# Intelligent Anomaly Detection System Based on Ensemble and Deep Learning

Babu Kaji Baniya
*Dept. of Computer Science & Information Systems*
*Bradley University*
Peoria, IL, United States
bbaniya@fsmail.bradley.edu

Thomas Rush
*Dept. of Computer Science & Information Systems*
*Bradley University*
Peoria, IL, United States
trush@mail.bradley.edu

***Abstract*—The ubiquity of the Internet plays a pivotal role in connecting individuals and facilitating easy access to various essential services. As of 2022, the International Telecommunication Union (ITU) reports that approximately 5.3 billion people are connected to the internet, underscoring its widespread coverage and indispensability in our daily lives. This expansive coverage enables a myriad of services, including communication, e-banking, e-commerce, online social security access, medical reporting, education, entertainment, weather information, traffic monitoring, online surveys, and more. However, this open platform also exposes vulnerabilities to malicious users who actively seek to exploit weaknesses in the virtual domain, aiming to gain credentials, financial benefits, or reveal critical information through the use of malware. This constant threat poses a serious challenge in safeguarding sensitive information in cyberspace. To address this challenge, we propose the use of ensemble and deep neural network (DNN) based machine learning (ML) techniques to detect malicious intent packets before they can infiltrate or compromise systems and applications. Attackers employ various tactics to evade existing security systems, such as antivirus or intrusion detection systems, necessitating a robust defense mechanism. Our approach involves implementing an ensemble, a collection of diverse classifiers capable of capturing different attack patterns and better generalizing from highly relevant features, thus enhancing protection against a variety of attacks compared to a single classifier. Given the highly unbalanced dataset, the ensemble classifier effectively addresses this condition, and oversampling is also employed to minimize bias toward the majority class. To prevent overfitting, we utilize Random Forest (RF) and the dropout technique in the DNN. Furthermore, we introduce a DNN to assess its ability to recognize complex attack patterns and variations compared to the ensemble approach. Various metrics, such as classification accuracy, precision, recall, F1-score, confusion matrix are utilized to measure the performance of our proposed system, with the aim of outperforming current state-of-the-art intrusion detection systems.**

***Index Terms*—cybersecurity, deep neural network, ensemble, generalizing**

## I. Introduction

Internet connectivity has brought about a tremendous transformative impact in various domains, encompassing communication, information sharing, and the provision of goods and services. According to statistics from the ITU, approximately 5.3 billion individuals were connected to the internet in 2022, as illustrated in Figure 1 [1]. This figure reflects the incremental growth of internet users from 2005 to 2018, with a substantial 24% increase since 2019, particularly following the onset of the pandemic. With the rapid expansion of internet access comes numerous advantages, but it also introduces formidable cybersecurity challenges. In the virtual environment, just like in the physical world, individuals with malicious intentions are consistently active around the clock [2]. To safeguard computer systems and network resources from unauthorized access and protect critical information and user credentials, several robust cybersecurity measures are employed. These measures include the implementation of firewalls, data encryption, various authentication techniques, antivirus software, and intrusion detection systems, among others [3]. These security practices are pivotal in defending against cyber threats, although they do not provide absolute guarantees of protection for computer systems and networks. Cybersecurity experts emphasize that cyberattacks are concerted efforts aimed at undermining the fundamental principles of confidentiality, integrity, and availability (CIA) within computer systems [4], [5].

Each cyber attack has unique sophisticated technique that causes the severe flaw of security measure (tools) in detection (before compromise the system). For example, denial of service (DoS) attack prevents the legitimate user for accessing the network and host computer, distributed denial of service (DDoS) attacks accomplish by flooding the ACK to target system/network using different sources to make service unable to user/s, and malware, characterized as a malevolent piece of software, is meticulously crafted to inflict harm upon computers, networks, and manipulate user data [6], [7]. This category encompasses an array of malicious entities such as computer viruses, worms, trojan horses, ransomware, spyware, and other insidious code [8], [9].

A low-footprint attack aims to minimize traces and evade remaining undetected for as long as possible, allowing attackers to achieve their goals with a reduced risk of being discovered. Many research studies and innovative ideas have already been put forward to develop an intelligent Intrusion Detection System (IDS) as a solid line of defense against low-footprint attacks. The IDS is classified into two major categories: Misuse-based Intrusion Detection System (MDS) and Anomaly-based Intrusion Detection System (ADS) [5], [10], [11]. MDS monitors network traffic or host traces to match observed behaviors against known threats and their indicators of compromise (IoCs), such as malicious network attacks, file hashes, byte sequences, etc. Although it provides higher detection rates and lower false positive rates (FPRs), it cannot identify zero-day attacks [6] or even variants of existing attacks. Moreover, it requires significant effort and expertise to frequently update the threat, involving a set of rules for each attack type [12]. On the other hand, an ADS creates a legitimate profile of network or host events and, using learning algorithms, detects any deviation from it as an anomaly. As it can detect both existing and new attacks, including zero-day attacks, and unlike MDS, does not require effort to generate rules or search for known IoCs. It simply identifies out-of-ordinary patterns better to trigger alerts than MDS when its detection method is well designed [3].

Despite the unweighted advantages of ADS, it encounters several challenges in terms of its applications. These challenges include dealing with dynamic environments since systems and networks evolve continuously, requiring constant updates and baseline monitoring [13]. Another challenge is scalability, as it may struggle to effectively monitor large and complex networks. This is because networks consist of various components, software, and platforms, each handling significant data volumes, high data rates, and a wide variety of dimensionality, making it more difficult for ADS to operate efficiently [3]. The backbone of ADS techniques typically includes ML, data mining, statistical models, fuzzy sets, knowledge bases, and various other methods and tools to detect and identify anomalies in network and system behavior [14]–[16]. These techniques are the fundamental building blocks of ADS.

UNSW-NB15 encompasses nine distinct types of cyber attack classes, each exhibiting unique attack patterns. Recognizing that a single classifier may struggle to effectively capture all nine patterns, including one for the normal class, we adopt an ensemble approach as best practice. An ensemble combines multiple classifiers, leveraging the strengths of each; if one classifier fails to grasp a particular attack pattern, others may fill the gap, enhancing network defense and safeguarding critical information. Although dataset comprises numerous features, their significance in detecting attack patterns varies. To address this variability, we incorporate a feature selection algorithm to identify the most relevant features for our feature pool [18], [19]. Additionally, we also introduce DNNs for their prowess in learning complex patterns

ISBN 979-11-88428-12-0 ICACT2024 February 04 ~ 07, 2024

and representations from input features. DNNs introduce non-linearities through activation functions, enabling them to model intricate relationships and capture dependencies within the features. Their ability to autonomously discover relevant features enhances pattern recognition. Thus, we employ DNNs for the detection of both normal and attack patterns, including the nine sub-categories.

Following the structured organization of the paper, Section II delves into the exploration of the anomaly-based method, providing a comprehensive understanding of this approach. In Section III, we conduct a meticulous description of the dataset used in the study. Moving forward, Section IV investigates the experimental results of both RF and DNN classifiers, presenting key findings and engaging in a thorough discussion. Finally, Section V encapsulates the paper, offering a succinct yet insightful conclusion that summarizes key takeaways and outlines potential directions for future work.

## II. Anomaly-based Intrusion Detection

Anomaly-based scenarios present a multitude of challenges. Firstly, the uneven distribution of samples among classes, where one class significantly outweighs the other, may introduce a bias toward the majority of samples, posing a hurdle for effective machine learning models. The imbalance in the UNSW dataset is notably evident, as highlighted in Table I. Class samples manifest unexpected variations, exemplified by the Normal class with the highest number of samples at 37,000 for training and 56,000 for testing, while Worms exhibit lower numbers at 44 for training and 130 for testing. Intruders continually evolve their techniques to circumvent existing security measures, presenting a challenge for traditional machine learning models, which may struggle to adapt without substantial modification, updates, or immediate human intervention. Additionally, the identification of relevant attack features, as shown in Figure 4 (the vertical axis represents the selected features, and the horizontal axis represents the feature importance), is crucial for precise anomaly detection in complex and high-dimensional datasets. To tackle this challenge, we introduce a feature selection technique to identify pertinent features from a feature pool [17]. Furthermore, we employ an ensemble approach, specifically random forest, for complex pattern recognition. The introduction of deep neural networks further enhances detection capabilities, collectively addressing the multifaceted challenges in anomaly misuse detection.

Due to the substantial variation in class samples within the UNSW-NB15 dataset [18], we addressed the imbalance by augmenting the size of the minority class through the generation of new instances. While this strategy enhances the model's ability to learn the minority class pattern, it also poses the risk of overfitting. To mitigate this risk, we carefully chose RF as an ensemble learning algorithm. RF constructs multiple decision trees and combines their predictions, offering resilience against overfitting compared to individual decision trees. Similarly, to counteract overfitting in DNNs, we implemented dropout as a regularization technique. Dropout functions by randomly deactivating a fraction of neurons in a layer during training, preventing the co-adaptation of hidden units and promoting independence among neurons. This dual approach contributes to a more robust and generalizable model.

TABLE I: UNSW-NB15 training and testing samples distribution in each class.

| Class | | Training samples | Testing samples |
|---|---|---|---|
| Normal | | 37,000 | 56,000 |
| Attack | Generic | 18871 | 40,000 |
| | Exploits | 11,132 | 33,393 |
| | Fuzzers | 6,062 | 18,184 |
| | DoS | 4,089 | 12,264 |
| | Reconnaissance | 3,496 | 10,491 |
| | Analysis | 677 | 2,000 |
| | Backdoor | 583 | 1,746 |
| | Shellcode | 378 | 1,133 |
| | Worms | 44 | 130 |

## III. Dataset Description

We employed the well-known intrusion detection UNSW-NB15 dataset to evaluate the performance of our proposed system. This dataset comprises normal and attack categories, with a particular focus on nine distinct sub-categories of attacks, namely: Backdoors, DoS, Exploits, Fuzzers, Reconnaissance, Shellcode, Analysis, Generic, and Worms shown in Table II. The dataset is further divided into a training set and a testing set, with the training set comprising 82,332 samples and the testing set containing 175,341 samples, resulting in a total of 257,673 data samples. It's worth noting that both the training and testing datasets are imbalanced (in term of classes: normal and attack, and corresponding sub-classes samples of attack), and we presented their distribution in percentages using pie charts in Figure 2.

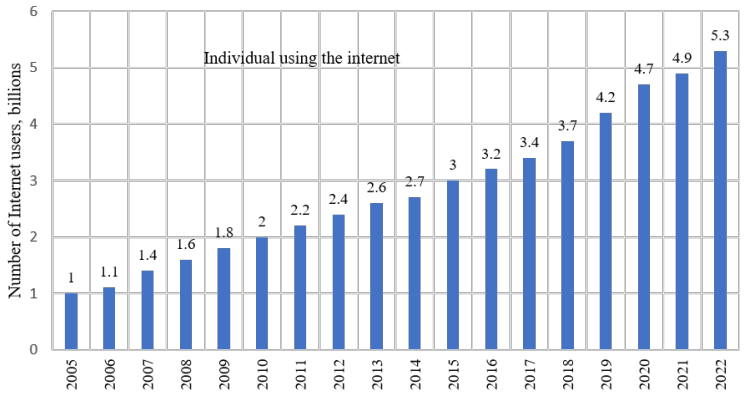



Fig. 1: It shows the increasing trend of internet users in the world's population in each year since 2005, the vertical axis presents the number of internet users in billion (around 66% of the world population using the internet) and horizontal axis represents year.

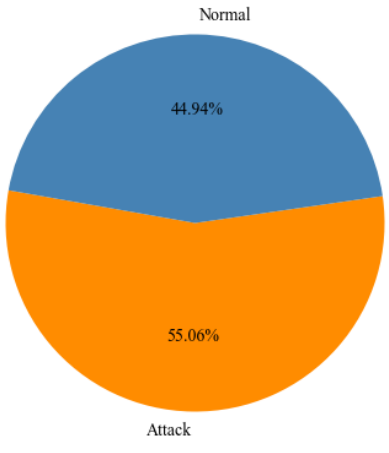
TABLE II: UNSW-NB15 dataset contains the nine different sub-types of attacks and their corresponding description [18].

| Attack types | Description |
|---|---|
| Worms | They are self-replicating malicious software programs that can spread across computer networks and systems without any user intervention. |
| Shellcode | It is designed to be injected into a target system to run specific commands and scripts, providing unauthorized access to the system. |
| Reconnaissance | The preliminary phase of an attack where an attacker gathers information about an entry point of vulnerable target system or network and this information is used for preparation of future attack. |
| Generic | A variety of different attack types that do not fit into the other. categories. |
| Exploits | The pieces of code that take advantage of vulnerabilities or weaknesses in system to gain unauthorized access. |
| DoS | It attacks disrupt the normal function of a system or network and makes the service unavailable to legitimate users. |
| Fuzzers | Launch attacks by sending random data to a system, assessing its resilience, and identifying vulnerabilities. |
| Analysis | Attack involves system analysis to identify weaknesses and potential targets for exploitation. |
| Backdoors | An unauthorized or hidden access point is created within a system or software, allowing attackers to gain access even after security measures have been implemented. |

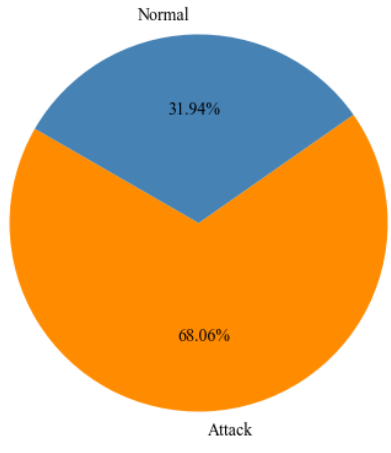
## IV. Experimental Results and Discussions

The assessment of our proposed system's performance involves a comprehensive analysis utilizing various metrics, such as accuracies, precision, recall, F1-score, and the receiver operating characteristic (ROC) curve. To ensure the resilience and consistency of the anomaly-based intrusion detection system, we conducted a thorough evaluation using RF and DNN classifiers. The outcomes of these classifiers were meticulously recorded and calculated based on specific formulas using four different terms: True Positive (TP), which represents instances when the system correctly detects anomalies in the dataset; True Negative (TN), denoting cases where the system correctly identifies the absence of anomalies; False Positive (FP), indicating instances where the system wrongly detects anomalies in the absence of risk in the dataset; and False Negative (FN), representing cases where the system fails to detect anomalies when the risk is present in the dataset. High precision and recall values signify the proposed model's accuracy in predictions while minimizing the omission of true positive instances, showcasing its ability to generalize effectively to unseen instances

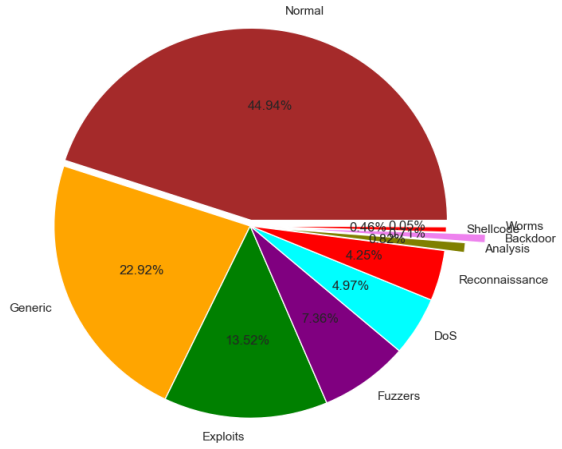
ISBN 979-11-88428-12-0



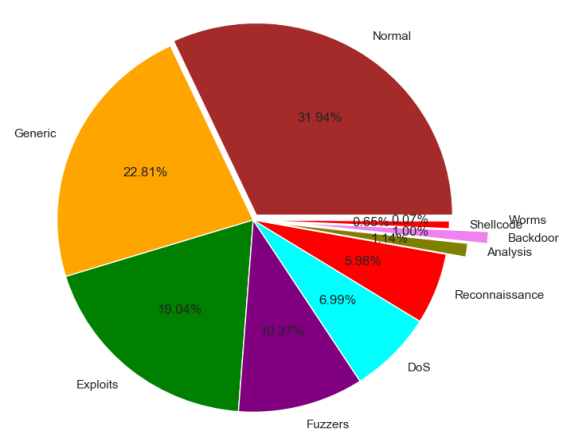

(a) The distribution of training set attack and normal class samples of UNSW-NB15 dataset




(b) The distribution of testing set attack and normal class samples of UNSW-NB15 dataset




(c) Normal and nine attack sub-categories samples distribution of UNSW-NB15 training set in pie chart




(d) Normal and nine attack sub-categories samples distribution of UNSW-NB15 testing set in pie chart

Fig. 2: Distribution of UNSW-NB15 dataset samples to their corresponding classes and sub-classes.

of the minority class. F1-score, considering both FP and FN, proves valuable for assessing the overall performance of the model on an imbalanced dataset like UNSW-NB15. Additionally, we visualize the ROC to gauge the model's ability to distinguish between positive and negative instances across varying probability thresholds. A high area under the curve signifies the model's effective discrimination between classes, a crucial aspect in evaluating its performance across different decision thresholds.

1) Accuracy: it estimates the ratio of risk recognized of the entire conditions (cases). If accuracy is higher, the machine learning model is better.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{1}$$

$$Precision = \frac{TP}{TP + FP}, \tag{2}$$

$$Recall = \frac{TP}{TP + FN}, \tag{3}$$

$$F1 - score = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}, \tag{4}$$

The confusion matrix for the UNSW-NB15 dataset, employing a RF classifier, reveals the model's effectiveness in distinguishing between Normal and Attack categories shown in Table III. With a high true positive count of 54,733 for Normal instances, the model excels in correctly identifying genuine Normal instances. However, a false negative count of 1,267 indicates instances where the model misclassifies actual Normals as Attacks. On the Attack side, the model correctly identifies 103,424 instances but erroneously classifies 15,917 instances as Normal. The overall accuracy stands at 90.20%, signifying the proportion of correct classifications. The F1-score, a harmonized measure of precision and recall, is robust at 90.45%. The precision of 91.98% underscores the accuracy of Normal predictions among instances classified as positive, while the recall of 90.20% indicates the model's capability to capture most actual Normal instances. This suggests that the RF classifier exhibits strong performance in classifying instances within the UNSW-NB15 dataset, achieving a balanced and accurate prediction of Normal and Attack categories.

TABLE III: Confusion matrix of UNSW-NB15 dataset of Normal and Attack categories by using RF classifier.

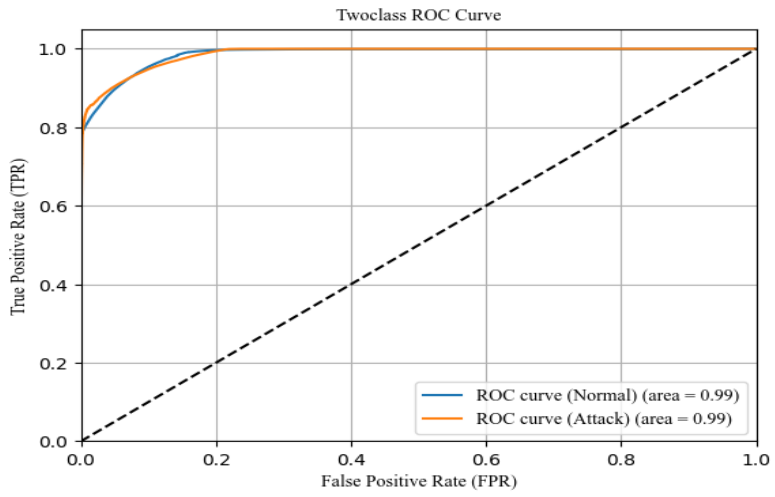
| | Normal | Attack |
|---|---|---|
| Normal | **54,733** | 1,267 |
| Attack | 15,917 | **103,424** |

TABLE IV: Confusion matrix of UNSW-NB15 dataset of Normal and Attack categories by using DNN classifier

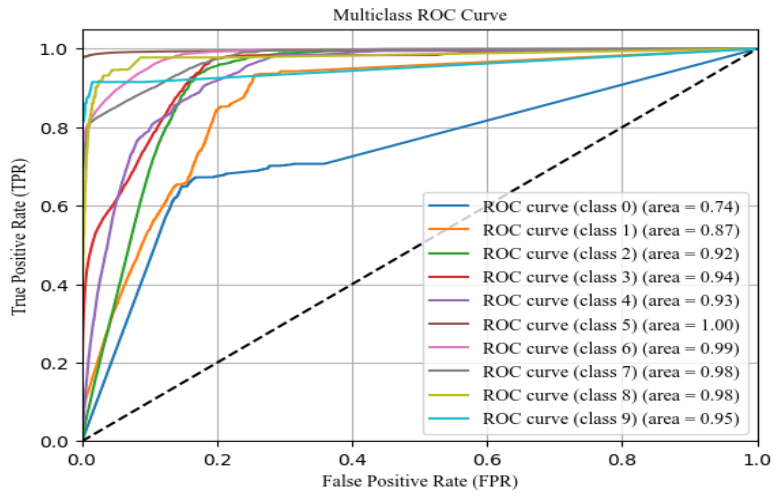
| | Normal | Attack |
|---|---|---|
| Normal | **54,878** | 1,122 |
| Attack | 19,305 | **100,036** |

The confusion matrix for the UNSW-NB15 dataset, employing a DNN algorithm, provides insights into the model's performance in distinguishing between Normal and Attack categories shown in Table IV. In the Normal class, the model achieves a high true positive count of 54,878 instances, indicating its ability to accurately identify genuine Normal instances. However, a false negative count of 1,122 suggests instances where the model misclassifies actual Normals as Attacks. On the Attack side, the model correctly identifies 100,036 instances but misclassifies 19,305 instances as Normal. The overall accuracy stands at 88.35%, representing the proportion of correct classifications.

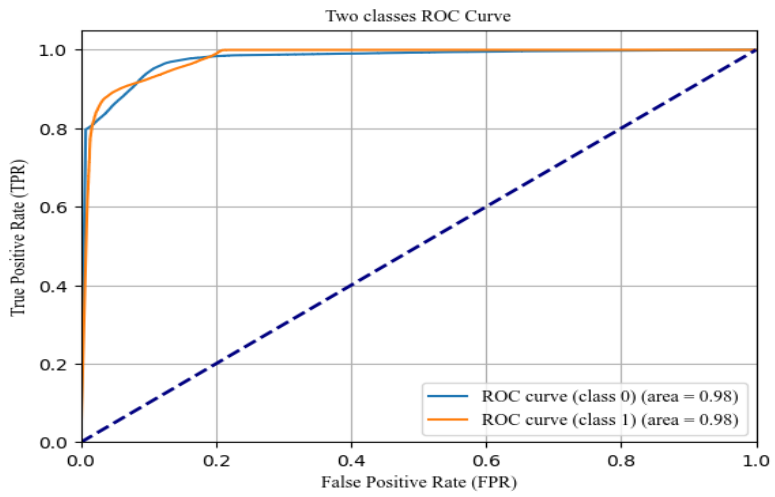
ISBN 979-11-88428-12-0



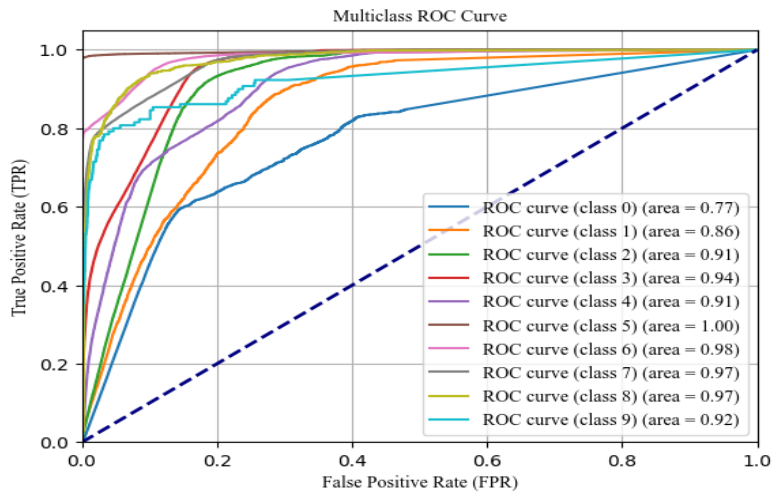

(a) ROC curve of two classes (attack and normal) of UNSW-NB15 dataset using RF classifier.




(b) ROC curve of normal and nine different sub-categories (of attack) of UNSW-NB15 dataset using RF classifier.




(c) ROC curve of two classes (attack and normal) of UNSW-NB15 dataset using DNN classifier.




(d) ROC curve of normal and nine different sub-categories (of attack) of UNSW-NB15 dataset using DNN classifier.

Fig. 3: ROC curve of two classes (Normal and Attack), and nine different attack sub-categories of UNSW-NB15 dataset using RF and DNN.

TABLE V: Confusion matrix of UNSW-NB15 dataset of normal and all sub-categories of attack by using RF classifier.

| | Analysis | Backdoor | DoS | Exploits | Fuzzers | Generic | Normal | Reconnaissance | Shellcode | Worms |
|---|---|---|---|---|---|---|---|---|---|---|
| Analysis | **43** | 103 | 1124 | 17 | 1 | 105 | 601 | 1 | 5 | 0 |
| Backdoor | 37 | **226** | 1,144 | 105 | 17 | 74 | 114 | 13 | 14 | 2 |
| DoS | 295 | 761 | **7,974** | 1,368 | 92 | 734 | 864 | 50 | 123 | 3 |
| Exploits | 381 | 911 | 10,067 | **18,143** | 262 | 1,089 | 1,850 | 505 | 154 | 31 |
| Fuzzers | 43 | 105 | 1140 | 272 | **2,578** | 128 | 13,832 | 11 | 73 | 2 |
| Generic | 4 | 8 | 262 | 288 | 23 | **39,318** | 84 | 4 | 8 | 1 |
| Normal | 0 | 1 | 18 | 398 | 605 | 4 | **54,912** | 47 | 15 | 0 |
| Reconnaissance | 47 | 163 | 1,340 | 802 | 24 | 130 | 226 | **7,744** | 14 | 1 |
| Shellcode | 0 | 0 | 34 | 127 | 25 | 14 | 262 | 21 | **649** | 1 |
| Worms | 0 | 0 | 2 | 51 | 1 | 2 | 5 | 2 | 0 | **67** |

TABLE VI: Confusion matrix of UNSW-NB15 dataset of normal and sub-categories of attack by using DNN classifier.

| | Analysis | Backdoor | DoS | Exploits | Fuzzers | Generic | Normal | Reconnaissance | Shellcode | Worms |
|---|---|---|---|---|---|---|---|---|---|---|
| Analysis | **46** | 48 | 1,275 | 56 | 1 | 0 | 521 | 11 | 42 | 0 |
| Backdoor | 37 | **80** | 1,326 | 77 | 31 | 2 | 60 | 73 | 51 | 9 |
| DoS | 313 | 356 | **9,131** | 1,095 | 94 | 20 | 578 | 229 | 432 | 16 |
| Exploits | 416 | 499 | 12,708 | **14,964** | 514 | 137 | 1,858 | 1,426 | 692 | 179 |
| Fuzzers | 57 | 54 | 1,458 | 232 | **5,068** | 194 | 10,429 | 361 | 317 | 14 |
| Generic | 15 | 11 | 357 | 275 | 41 | **39,165** | 73 | 29 | 25 | 9 |
| Normal | 8 | 2 | 181 | 311 | 1,961 | 20 | **53,247** | 181 | 84 | 5 |
| Reconnaissance | 49 | 63 | 1,573 | 299 | 44 | 1 | 425 | **7,959** | 78 | 10 |
| Shellcode | 1 | 0 | 17 | 56 | 34 | 2 | 157 | 155 | **708** | 3 |
| Worms | 0 | 0 | 7 | 52 | 3 | 2 | 7 | 4 | 5 | **50** |

The F1-score, a balanced measure of precision and recall, is robust at 88.63%. The precision of 90.93% emphasizes the accuracy of Normal predictions among instances classified as positive, while the recall of 88.35% indicates the model's capability to capture most actual Normal instances. This suggests that the DNN algorithm exhibits strong performance in classifying instances within the UNSW-NB15 dataset, achieving a balanced and accurate prediction of Normal and Attack categories.

The evaluation of multiclass intrusion detection performance, as indicated by the confusion matrix for the UNSW-NB15 dataset using the RF classifier, provides valuable insights into the classification accuracy of various classes shown in Table V. Notably, the classes Analysis, Backdoor, and Exploits exhibit a high degree of overlap with the DoS class, implying shared characteristics among these categories. Additionally, these classes show misclassifications with the Normal class, indicating similarities in their features. The Fuzzers class, in

ISBN 979-11-88428-12-0

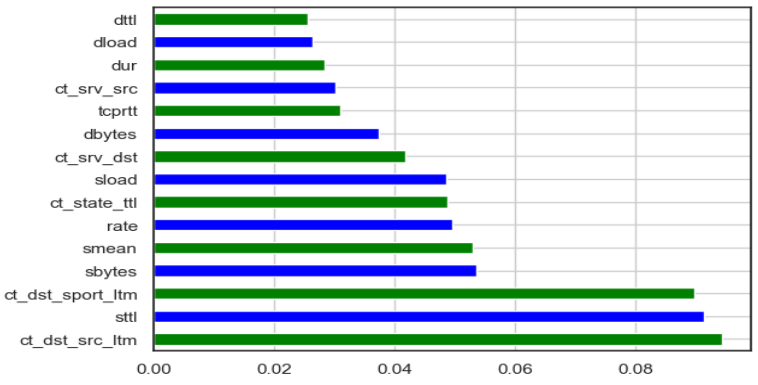



Fig. 4: It shows the feature ranking and their corresponding importance using RF of UNSW-NB15 dataset.

particular, demonstrates a pronounced overlap with the Normal class compared to other classes in the dataset. While the Worms class has relatively few samples, it shows an overlap with the Exploits class. On the contrary, the remaining classes are accurately classified by the RF classifier. The overall classification accuracy metrics are as follows: accuracy (75.17%), F1 score (72.93%), precision (77.45%), and recall (75.17%). These metrics collectively reflect the model's ability to correctly classify instances across different classes, with a notable focus on its accuracy and precision in handling the unique characteristics of each class. Almost the similar result obtained from DNN classifier and results shown in VI.

The Table VII presents a comparative analysis of the performance measures between RF and DNN classifiers, assessing their effectiveness in both two-class and multiclass scenarios. In the two-class classification, RF outperforms DNN across various metrics. RF achieves a higher accuracy (90.20%) compared to DNN (88.35%), and a superior F1-score (90.45%) compared to DNN (88.63%). The precision of RF (91.98%) also exceeds that of DNN (90.93%). Moving to the multiclass setting, RF maintains its dominance, exhibiting a higher accuracy (75.17%), F1-score (72.93%), and precision (77.44%) compared to DNN (74.33%, 73.07%, and 77.86%, respectively). These results emphasize the robust performance of RF in both two-class and multiclass classification scenarios, highlighting its efficacy in accurately classifying instances across various metrics. Our overall results are also highly competitive with the baseline model [3] which originally collected the UNSW-NB15 dataset.

TABLE VII: Different performance measures of RF and DNN classifiers in %.

| Classifier | Accuracy | F1-score | Precision | Recall |
|---|---|---|---|---|
| RF (Two-class) | 90.20 | 90.45 | 91.98 | 90.20 |
| DNN (Two-class) | 88.35 | 88.63 | 90.93 | 88.35 |
| RF (Multiclass) | 75.17 | 72.93 | 77.44 | 75.17 |
| DNN (Multiclass) | 74.33 | 73.07 | 77.86 | 74.33 |

ROC curve is a graphical representation of a classifier's performance across various threshold settings shown in Figure 3. It illustrates the trade-off between true positive rate (TPR) and false positive rate (FPR) at different classification thresholds. Area under the ROC curve measures the model's ability to distinguish between classes shown in Figure 3a. An area of 0.99 for both the "Normal" and "Attack" classes indicates very high performance in terms of classification. An AUC of 0.99 suggests that the RF classifier has an excellent ability to separate between the "Normal" and "Attack" classes, showcasing strong performance in terms of true positive rate and false positive rate. Higher AUC values generally indicate better model performance. Similarly, we presented the area under the ROC curve of multiclass (Normal and 9 different sub-categories attack) RF classifier in Figure 3b. We also plotted the area under ROC curve for both two class and multiclass DNN classifier, and shown in Figure 3c and Figure 3d.

## V. Conclusions

We introduced an ADS utilizing RF and DNN classifiers to identify diverse anomaly and normal patterns. Both classifiers effectively distinguish various intruder patterns, and we explored crucial attack features for precise anomaly detection in complex, high-dimensional datasets. To address this challenge, we introduced a feature selection technique to identify pertinent features and minimize computational complexity. With multiple subcategories of attacks, each with distinct characteristics, RF demonstrated the ability for complex pattern recognition. Additionally, DNN was implemented to further enhance detection capabilities, collectively addressing multifaceted challenges in anomaly detection. The highly imbalanced UNSW-NB15 dataset prompted us to implement oversampling, carefully designing RF and DNN to prevent overfitting. We evaluated performance using diverse metrics, including classification accuracy, class label accuracy using the confusion matrix, precision, recall, F1-score, and ROC curve. The consistent and convincing results obtained from both classifiers underscore the effectiveness and reliability of the proposed method.

Our immediate plan involves implementing time-based features for intrusion detection to precisely detect evolving intrusion patterns over time, enhancing host or network computer security.

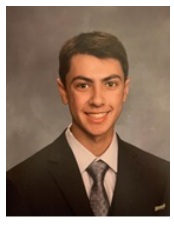
## Acknowledgment

This material is based on work supported by the National Science Foundation under Grant Number HBCU-EiR-2101181. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation (NSF).

## References

[1] Source link: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[2] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, "Robust Intelligent Malware Detection Using Deep Learning," in IEEE Access, vol. 7, pp. 46717-46738, 2019.
[3] N. Moustafa, J. Slay, and G. Creech, "Novel Geometric Area Analysis Technique for Anomaly Detection Using Trapezoidal Area Estimation on Large-Scale Networks," in IEEE Transactions on Big Data, vol. 5, no. 4, pp. 481-494, 1 Dec. 2019.
[4] R. Heady, G. F. Luger, A. Maccabe, and M. Servilla, "The Architecture of a Network Level Intrusion Detection System," Albuquerque, NM, USA: Dept. Comput. Sci., College Eng., Univ. New Mexico, 1990.
[5] N. Moustafa, and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in Proc. Military Commun. Inf. Syst. Conf., pp. 1–6, 2015.
[6] T. Giannetsos and T. Dimitriou, "Spy-sense: Spyware tool for executing stealthy exploits against sensor networks," in Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Secur. Privacy, pp. 7–12, 2013.
[7] Y. Ye, Tao Li, D. Adjeroh, and S. S. Iyengar, "A Survey on Malware Detection Using Data Mining Techniques," ACM Comput. Surv. 50, 3, Article 41, May 2018.
[8] M. Ligh, S. Adair, B. Hartstein, and M. Richard, "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code," Wiley Publishing, 2010.
[9] M. Sikorski, and A. Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software," Computers and Security, v6, pp. 802-803, 2012.
[10] W. Lee, S. J. Stolfo, and K. W. Mok, "A data mining framework for building intrusion detection models," in Proc. IEEE Symp. Secur. Privacy, pp. 120–132, 1999.
[11] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maci-a-Fern-andez, and E. V-azquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Comput. Secur., vol. 28, no. 1, pp. 18–28, 2009.
[12] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 447–456, Feb. 2014.
[13] G. Creech and J. Hu, "A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns," IEEE Trans. Comput., vol. 63, no. 4, pp. 807–819, Apr. 2014.
[14] W. Hu, J. Gao, Y. Wang, O. Wu, and S. Maybank, "Online adaboost-based parameterized methods for dynamic distributed network intrusion detection," IEEE Trans. Cybern., vol. 44, no. 1, pp. 66–82, Jan. 2014.
[15] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, "RePIDS: A multi tier real-time payload-based intrusion detection system," Comput. Netw., vol. 57, no. 3, pp. 811–824, 2013.
[16] M. Almseidin and S. Kovacs, "Intrusion detection mechanism using fuzzy rule interpolation," arXiv preprint arXiv:1904.08790, 2019.
[17] B. K. Baniya, "Intrusion Representation and Classification using Learning Algorithm," 2022 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon-Do, Korea, Republic of, pp. 279-284, 2022.
[18] N. Moustafa, "Designing an online and reliable statistical anomaly detection framework for dealing with large high-speed network traffic," Diss. University of New South Wales, Canberra, Australia, 2017.
[19] B. K. Baniya and E. Z. Gnimpieba, "The Effectiveness of Distinctive Information for Cancer Cell Analysis Through Big Data," In: Arai, K., Kapoor, S. (eds) Advances in Computer Vision. CVC 2019. Advances in Intelligent Systems and Computing, vol 944. Springer, Cham.
[20] B. K. Baniya and J. Lee, "Importance of audio feature reduction in automatic music genre classification," Multimed Tools Appl 75, 3013–3026 (2016). https://doi.org/10.1007/s11042-014-2418-z

**Babu Kaji Baniya** holds a B.E. degree in Computer Engineering from Pokhara University, Nepal, which he obtained in 2005. He further pursued his education and completed an M.E. and Ph.D. in Department of Computer Science and Engineering from Chonbuk National University, Republic of Korea in 2015. Following his doctoral studies, he gained valuable experience as a postdoctoral researcher in the Department of Computer Science and Biomedical Engineering at the University of South Dakota. He then served as an assistant professor in the Department of Computer Science and Digital Technologies at Grambling State University, Louisiana. Currently, he holds the position of assistant professor in the Department of Computer Science and Information Systems at Bradley University, located in Peoria, Illinois. Throughout his career, he has taught a wide range of Computer Science courses at both the graduate and undergraduate levels. His research interests span several key areas, including audio signal processing, information retrieval, cybersecurity, bioinformatics, Big Data, and machine learning. A specific focus of his research involves the application of machine learning and deep learning algorithms in securing the Internet of Medical Things (IoMT). He is also IEEE member.



**Thomas Rush** is currently pursuing a B.S. degree in Computer Science with a concentration in Data Science at Bradley University in Peoria, Illinois. His research experience includes working as a Research Assistant to Dr. Baniya at Bradley University, where he focused on classifying Android malware using a variety of machine learning models and deep learning techniques. Thomas has applied these skills in practical settings, having completed coursework in Data Science, Machine Learning, Data Mining, and Artificial Intelligence at Bradley University. Additionally, he contributed to data analytics for the Bradley University Men's Soccer Team through his senior capstone project.

ISBN 979-11-88428-12-0