Network Intrusion Category Detection on UNSW-NB15 Dataset (NICD)

Fahim Faysal Apurba
Department of ECE
North South University
Dhaka, Bangladesh
fahim.apurba@northsouth.edu
1921442642

Sojibul Islam Sojib
Department of ECE
North South University
Dhaka, Bangladesh
sojibul.sojib@northsouth.edu
1921331642

Tanzim Khan
Department of ECE
North South University
Dhaka, Bangladesh
tanzim.khan@northsouth.edu
1913009642

MD Sabbir Hossain
Department of ECE
North South University
Dhaka, Bangladesh
sabbir.hossain02@northsouth.edu
1610443042

***Abstract*—Network Intrusion are becoming more frequent and sophisticated over time. Defense plans must adapt and continuously innovate in response to the complexity and sophistication that are rising. Despite their continued widespread usage, conventional intrusion detection and deep packet inspection techniques and advised, are insufficient to address the needs of escalating security risks. Using machine learning techniques, already many fabulous works has been done previously on this dataset, but all of them can only detect whether it is an attack or not. In this paper, our main focus was to detect the category of the attack and finding out the best performing machine learning algorithm among all possible algorithms that could have been applied. So, we have shown an approach called feature Filtering in the pre-processing stage, where all unnecessary features have been removed and prepared the dataset in an efficient manner. Then, we have applied various algorithm to find out the best performing algorithm among them. Finally, our approach has showed such a performance, which can be called state-of-the-art.**

***Index Terms*—Network Intrusion, feature Filtering, preprocessing, machine learning, security risks**

I. Introduction

Detecting cyber attacks is a crucial aspect of maintaining the security and integrity of computer systems and networks. Over the years, various projects and initiatives have been developed to improve the detection capabilities and respond effectively to cyber threats. Here is a background on some key aspects of detecting cyber attacks projects: Intrusion Detection Systems (IDS): Intrusion Detection Systems are software or hardware-based solutions designed to monitor network traffic and identify any suspicious or malicious activities[14]. IDS can be classified into two main types: network-based (NIDS) and host-based (HIDS). NIDS monitor network traffic, while HIDS analyze activities on individual hosts or devices. These systems use different techniques such as signature-based detection, anomaly detection, and behavioral analysis to identify potential cyber attacks. Security Information and Event Management (SIEM): SIEM systems collect and analyze security events and logs from various sources within a network. They provide a centralized view of the security posture and enable real-time monitoring, threat detection, and incident response.[11] SIEM solutions typically employ correlation rules, machine learning algorithms, and statistical analysis to identify patterns or anomalies that could indicate a cyber attack. Machine Learning and Artificial Intelligence (AI): Machine learning and AI techniques have gained prominence in cyber attack detection.[5]

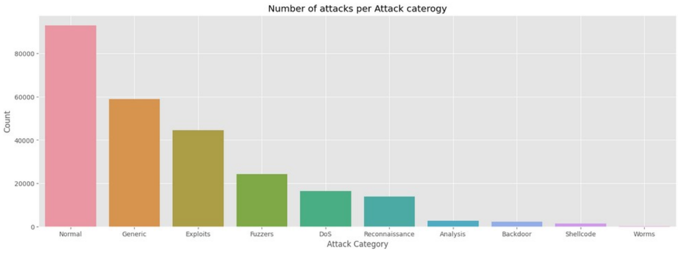


Fig. 1. Network Attack Categories

These technologies can analyze large volumes of data, identify patterns, and detect anomalies that may signify a cyber attack. Machine learning models can be trained on historical data to recognize known attack patterns and improve detection accuracy over time. AI-based systems can also adapt and learn from new threats to enhance their detection capabilities. Threat Intelligence: Threat intelligence involves gathering information about potential cyber threats and attackers to understand their motives, methods, and indicators of compromise.[13] Threat intelligence feeds provide real-time data on known malicious entities, attack techniques, and vulnerabilities. Integrating threat intelligence into detection systems enhances their ability to identify and respond to emerging cyber threats effectively. Collaborative Defense: Many organizations and security communities work together to share threat information and collaborate on cyber attack detection. Initiatives such as Information Sharing and Analysis Centers (ISACs), Computer Emergency Response Teams (CERTs), and industry-specific forums facilitate the exchange of threat intelligence, best practices, and incident response strategies. Collaboration helps in detecting attacks more efficiently by leveraging collective knowledge and resources. Big Data Analytics: With the ever-increasing volume of data generated in today's digital landscape, big data analytics plays a crucial role in cyber attack detection.

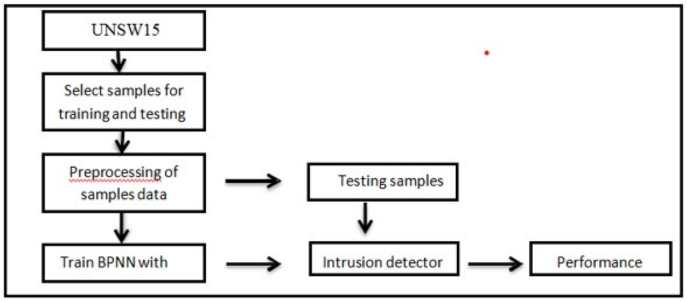

UNSW15
Select samples for training and testing
Preprocessing of samples data
Testing samples
Train BPNN with
Intrusion detector
Performance

Fig. 2. machine learning approach to detect NICD

Analyzing vast amounts of structured and unstructured data can uncover hidden patterns and indicators of compromise. Big data platforms enable real-time processing, storage, and analysis of diverse data sources, enabling organizations to detect and respond to cyber attacks more effectively. Threat Hunting: Threat hunting is a proactive approach to cyber attack detection that involves actively searching for threats within an organization's network or systems. It combines human expertise and automated tools to identify advanced and persistent threats that may evade traditional security measures. Threat hunters use various techniques, including log analysis, behavior analysis, and penetration testing, to detect and mitigate cyber attacks before they cause significant damage. These projects and approaches collectively contribute to the ongoing effort to enhance the detection of cyber attacks. As cyber threats evolve, organizations and security professionals continually refine their strategies and leverage new technologies to stay ahead of attackers and protect critical systems and data[16].

Inspired by this observation, Mirzadeh et al. [17] proposed and worked on a new distillation framework called Teacher Assistant Knowledge Distillation, which introduces intermediate neural networks (teacher-assistant/TA) between the teacher and student to try and bridge the gap between the two. Chen et al. [18] worked on improving the capability of the student model by reusing the teacher classifier for better generalization of the outputs.

In this paper, we leverage the concepts introduced to run a series of experiments in an attempt to narrow the rift regarding performance and accuracy after knowledge distillation compared to the teacher. We implement the TAKD framework, where there is a pre-trained teacher model, a teacher-assistant/TA model, and a student model. Knowledge distillation occurs from the teacher to the TA to the student model. The student model reuses the fully connected layer/classifier layer of the teacher model to help better generalize the outputs, in addition to utilizing the dark knowledge obtained from the TA model by distillation. An illustration of our proposed idea is demonstrated in.

II. Related Work

A study by Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, Farhan Ahmad in 2020 explored Network intrusion detection system: A systematic study of machine learning and deep learning approaches. This study first clarifies the concept of IDS and then provides the taxonomy based on the notable ML and DL techniques adopted in designing network-based IDS (NIDS) systems.In this study they found accuracy as high as 95 percent[1].An application of machine learning to network intrusion detection by C. Sinclair,L. Pierce,S. Matzner describes the machine learning methodology and the applications employing machine learning to network intrusion detection.they have adapted existing machine learning applications to develop rules for a deployed IDS. The rule generation component of NEDAA is layered onto an expert system that enhances the ability of the IDS to filter anomalous connections.The main result of the presented material is the production of rules for compilation into the expert system[2].An article Machine Learning for Reliable Network Attack Detection in SCADA Systems by Rocio Lopez Perez, Florian Adamsky†, Ridha Soua†, and Thomas Engel† describes Machine Learning (ML) for intrusion detection in SCADA systems using a real data set collected from a gas pipeline system and provided by the Mississippi State University (MSU). The contribution of this paper is twofold: 1) The evaluation of four techniques for missing data estimation and two techniques for data normalization, 2) The performances of Support Vector Machine (SVM), and Random Forest (RF) are assessed in terms of accuracy, precision, recall and F1 score for intrusion detection. Two cases are differentiated: binary and categorical classifications.They provided a complete comparison between these algorithms along with the random hyper-parameter search results[3]. A study Internet of Things Cyber Attacks Detection using Machine Learning by Jadel Alsamiri , Khalid Alsubhi describes various machine learning algorithms that can be used to quickly and effectively detect IoT network attacks. A new dataset, Bot-IoT, is used to evaluate various detection algorithms. In the implementation phase, seven different machine learning algorithms were used, and most of them achieved high performance[4].Modern smart grid systems are heavily dependent on Information and Communication Technology, and this dependency makes them prone to cyber-attacks.Sequential Supervised Machine Learning Approach for Cyber Attack Detection in a Smart Grid System by Yasir Ali Farrukh ,Zeeshan Ahmad, Irfan Khan,Rajvikram Madurai Elavarasan describe two-layer hierarchical machine learning model having an accuracy of 95.44 percent to improve the detection of cyberattacks. The first layer of the model is used to distinguish between the two modes of operation - normal state or cyberattack. The second layer is used to classify the state into different types of cyberattacks[5].With the development of the Internet, cyber-attacks are changing rapidly and the cyber security situation is not optimistic.A study "Machine Learning and

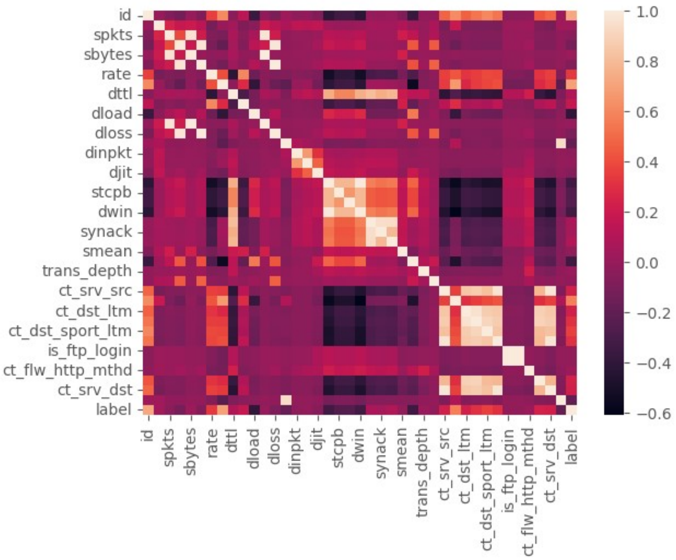


Fig. 3. correllation matrix

Deep Learning Methods for Cybersecurity” by Yang Xin, Lingshuang Kong , Zhi Liu, , Yuling Chen , Yanmiao Li , Hongliang Zhu , Mingcheng Gao , Haixia Hou , Chunhua Wang ,the paper report describes machine learning (ML) and deep learning (DL) methods for network analysis of intrusion detection and provides a brief tutorial description of each ML / DL method. Papers representing each method were indexed, read, and summarized based on their temporal or thermal correlations.The paper, which has mostly focused on the last three years, introduces the latest applications of ML and DL in the field of intrusion detection[6].Artificial intelligence (AI), and in particular machine learning(ML), deep learning (DL) has seen huge pace in recent years and is now set to really start influencing all aspects of community and occupations in which people are engaged.”The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace”by B. Geluvaraj, P. M. Satwik and T. A. Ashok Kumar describes the challenges and what is the role of AI, ML, and DL in avoiding attack in future[7].

III. Proposed Methodology

The main method was feature filtering in a very optimum manner. We have made a correlation matrix of all features. Then, we have find out the best features among them. After that we have clean the dataset properly and transform the all features into numaric values. Then, we applied all possible algorithm of ML and we have reached to the realization that random forest has been working best in detecting the category of the attack.

A. *Dataset:*

The UNSW-15 dataset is a widely used dataset in the field of network security and intrusion detection. It was developed by researchers at the University of New South Wales (UNSW), Australia. The primary objective of this dataset is to facilitate the development and evaluation of network intrusion detection systems (NIDS) by providing a realistic and comprehensive collection of network traffic data.

The dataset is derived from real-world network traffic captured in a controlled environment. It contains a diverse range of network attack scenarios, including different types of intrusion attempts and malicious activities. These attack categories cover a wide range of behaviors such as Denial of Service (DoS), probing, unauthorized access, and more. In addition to attack traffic, the dataset also includes normal traffic patterns to enable the detection of anomalous behavior. The UNSW-15 dataset provides detailed features extracted from network traffic flows. These features encompass various aspects of the communication, including source and destination IP addresses, port numbers, protocols, flow durations, packet lengths, inter-arrival times, flags, and statistical properties. These features are designed to capture both packet-level characteristics and higher-level flow-level properties.

With a total of 70 features, the dataset offers rich and diverse information for researchers and practitioners to explore different approaches in feature engineering, machine learning algorithms, and anomaly detection techniques. The availability of labeled samples for different attack categories allows for supervised learning tasks, enabling the development and evaluation of accurate attack classification models.

By utilizing the UNSW-15 dataset, researchers and practitioners can benchmark their intrusion detection algorithms, compare the performance of different methods, and develop robust and effective network security solutions. The dataset has played a significant role in advancing the field of network security, enabling the development of more sophisticated and reliable intrusion detection systems to protect against evolving cyber threats.

The UNSW-15 dataset includes the following 70 features:

Source IP, Destination IP, Source Port, Destination Port, Protocol, Timestamp, Flow Duration, Total Fwd Packets, Total Backward Packets, Total Length of Fwd Packets, Total Length of Bwd Packets, Fwd Packet Length Max, Fwd Packet Length Min, Fwd Packet Length Mean, Fwd Packet Length Std, Bwd Packet Length Max, Bwd Packet Length Min, Bwd Packet Length Mean, Bwd Packet Length Std, Flow Bytes/s, Flow Packets/s, Flow IAT Mean, Flow IAT Std, Flow IAT Max, Flow IAT Min, Fwd IAT Total, Fwd IAT Mean, Fwd IAT Std, Fwd IAT Max, Fwd IAT Min, Bwd IAT Total, Bwd IAT Mean, Bwd IAT Std, Bwd IAT Max, Bwd IAT Min, Fwd PSH Flags, Bwd PSH Flags, Fwd URG Flags, Bwd URG Flags, Fwd Header Length,

Fwd Packets/s, Bwd Packets/s, Min Packet Length, Max Packet Length, Packet Length Mean, Packet Length Std, Packet Length Variance, SYN Flag Count, ACK Flag Count, URG Flag Count, CWE Flag Count, Down/Up Ratio, Average Packet Size, Avg Fwd Segment Size, Avg Bwd Segment Size, Fwd Avg Bytes/Bulk, Fwd Avg Packets/Bulk, Fwd Avg Bulk Rate, Bwd Avg Bytes/Bulk, Bwd Avg Packets/Bulk, Bwd Avg Bulk Rate, Subflow Fwd Packets, Subflow Fwd Bytes, Subflow Bwd Packets, Subflow Bwd Bytes, InitWinbytesForward, InitWinbytesBackward, actDataPktFwd, minSegSizeForward.

B. Pre-processing the Dataset

The splitting of the UNSW-15 dataset is an essential step in machine learning tasks to ensure unbiased evaluation and effective model development. Typically, the dataset is divided into three main subsets: the training set, the validation set, and the test set. The splitting process aims to allocate data samples to these subsets while maintaining a balance between attack categories and preserving the integrity of the dataset.

Training Set: The training set comprises the largest portion of the dataset and is used for model training. It is crucial for the model to learn patterns and features from this set. Around 80 percent of the dataset is allocated to the training set. The training set has included a representative distribution of normal traffic and various attack categories to ensure that the model learns to distinguish between them effectively.

Test Set: The test set is used for the final evaluation of the trained model's performance. It provides an unbiased assessment of the model's ability to generalize to unseen data. The test set should include a representative distribution of normal traffic and attack categories that were not encountered during the training and validation phases. Generally, around 20 percent of the dataset is allocated to the test set.

Then, we have removed all unnecessary features from the dataset. We have removed 41 features among 70. Actually, we figured out the unnecessary features through feature filtering correlation matrix. Then, we have converted all the categorical values into numerical values before applying algorithm.

C. Applied Algorithms

Extreme Learning Machine:

Extreme Learning Machine (ELM) is a learning algorithm that utilizes feedforward neural networks with a single layer or multiple layers of hidden nodes. These hidden nodes are tuned at random and their corresponding output weights are analytically determined by the algorithm. According to the creators, this learning algorithm can produce good generalization performance and can learn a thousand times faster than conventional learning algorithms for feedforward neural networks, this is how it works(Huang, Zhu, and Siew 2006).[9]

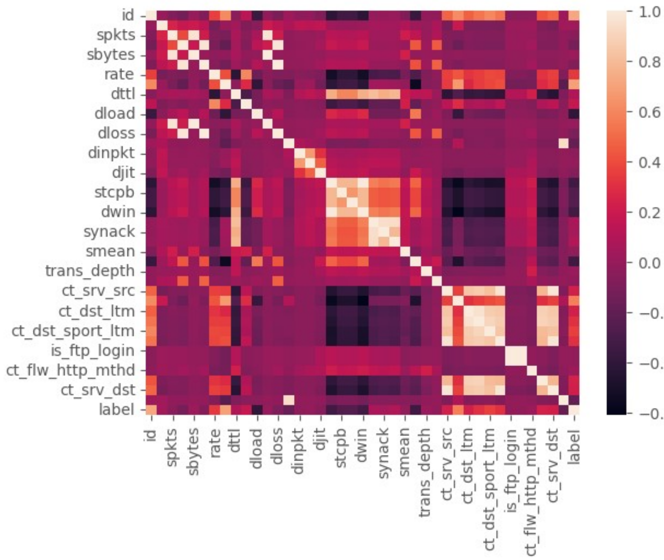


Fig. 4. correllation matrix

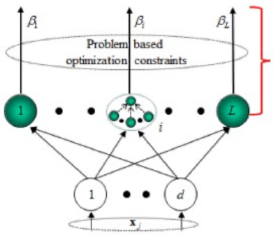


Fig. 5. Simplified illustration of ELM Algorithm(Huang 2015)

Random Forest:

Random Forest (RF) is a supervised machine learning algorithm that involves the use of multiple decision trees in order to perform classification and regression tasks (Ho 1995). The Random Forest algorithm is considered to be an ensemble machine learning algorithm as it involves the concept of majority voting of multiple trees. The algorithm's output, represented as a class prediction, is determined from the aggregate result of all the classes predicted by the individual trees. Recent studies have explored the capabilities of Random Forest in security attacks, specifically in injection attacks, spam filtering, malware detection and more (Kapoor, Gupta, and Kumar 2018 and Khorshidpour, Hashemi, and Hamzeh 2017)[9].

Support Vector Machine:

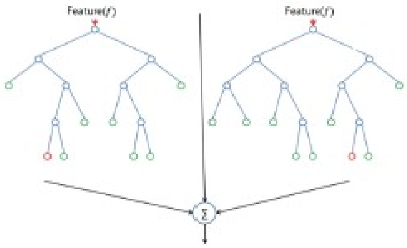


Fig. 6. Simplifed illustration of the Random Forest Algorithm(Khorshidpour, Hashemi, and Hamzeh 2017)

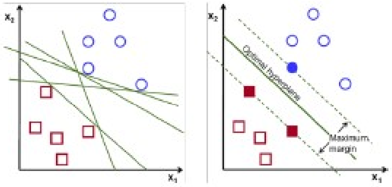


Fig. 7. Simplified illustration of the Support Vector Machine(Gandhi 2018)

Support Vector Machine (SVM) is a supervised learning model used for regression and classifcation analysis. It is highly preferred for its high accuracy with less computation power and complexity. SVM is also used in computer security, where they are used for intrusion detection. For example, One class SVM was used for analyzing records based on a new kernel function (Wagner, Francois, Engel, et al. 2011) and accurate Internet traffic classification (Yuan et al. 2010).[9]

Logistic Regression:
Logistic regression is a supervised learning model that is used as a method for binary classification. The term itself is borrowed from Statistics. At the core of the method, it uses logistic functions, a sigmoid curve that is useful for a range of fields including neural networks. Logistic regression models the probability for classification problems with two possible outcomes. Logistic regression can be used to identify network traffic as malicious or not (Bapat et al. 2018).[7]

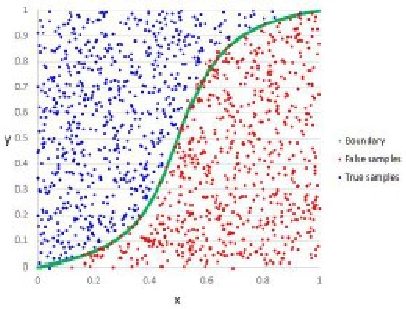
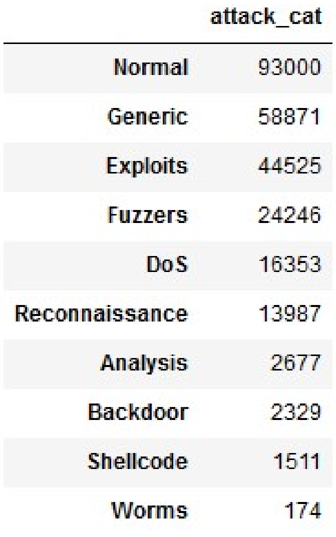


Fig. 8. Simplied Illustration of the Support Vector Machine (Brid 2018)



	attack_cat
Normal	93000
Generic	58871
Exploits	44525
Fuzzers	24246
DoS	16353
Reconnaissance	13987
Analysis	2677
Backdoor	2329
Shellcode	1511
Worms	174

Fig. 9. number of categorical attacks

D. Reproducibility

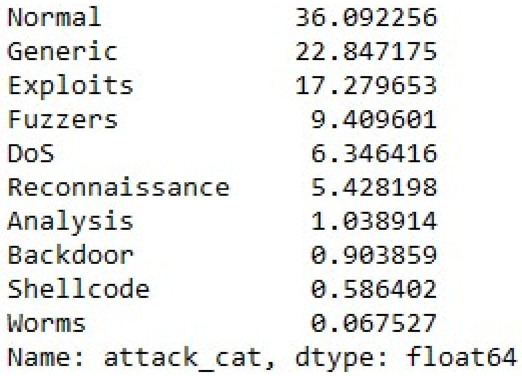
All experimental settings, including dataset details, model architectures, hyperparameters, and training procedures have been documented to ensure reproducibility.

IV. Results and Analysis

After applying our method **feature filtering**, we have left with 29 efficient features and these are:
'dur', 'proto', 'service', 'state', 'spkts', 'dpkts', 'sbytes','dbytes', 'rate', 'sttl', 'dttl', 'sload', 'sloss', 'dloss', 'sinpkt', 'swin', 'stcpb', 'dtcpb', 'dwin', 'dmean', 'ctSrvSrc', 'ctStateTtl','ctDstDtm', 'ctSrcDportLtm', 'ctDstPortLtm', 'ctDstSrcLtm','ctSrcLtm', 'ctSrvDst', 'attackCat',
at the pre-processing stage and we have transformed all the values to numerical.
Here, our target category was **AttackCategory** not **label**, because, our main goal was to detect the catagory of attack though we also find out the performance of the of label for our approach (whether it is an attack or not).
Nevertheless, there are 10 types of attack and these are:
'Reconnaissance', 'Shellcode', 'Fuzzers', 'Generic', 'Analysis', 'Exploits', 'DoS', 'Backdoor', 'Worms', 'Normal'.
Most importantly here, we consider also 'normal' as a category of attack.

Then, we apply various suitable algorithm to experience the performance.

And after experiment we get for 'label' (whether it's an attack or not):



```
Normal            36.092256
Generic           22.847175
Exploits          17.279653
Fuzzers            9.409601
DoS                6.346416
Reconnaissance     5.428198
Analysis           1.038914
Backdoor           0.903859
Shellcode          0.586402
Worms              0.067527
Name: attack_cat, dtype: float64
```

Fig. 10. percent of categorical attacks

TABLE I
PERFORMANCE COMPARISON FOR TRAIN AND TEST DATASET FOR ALREADY EXISTED WORKS AND OUR WORK:

	Performance (Accuracy)	
	Train set	**Test set**
Our Approach	**100.0**	**100.0**
Best Of others'	**96.85**	**95.21**

From this table we can say that our feature filtering approach shows a state-of-the-art.

TABLE II
PERFORMANCE COMPARISON TABLE FOR OUR MAIN GOAL WHICH IS ATTACK CATEGORY DETECTION FOR THE ALGORITHM WHICH IS WORKING BEST

	Performance (Accuracy)	
	Train set	**Test set**
Random forest	**91.62**	**82.89**
ETA	**91.11**	**81.93**
Logistic Regression	**89.41**	**49.25**
KNN, p=1	**68.59.41**	**66.55**
KNN, p=2	**68.35**	**66.52**
Decision Tree	**time consuming(not working)**	**(not working)**
Naive Bayes	**46.87**	**47.27**
Polynomial Regression	**(not applicable**	**(not applicable**

So, from this table we can say the Random Forest algorithm is working best for attack category detection and also label detection as well.

V. CONCLUSION

Here, successfully achieved out goal of network attack category detection with a very handsome performance and also able to find the best performing algorithm for this case and which is 'Random Forest'. Moreover, our optimized feature filtering technique works greatly.

VI. ACKNOWLEDGMENT

First and foremost, I would like to thank Allah (SWT) for granting me permission to work on this project and for providing me with a bountiful supply of resources.

I would like to express my gratitude to Rifat Sir,my instructor for his advice and ongoing assistance in finishing this undertaking. He provided me with some helpful advice on how to improve the project and how to do effective research. My supervisor's patience and support have motivated me to be more imaginative in this assignment.Even though I don't often see him, his words never leave my ears. We are grateful for this wonderful chance.

Thank you also to all my fellow friends that help me a lot in completing this project. They always give advice and guidance to make sure that we will do excellent work. Lastly, I would like to thank all of the people who have contributed directly or indirectly towards the success of this project.

REFERENCES

[1] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and Deep Learning Approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, 2020. doi:10.1002/ett.4150

[2] C. Sinclair, L. Pierce, and S. Matzner, "An application of machine learning to network intrusion detection," Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99). doi:10.1109/csac.1999.816048

[3] R. Lopez Perez, F. Adamsky, R. Soua, and T. Engel, "Machine learning for reliable network attack detection in SCADA systems," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018. doi:10.1109/trustcom/bigdatase.2018.00094

[4] J. Alsamiri and K. Alsubhi, "Internet of things cyber attacks detection using machine learning," International Journal of Advanced Computer Science and Applications, vol. 10, no. 12, 2019. doi:10.14569/ijacsa.2019.0101280

[5] Y. A. Farrukh, Z. Ahmad, I. Khan, and R. M. Elavarasan, "A sequential supervised machine learning approach for cyber attack detection in a smart grid system," 2021 North American Power Symposium (NAPS), 2021. doi:10.1109/naps52732.2021.9654767

[6] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018. doi:10.1109/access.2018.2836950

[7] B. Geluvaraj, P. M. Satwik, and T. A. Ashok Kumar, "The future of cybersecurity: Major role of Artificial Intelligence, Machine Learning, and Deep Learning in cyberspace," International Conference on Computer Networks and Communication Technologies, pp. 739–747, 2018. doi:10.1007/978-981-10-8681-6$_6$7

[8] DETECTION OF CYBER ATTACK IN NETWORK BY USING MACHINE LEARNING, 1G UTHEJ, 2K MOHAMMED HUZAIFA, 3BALA SURESH BABU, 4A SAI KUMAR, 5Dr. C.GULZAR 1234B.Tech Student , 5Associate Professor DEPARTMENT OF CSE Dr. K. V. SUBBAREDDY INSTITUTE OF TECHNOLOGY, KURNOOL. Vol 13, Issue 06, June/2022 ISSN NO:0377-9254

[9] Cyber Attack Detection thanks to Machine Learning Algorithms, COMS7507: Advanced Security Antoine Delplace a.delplace@uq.net.au, Sheryl Hermoso, s.hermoso@uq.net.au, Kristofer Anandita k.anandita@uq.net.au University of Queensland, May 17, 2019

[10] Defang Chen, Jian-Ping Mei, Yuan Zhang, Can Wang, Zhe Wang, Yan Feng, and Chun Chen. Cross-layer distillation with semantic calibration. In *Proceedings of the AAAI Conference on Artificial Intelligence*, pages 7028–7036, 2021

[11] Cyber-attack Detection Strategy Based on Distribution System State Estimation, Huan Long, Member, IEEE, Zhi Wu, Member, IEEE, Chen Fang, Wei Gu, Senior Member, IEEE, Xinchi Wei, and Huiyu Zhan

[12] Deep Anomaly Detection with Deviation Networks, Guansong Pang, Chunhua Shen, Anton van den Hengel, Australian Institute for Machine, The University of Adelaide, Adelaide, Australia

[13] Detecting web attacks with end-to-end deep learning, Yao Pan1* , Fangzhou, Zhongwei Teng1, Jules White1, Douglas C. Schmidt1, Jacob Staples2, Pan et al. Journal of Internet Services and Applications (2019) 10:16 https://doi.org/10.1186/s13174-019-0115-x and Lee Krause2

[14] Cyber Attack Detection Dataset: A Review To cite this article: Nur Nadiah Mohd Yusof and Noor Suhana Sulaiman 2022 J. Phys.: Conf. Ser. 2319 012029

[15] Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach Mehmet Necip Kurt, Oyetunji Ogundijo, Chong Li, and Xiaodong Wang.

[16] A Review of Big Data in Network Intrusion Detection System: Challenges, Approaches, Datasets, and Tools Reem Alshamy1*, Mossa Ghurab2 1,2Dept. of Computer Science, Faculty of Computer and Information Technology (FCIT), Sana'a University, Sana'a, Yemen *Corresponding Author: r.alshamy@su.edu.ye, Tel.: +967-770609449 DOI: https://doi.org/10.26438/ijcse/v8i7.6275 — Available online at: www.ijcseonline.org

[17] DETECTION OF CYBER ATTACK IN NETWORK BY USING MACHINE LEARNING, 1G UTHEJ, 2K MOHAMMED HUZAIFA, 3BALA SURESH BABU, 4A SAI KUMAR, 5Dr. C.GULZAR 1234B.Tech Student , 5Associate Professor DEPARTMENT OF CSE Dr. K. V. SUBBAREDDY INSTITUTE OF TECHNOLOGY, KURNOOL. Vol 13, Issue 06, June/2022 ISSN NO:0377-9254