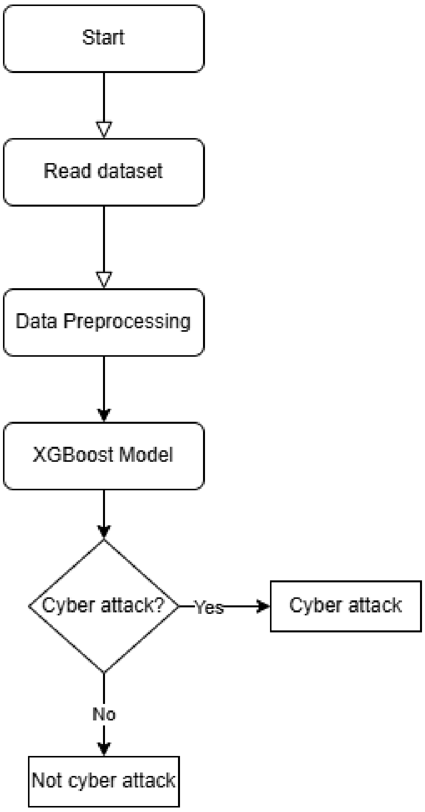
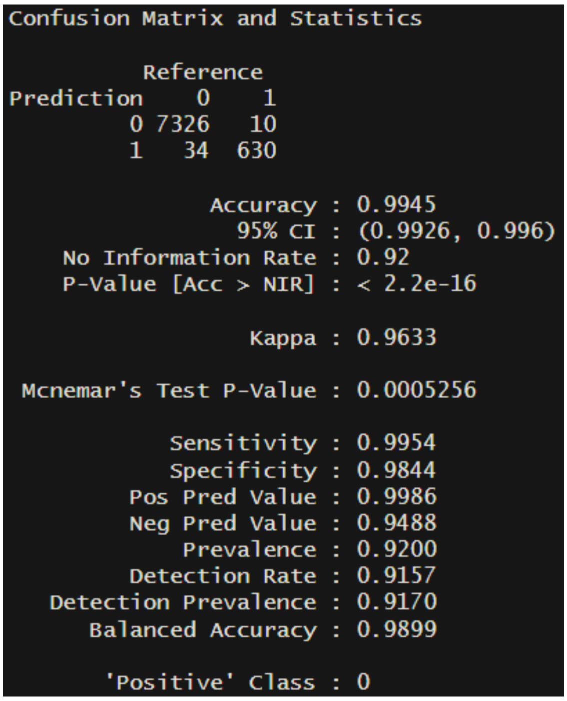


Figure 3.1 Flow Chart

Before starting to code the project, I researched which machine learning model would be suitable for analyzing this dataset. As a result of my research, I decided to use XGBoost. I used RStudio for coding. When starting to code, I loaded the necessary libraries "data.table", "caret" and "xgboost". Then, I pulled the feature names from the "NUSW-NB15_features.csv" file that holds the feature data of the dataset and assigned the feature names. I cleaned the missing (NA) data and removed the "attack_cat" column, which would affect the accuracy of the prediction model excessively, i.e. cause "data leakage", since it had a large effect on the calculation. The "proto, service, state" columns, which are categorical variables, were converted to factor types so that the model could process the data correctly. Single-valued columns were removed because they did not contribute to the model. One-Hot Encoding (making each category a separate column) was applied to categorical columns. Then I divided the dataset into train and test. XGBoost model parameters were determined and the model was trained. Finally, prediction was made and the results were evaluated.

4. TEST RESULTS AND COMMENTS

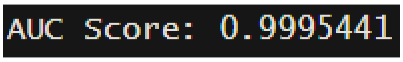


```
Confusion Matrix and Statistics

          Reference
Prediction    0    1
         0 7326   10
         1   34  630

               Accuracy : 0.9945
                 95% CI : (0.9926, 0.996)
    No Information Rate : 0.92
    P-Value [Acc > NIR] : < 2.2e-16

                  Kappa : 0.9633

 Mcnemar's Test P-Value : 0.0005256

            Sensitivity : 0.9954
            Specificity : 0.9844
         Pos Pred Value : 0.9986
         Neg Pred Value : 0.9488
             Prevalence : 0.9200
         Detection Rate : 0.9157
   Detection Prevalence : 0.9170
      Balanced Accuracy : 0.9899

       'Positive' Class : 0
```

Figure 4.1 Confusion Matrix and Statistics

- Values on the confusion matrix are True Positive=7326, False Negative=10, False Positive= 34, and True Negative= 630.
- The accuracy rate was 99.45%.
- The confidence interval of the model was (0.9926, 0.996).
- NIR shows the accuracy rate of the model in predicting the most common class (0).
- P-Value means model's accuracy is quite high.
- Kappa shows how much the accuracy of this model differs from the accuracy of another model.
- Mcnemar's Test shows that the model makes errors between certain classes.

We can observe how accurate the prediction is made by looking at the sensitivity, specificity, positive predicted value, negative predicted value, prevalence, detection rate, detection prevalence and balanced accuracy rates. Based on these results, we can say that the model performs well.



```
AUC Score: 0.9995441
```

Figure 4.2 AUC Score

The area under the ROC curve is named AUC score. When we observe the AUC score value of the prediction model, we see that the model can distinguish between attack and normal traffic values with 99.95% success.

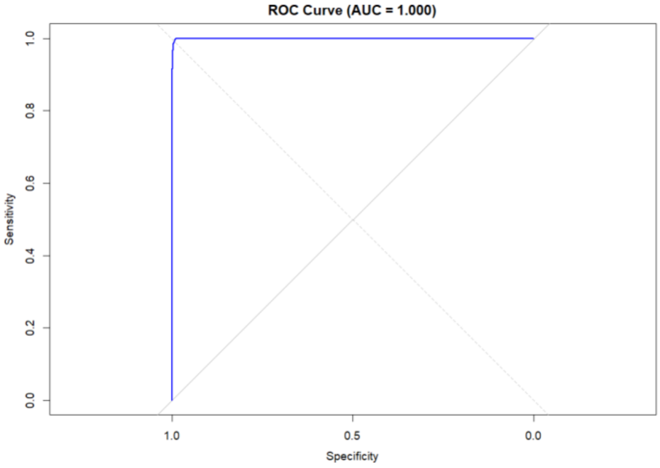


Figure 4.3 ROC Curve

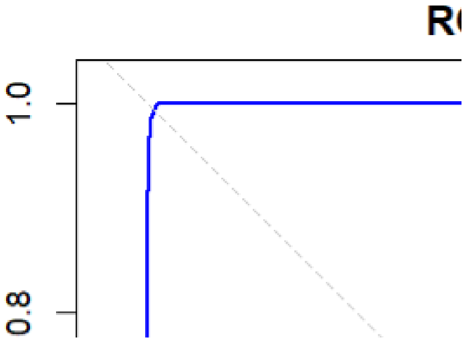


Figure 4.4 Zoomed In ROC Curve

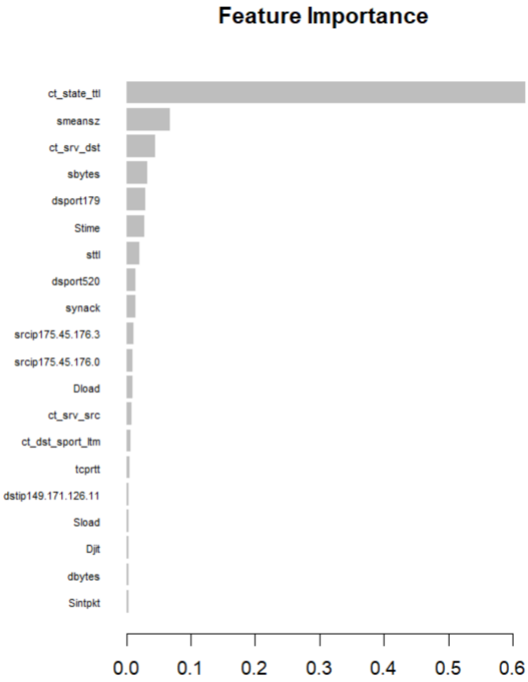
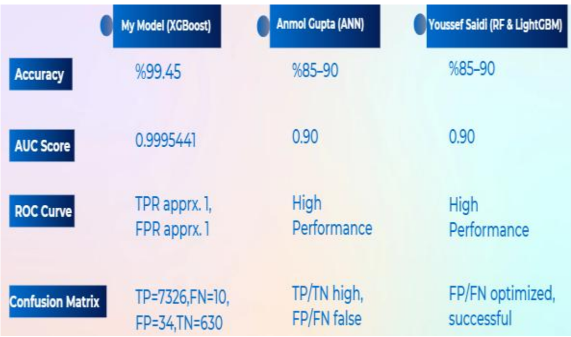


Figure 4.5 Feature Importance

Feature importance is a score calculation made to observe which feature will affect the model more. The higher the score of the feature, the more the model is affected. The "ct_state_ttl" feature received the highest score by far, followed by the "smeansz" feature with the second highest score.



	My Model (XGBoost)	Anmol Gupta (ANN)	Youssef Saidi (RF & LightGBM)
Accuracy	%99.45	%85-90	%85-90
AUC Score	0.9995441	0.90	0.90
ROC Curve	TPR apprx. 1, FPR apprx. 1	High Performance	High Performance

Confusion Matrix	TP=7326,FN=10,
	FP=34,TN=630
		TP/TN high,
		FP/FN false
			FP/FN optimized,
			successful

Figure 4.6 Comparison Table

5. CONCLUSION

To conclude, one of the many usage of AI is using machine learning models to predict the cyber attacks. Model can be changed with respect to the dataset we are using and the predicted feature.

REFERENCES

[1] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2(173). https://doi.org/10.1007/s42979-021-00557-0

[2] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2021). Weaponized AI for cyber attacks. Journal of Information Security and Applications, 57, 102722. https://doi.org/10.1016/j.jisa.2020.102722

[3] Chakraborty, A., Biswas, A., & Khan, A. K. (2022). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. arXiv. https://arxiv.org/abs/2209.13454

[4] Alionsi, D. D. D. (2023). AI-driven cybersecurity: Utilizing machine learning and deep learning techniques for real-time threat detection, analysis, and mitigation in complex IT networks. *Advances in Engineering Innovation*, 3, 27–31. https://doi.org/10.54254/2977-3903/3/2023036 ·

[5] TechTarget. (n.d.). *Singularity (the)*. Retrieved from https://www.techtarget.com/searchenterpriseai/definition/Singularity-the

[6] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 dataset). University of New South Wales. Retrieved from https://research.unsw.edu.au/projects/unsw-nb15-dataset

[7] Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." *Military Communications and Information Systems Conference (MilCIS)*, 2015. IEEE, 2015.

[8]Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset." *Information Security Journal: A Global Perspective* (2016): 1-14.

[9]Moustafa, Nour, et al. "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks." *IEEE Transactions on Big Data (2017).*

[10]Moustafa, Nour, et al. "Big data analytics for intrusion detection system: statistical decision-making using finite dirichlet mixture models." *Data Analytics and Decision Support for Cybersecurity. Springer, Cham, 2017.* 127-156.

[11]Sarhan, Mohanad, Siamak Layeghy, Nour Moustafa, and Marius Portmann. NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems. In *Big Data Technologies and Applications: 10th EAI International Conference, BDTA 2020, and 13th EAI International Conference on Wireless Internet, WiCON 2020, Virtual Event, December 11, 2020, Proceedings* (p. 117). Springer Nature.

[12] Built In. (n.d.). *What is feature importance?*. Built In. https://builtin.com/data-science/feature-importance

[13] Gupta, A. (n.d.). *UNSW_NB15 | Cybersecurity Threat Detection | ANN* [Kaggle Notebook]. Kaggle. https://www.kaggle.com/code/getanmolgupta01/unsw-nb15-cybersecurity-threat-detection-ann

[14] Saidi, Y. (n.d.). *UNSW-NB15 Cybersecurity Threat Detection* [Kaggle Notebook]. Kaggle. https://www.kaggle.com/code/youssefsaidi/unsw-nb15-cybersecurity-threat-detection