**An Efficient Machine Learning based Multiclass Cyber Attacks Classification and Prediction**

Tahz Ullah[[1]](#footnote-1), Ghassan Husnain[[2]](#footnote-2), Waqas Ahmad[[3]](#footnote-3), Gulbadan Sikander[[4]](#footnote-4), Muniba Ashfaq[[5]](#footnote-5)

***Abstract***

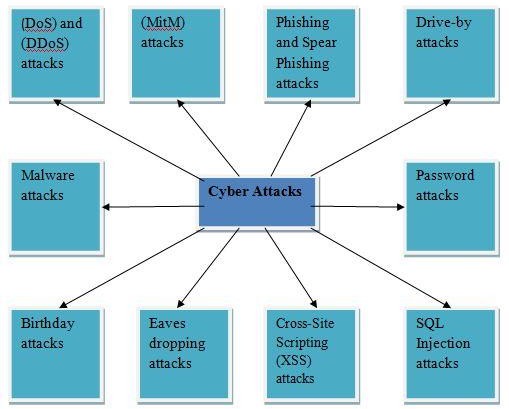
*Security breach involves an attempt to attack a machine for data theft and compromising network resources to retrieve unauthorized information, network infrastructure, etc. The purpose of network attacks is to obtain information gathering, destroy network infrastructure and compromise data, etc. Cyberattack wields the deliberate contrivance of malicious code within the system’s logic and information to elicit unauthorized information through such hoodwinks resulting in cybercrime and fraud. This paper proposes a suitable classifier for cyberattack prediction based on an enhanced machine-learning technique. The study aims to identify and predict various techniques of cyberattacks such as Random Forest and XGBoost and other classifications for detection of attacks w.r.t. information available to the public. According to the findings, Random Forest recall (RE) accuracy is 69% and precision (PR) is 69% for the initial classification that is Random Forrest. The F1 score of 69% is represented by the average accuracy. According to the report, the XGBoost model performed with precision (PR) of 75% and recall (RE) of 75% accuracy while using the second classification approach. Our model's average accuracy (AC) is 75%. Both models namely Random Forest and XGBoost show superiority over well-established methods for the classification and prediction of cyber-attacks.*

***Keywords***: Cyber-attacks, XGBoost Classifier, Random Forest Classifier, Machine Learning, Confusion Matrix.

**Introduction**

An attack is executed from one computer to another computer to target networks or websites. The motivation behind the attack is to gather information and introduce trespassers harming the network infrastructure endeavoring into the definition of cybercrime. A cyber-attack is an information system in which a person or organization maliciously and intentionally attempts to destroy another person or organization. One of the persuasions of such an attack is the possible chance of raffling benefits by destroying the target network infrastructure or intimidating threats. It is the use of some nonsense method to change coding systems, logic, or information, which leads to bad results that can get illegal information, and then it became a cybercrime, such as information fraud [Javed,2019].

*Types of Cyber Attacks*

Cyber-attack conundrum comprises targeting unauthorized computers, networks, or websites with certain offensive motivations, such as information gathering to rummage through the routine working of network infrastructure and data information systems by using a variety of methods [Ju, Ankang,2019]. The following figure 1 shows the most common cyberattacks.

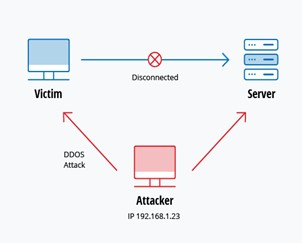
**Fig. 1: Types of Cyber Attacks [2]**

DoS and DDoS Attacks

Denial of service (DoS) and Distributed Denial of Service (DDoS) attacks the assets of the system and therefore cannot respond to check requests. Distributed denial of service (DDoS) attacks as well as a hit system resource. A denial-of-service attack (DoS) does not present a direct benefit to the attacker. For some of them, it is enough to satisfy the service rejection. Nonetheless, if the attacked resources are commercial competitors, the revenue of the attacker is practically well sufficient. Denial of service assaults are now commonly used to launch other forms of attacks by temporarily putting the system offline. There are unusual types of DoS and DDoS attacks [Fang,2019].

Man-in-the-Middle (MitM) Attacks

When hackers place themselves between the user and the server, a Man-in-the-Middle (MitM) attack occurs. Here are a few regular Man-in-the-Middle attack types. In this kind of attack, a session between a trustworthy user and a web server is hijacked by the attacker. The attack system replaces its scientific subject deal with a determined client at the same time as the server continues the setting and the basic intellectual process communicates with the client as in own Fig. 2.



**Fig. 2: Man-in-the-Middle (MitM) Attacks [3]**

Phishing Attacks

A phishing attack is a socially engineered attack to transfer an email to appear to come from a trusted source, to obtain personal information, or to influence the user to perform certain actions such as getting hold of other credentials or other secure information such as credit card numbers, etc. It may engage an associate degree attached to an associate degree email, which spreads malware to your account. It may even be a link to an illegal website associated with a degree that will trick you interested in downloading malware or providing your data. Spear phishing is an under-attack phishing campaign. Attackers need to spend a lot of time on spear phishing. Therefore, spear-phishing may be difficult to recognize and even more difficult to protect. One of the best ways for hackers to engage in spear-phishing attacks is email spoofing [Wang, Zhongqing, 2017].

Drive-by Attacks

Pass-through transmission attacks are standard techniques for distributing malware. Hackers seem for insecure websites and embed nasty scripts into Hypertext Transfer Protocol (HTTP.) or Hypertext Processor (PHP) code on a single page. This script may set up malware openly on a personal computer that accesses the location or redirect the victim to a hacker-controlled website.

Password Attack

A password attack is the majority common method for authenticating users of the information system. Obtaining passwords is a regular and useful attack way. This is the most common attack used for social media accounts like Facebook, Gmail, Twitter, etc. where people publicly communicate and share their information [Kim, Youngsoo,2014].

SQL injection Attack

Structured query language (SQL) injection is suitable for general problems of database-driven websites. This happens when criminals execute (SQL) queries against the database by entering data from the user to the server. Insert structured query language (SQL) commands into the data plane input (for example, instead of a login name or password) to run predefined structured query language (SQL) commands. A successful structure query language (SQL) injection attack can understand sensitive data from the database, convert, insert, update or delete database data, perform operational operations such as closing the database, repairing the content of known files, and in several cases, Issue commands to the operating system [Sarkar,2019].

Eaves-Dropping Attack

An eavesdropping attack occurs by intercepting system traffic. Eavesdropping, is an attacker attacking account information with important mailing and other secret information that users may send over on the network system. Following are types of Eaves-Dropping attacks.

* + - * Passive eavesdropping

A hacker distinguishes the information by change into the communication transmission in the network.

* + - * Active eavesdropping

A hacker effectively gets the data by camouflaging himself as a friendly unit and by sending queries to transmitters [Saeed, Nasir, Waqas Ahmad,2018].

Birthday Attack

A birthday attack is a possibility of discovering two arbitrary messages that produce the same mark (MD) when the process by a mix-up function. If the attacker calculates a similar Markle- Damaged (MD) for the user's message, they can safely restore the user's messages by his messages, even if he compares the tag- curse (MD), the receiver cannot detect the replacement [Albladi,2018].

Malware Attack

Malware can define as unnecessary software that is installed on your system without your authorization. It can join itself to the rightful code and spread it. It is capable of lurking in helpful applications or copying over the Internet [Husnain, Ghassan,2023].

*Research Gap*

Some recent research on cyber security prediction and classification are as follows:

George Onoh [Onoh, George,2018] investigates two questions. The first one is working on cyber-attacks and their detection in publicly available data or information. Second is how the existing data could be utilized for predicting cyber-attack. Researchers stored daily data of brute force and password-guessing attacks. Using a Naive Bayesian classifier for classification and obtained 63% accuracy of prediction. The total number of instances used in this research work is 30 and classified only 19. In this research work, we will be using existing data of cyber-attacks to generate new data based on existing data. That can provide help in future decision-making. It is important to propose and perform an enhanced method for the prediction of cyber-attacks and proposed a more powerful classifier. The following are the main contributions of this study.

* To propose an efficient and enhanced method for the classification and prediction of cyber-attack.
* To learn how to predict which attacks will happen, a machine-learning algorithm will need to be supervised.
* To compare the proposed method with well-established methods for the prediction of cyber-attacks.

**Literature Review**

Amir Javed *et al.* [Javed,2019] build a sufficient algorithm that abuses machine movement information and Twitter information in order toward forwarding post-execution categorization of such Uniform Resource Locator (URL) to malicious to predict that the computer address will be in interaction with the computer address 0.99 F1 scores (using 10 x cross-validations) and 0.83 (using an invisible check set) were maliciously obtained within 1 second. Therefore, provide a base to kill the relationship with the server previous to the attack is finished, pro-actively prevent, and prevent attacks.

Ankang-Ju *et al.* [Ju, Ankang,2019] reviewed a completely different knowledge fusion mechanism, namely the association of heterogeneous multi-source knowledge. On this basis, we tend to suggest a large knowledge analysis framework for targeted cyberattack detection and provide a basic plan for correlation analysis. They are provided with the capability to compare multi-source security knowledge and effectively evaluate attack intent. Xing Fang, Maochao Xu *et al.* [Fang,2019] developed a deep learning framework using a two-way perennial neural network with long memory called BRNN- LSTM. Experimental studies show that BRNN-LSTM achieves a high percentage of prediction accuracy than applied mathematical methods.

Zhongqing Wangyz *et al.* [Wang, Zhongqing, 2017] planned a fine-grained ranked stream model to capture linguistics data over an infinitely long history and reveal burstiness and trends. Empirical analysis shows that social text streams area unit so informative for DDoS prediction, and our planned ranked model is simpler compared to robust baseline text stream models and distinct bag-of-words models. Youngsoo Kim *et al.* [Kim, Youngsoo,2014] proposed several examples and options of modern cyberattacks and express phases of them. Finally, we tend to conclude that solely the conception of counterintelligence will defend these cyber threats.

Soumajyoti Sarkar *et al.* [Sarkar,2019] used data from the Dark Web Forum to predict corporate cyber-attacks by investing in user interaction reply network structures. We tend to use a set of social networking options to validate their binary classification flaws in the use of supervised learning models, which attempt to predict whether a company will attack any particular date. We tend to conclude from our experiments that victim data from 53 forums in the Darknet predicts two completely different security incidents of cosmic tissue attacks over 12 months, analyzing clues between user teams. The structure is best to simply learn the network center like page rank or expect users to post statistics in the forum.

In [Saeed, Nasir, Waqas Ahmad,2018], an automatic active attack jamming technique was introduced that uses practical analysis techniques used inside monetary engineering to recognize secret code. At similar times, deep learning was used to study evidence of cyber-attacks. The results of Samar Mu-slash Al-blade *et al.* [Albladi,2018] show that individuals reply to cyber-attacks that otherwise support their demographics. Also, people's abilities, networking expertise, and their limited links to a stranger in community networks will reduce their chances of becoming victims of certain attacks. In [Husnain, Ghassan,2023] describe the use of social media as a crowdsourced sensing element to increase insight addicted to current cyber-attacks. The approach detects various network attacks and requires only a small number of seed event triggers among victims of pollution monitoring. A sample that is guided or marked. A new problem growth strategy that supports convolution kernel and dependence resolution helps model the language configuration and helps distinguish key event personality. Throughout the comprehensive analysis of tweets, we tend to prove with the aim of our method systematically identifies and encodes actions, which is superior to existing methods.

George Onohet [Onoh, George,2018] investigates about two questions. The first one is how are outside organizations able to identify cyber-attack incidents using only publicly accessible information. The second is how to be capable of using this information for predicting cyber-attacks. He stored daily data of brute force and password-guessing attacks. Using the Naive Bayesian classifier for classification 63% accuracy and achieved 71% average accuracy of prediction. The total number of instances used in this research work is 30 and classified only 19. This proposed work is to guess future cyber-attacks on the available data.

In [Husnain, Ghassan,2022], a preliminary investigation of the Enron email dataset is conducted and the efficiency of obtainable SNA indicators is investigated in building a ladder in social networks produced from email communication information. Then, they tend to test the metrics on contemporary datasets to charge the efficiency of our outcome results on alternative networks. In [Ahmad, Waqas,2020], proposed that AI is getting utilized in digital security in every guard and offence exercise, along with conversations on digital assaults focused on AI models. In particular, they tend to talk about the uses of AI in finishing digital assaults, as in great botnets, progressed skewer fishing, and hesitant malware. they tend to also legitimize the apparatus of AI in digital security, such as in danger identification and deterrent, malware recognition and grouping, and system chance checking.

Aldo Hern Mendez Suarez1 *et al.* [Husák,2018] proposed ways to track social information that would activate cyber-attacks. The major involvement in the journal forecast of the tweet, whose content is related to security attacks, and the detected events support the first normalization. Martin Husa'k *et al.* [Almukaynizi,2017] proposed two methods to support separate models, like an attack map, Bayesian network, and Mark off model, and constant models, such as Statistics and grey models were investigated and compared. They tend to talk about machine learning and information processing methods further, which have recently received a group of interest and seem to be capable of this permanent dynamic environment, namely network safety. The investigation also focused on the rational use of the method and issues associated with its analysis.

Mohammed Almukaynizi1 *et al.* [Chambers,2018] proposed a technique that combines social network analysis with machine learning techniques to predict liability utilization. The technology utilization options support user attributes in dark/deep sites, similar to options resulting from liability knowledge. Their results show the options calculated from client social relationships be a great indication of future cyber-attacks. They tend to experiment with real-world hackers and use knowledge, and to maintain accuracy by considering F1 scores on June 6, 1944, proving that social networking knowledge can improve recall rates. They tend to think that this may be due to the social network structure associated with a positive exploit author, indicating that they can write down the attacks that were later used in the associated attack.

Nathanael Chambers *et al.* [Okutan,2017] explored natural language processing methods to use social media as an associated indirect live broadcast of online checkpoints. They tend to describe the 2 learning frameworks used for this task: feedforward neural networks and partially labelled LDA models. The important limitation of each model before work is (the average ratio is 20%). They tend to show that topic-based models allow for preliminary fine-grained analysis of the public’s response to modern cyberattacks; multiple “stages” of observation are discovered. This is usually the main model for every detection of cyber-attacks (with the best performance), and the correlation provides an analysis and a way for the public to explain the service interruption. They tend to describe the model, the present experiment of the largest tweet DDoS corpus to date, and the conclusions related to the public response analysis that supports the output of the learning model.

Ahmet Okutan1 *et al*. [Shu, Kai,2018] Preliminary results of the initial transmission of signals from worldwide events and social media using Bayesian classifiers explain the promising predictive analysis of anonymous organizations, even if the signal is not a Corrupt organization. In [Husnain, Ghassan,2022], proposed devices that use emotions in social media as a higher level of awareness, detection, and prediction of cyber-attacks. They tend to develop an efficient unsupervised expressive prediction model that uses expressive signals. A victimization approach is a part of the logistic regression predictor. Emotional changes are associated with attack opportunities. The realistic social media knowledge experiments around the hacker's divestiture attack demonstrate the effectiveness of the planned emotional model in understanding and predicting cyber-attacks.

Amy Sliva1 *et al.* [Sun, Nan,2018] proposed a sub-degree method that uses emotional polarity as a device for the social performance of teams on social media as a pointer of cyberattack performance. They tend to develop an unsupervised emotional prediction method for associate degrees, which uses emotional signals to reinforce emotional signals from lean substance indicators. To explore the effectiveness of emotional polarity as a measure of relevance to cyber-attacks. They tend to experiment with real-world information from Twitter, which corresponds to the familiar attack of hacker-splitting clusters.

Sun *et al*. [Alqubaiti,2016] investigated the rising analysis by reviewing the dominant number of recent representative works. They tend to jointly mine and précis the information-driven analysis methods normally used in this rapidly evolving field. Consistent with the various stages of the methodology, each work to predict cyber-security incidents has been thoroughly studied. The challenges and future directions in this area are mentioned. Zahra Y. Alqubaiti *et al.* [Xu, Maochao,2018] explores the link between user security perception and their actual actions on social networking site. The Protection motivation theory (PMT), which examines appeals from the ground up, has been commonly used to observe people's actions in the area of information protection. They tend to suggest that the PMT hypothesis can furthermore be customized to clarify and predict the behavior of social media users with security risks. They tend to use web-based surveys to provide the user with a sense of protection on social networking sites and to gather knowledge about their actual behavior.

In [Husnain, Ghassan,2023], reported on applied mathematical analysis of violations of events to admire cyber hacking activities involving malware attacks for 12 years (2005-2017). They tend to show that according to the survey results in the literature, the arrival time and violation size of each hacker violation should be engraved through a random process, not the result of the exhibition autocorrelation. Then, they tend to propose a specific theoretical account model separately; the match arrival interval is therefore consistent with the size of the violation. they did additionally indicate that this model will predict the coming time and thus the size of the violation. In arrange to get a deeper understanding of the evolution of hacking events; they work to conduct each qualitative and quantitative trend analysis of the information set. they tend to extract a range of cyber-security insights, while cyber hacking threats become bad in terms of occurrence, but do not affect the level of scratch.

Zhenxin Zhan1 *et al.* [Alqahtani,2020] proposed the error handling of innovative methods for grey box prediction. The system advocate utilizes a gray box model to provide accommodation for applied mathematical characteristics/phenomena exhibited by the information. in particular, they did show that the gray box model adapted to remote dependent (LRD) development will predict the attack rate 1 hour to the lead of time (i.e., the number of attacks per component-time). The accuracy rates were 70.2 and 82.1%, respectively. For the most effective information in our information, this may be the main result of the practicality of the forecast in the area. For the prediction, they investigate the error region unit caused by the model's inability to predict a large attack rate, and the unit of the region is called the extreme value in the statistics. This prompted the United States of America to study extreme value development through the Abuse 2 supplemental approach: Acute Price Theory (EVT) and Statistical Theory TST. The proposed long-term prediction on based use EVT. While the gray box TST model predicts attack rates one hour with an accuracy of 86.0 and 87.9%. We tend to explore the connection between the two methods and indicate the direction of future analysis. This predictive research relies on special cyber-attack and their information, this approach applies to researching cyber-attack information.

Well-known machine learning classification techniques, especially Bayesian networks, naive Bayes classifiers, decision trees, random decision forests, random trees, decision-making Tables, and artificial neural networks to identify due to intrusions provide shrewd help in the field of network security. Finally, they tested the feasibility of different checks on cybersecurity data sets with several types of cyberattacks and evaluated the adequacy of performance indicators, precision, recall, f1 score, and accuracy.

**Material and Methods**

This section presents different steps for the classification and prediction of cyber-attacks which are as follows:

1. Phase I, is to analyze the existing research work through a research study about cyber-attack their most common types, and cyber-attacks future prediction analysis.
2. In phase II, we propose a simple enhanced method for classification and prediction and we can use preprocessing techniques, data wrangling, feature scaling, etc.
3. In phase III, proposing an efficient and very fast classifier for our work to obtain the best results with accuracy for classification and prediction.
4. In phase IV, evaluate and validates the outcome.

*Data Set*

KDD data set has been initially selected from UCI that contains information about cyber-attacks. Count of data set is shown in Table.1. Fig. 3. illustrates the proposed work.

***Table I***

*KDD Data Set*

|  |  |
| --- | --- |
| **Number of Rows** | **Number of Columns** |
| 22543 | 43 |

The dataset consists of different features of cyber-attacks. The proposed work is displayed in data set using Python in the Fig.4 below. This data has different columns TCP, private, REJ, and Neptune. That has all information about types of networks, media, and all attacks.

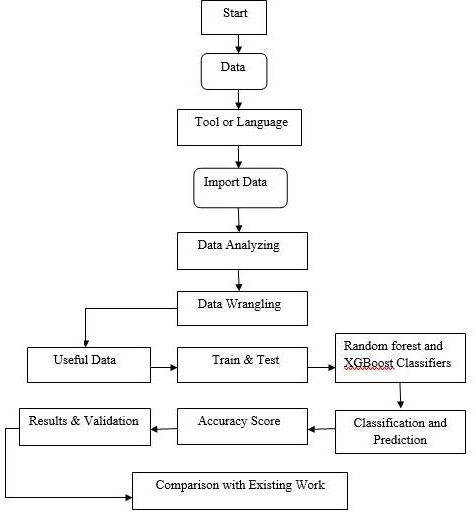
*Tool & Language*

Python language is chosen for its customizable and simple features along with less code and implicit libraries with explicit practicality. In the Jupiter notebook, Python is used which is open-source.

*Data Analyzing*

Data analysis is a very important stage used in data science and other related areas. In this first, we work to understand information and its relation to each other. Also, we create a visual form of data to give reliable insights info. So, data analysis helps us to understand the information in a great easy way. The following figure shows a graphical presentation of the network medium.

The Fig.5 shows the network medium or path which are used in attacks. There is a total number of three medium TCP, UDP, and ICMP. The TCP is 18879, UDPis 2621, and ICMP is 1043. Here maximum used is TCP. The next is data wrangling for missing values. The next is data wrangling for missing values. The next one is attacks which have been done already. (103 A/m).” Do not write “Magnetization (A/m) 1000” because the reader would not know whether the top axis label in Fig. 1 meant 16000 A/m or 0.016 A/m. Figure labels should be legible, approximately 8-to- 10-point type. Fig. 6 shows all attacks which have previously been done.

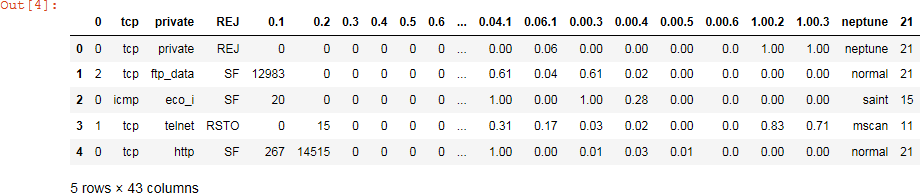


**Fig. 3: Flowchart for the developed method**

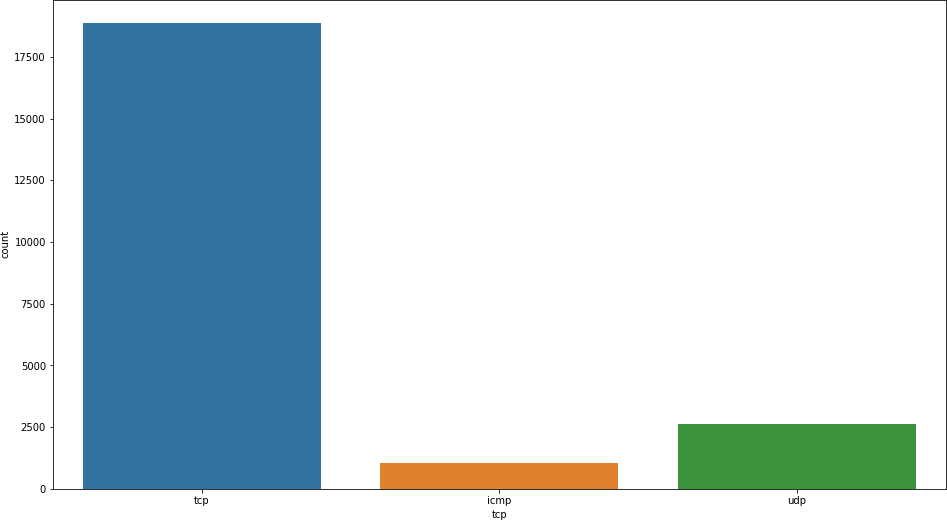
**Results**

*Random Forest Classifier*

In the initial stage of classification, which combines decision trees, a random forest method is used. A random forest classification algorithm was employed in the proposed study. A lot of selections are made using the most well-liked and effective machine learning classification technique, random forest. In this approach of classification, learning is first done from the input data and the learned data is used for classification.



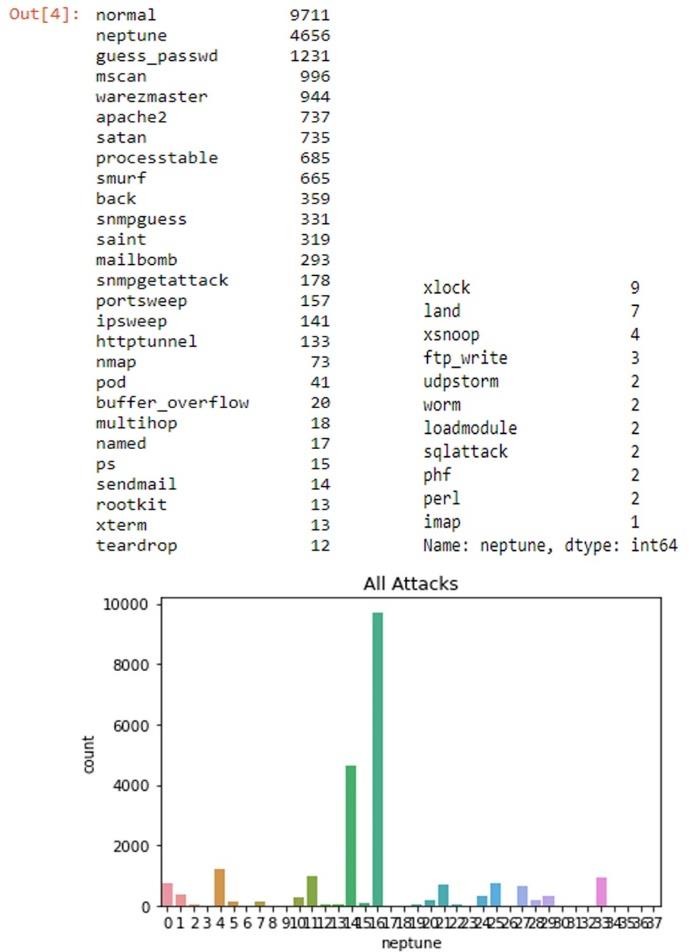
**Fig. 4: Proposed dataset**



**Fig.5: Network Medium**

First Confusion Matrix

The performance for machine learning classification is summarized using this first confusion matrix. We can better understand the effectiveness of the classification model and the types of errors it generates by calculating this technique. It is used to classify actual and predicted labels. They offer a visual representation of the classifier and its performance. The confusion matrix for our model is displayed in Fig. 7. The entire number of real labels and expected labels for categorization is represented by the confusion matrix. A combination of True-Positive, True-Negative, False-Positive, and False-Negative numbers make up these actual and anticipated labels.



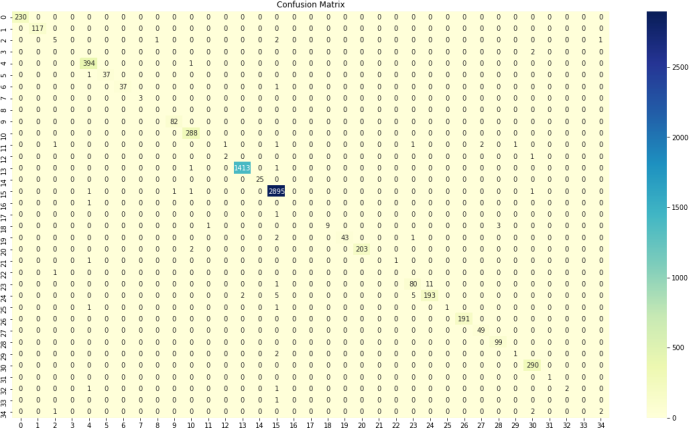
**Fig. 6: Different Cyber-attacks**

We will determine our model's categorization and prediction accuracy using these numbers.

* + - * TN stands for True-Negative: it is the total value of accurate predictions for which an instance is negative.
      * FP stands for False-Positive: it is an inaccurately predicted quantity value whose occurrence is positive.
      * False-Negative, or FN, refers to how many incorrect predictions an instance negates.
      * True-Positive, or TP, refers to a quantitative value that was correctly anticipated and whose instance was positive.

Results of Random Forest Classifier

Fig. 7 illustrates the confusion matrix of proposed ed dataset. As a result, there are a total of six labels in this confusion matrix including True positive, True negative, False positive, False negative etc. Using this confusion matrix, we computed the performance of our suggested model by the accuracy of our classification reports and prediction outcomes to gauge the outcome of proposed model.



**Fig. 7: First Confusion Matrix of Proposed dataset**

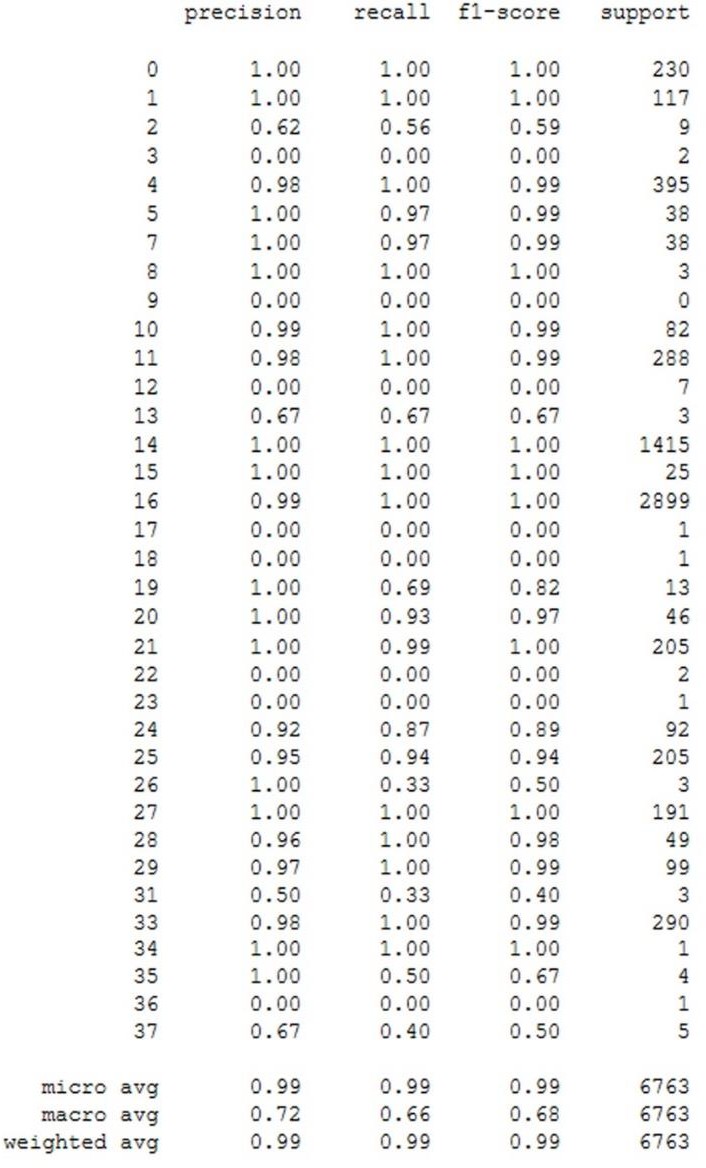
First Classification Report of Random Forest

Now we use the aforementioned confusion matrix to calculate the performance of our model. The table below lists the proposed model's accuracy-based performances. Based on the aforementioned confusion matrix, performance metrics including accuracy (AC), precision (PR), recall (RE), and F-measure (F1) are computed. The full classification is shown in Fig. 8. The confusion matrix is used to construct these reports, and the following formulas of precision, recall, and F1 score. The Precision (PR) and recall (RE) for the categorization report in Table 2 are both 69% accurate. Our model's 69% average accuracy (AC) is remarkable. Moreover, the average accuracy represents the F1 score.

# ***Table 2***

# *Performance Measure of Proposed Work*

|  |  |  |  |
| --- | --- | --- | --- |
| **Accuracy (%)** | **Precision (%)** | **Recall (%)** | **F1 Score (%)** |
| 69 | 69 | 69 | 69 |



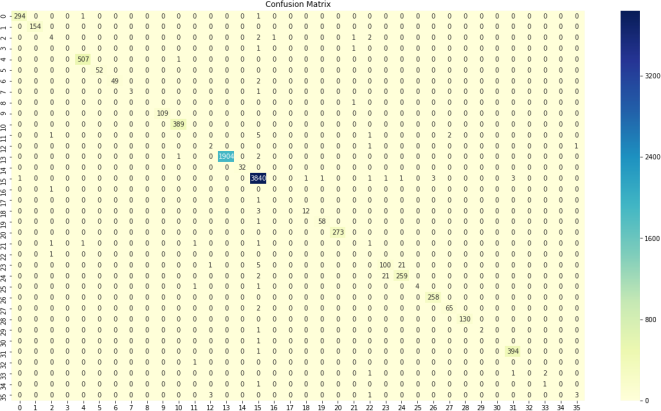
**Fig. 8: First Classification Report of Random Forest**

*XGBoost Classifier*

One of the effective machine learning models is XGBoost. Popular machine learning algorithms demands efficiency in terms of processing performance especially when working with huge data sets. Accuracy, speed, and scalability of XGBoost have developed into mature models for data science contests. It is essential to have high execution speed and precision. Although quicker than previous methods, it functions similarly to a tree or a random forest. It works well with big data sets. The confusion matrix and classification outcomes of XGBoost are as follows.

Second Confusion Matrix

The XGBoost classifier is represented by the second confusion matrix. The confusion matrix for XGBoost model performance identification is displayed in the Fig. 9 below.



**Fig. 9: Second Confusion Matrix of XGBoost**

Second Classification Result

The aforementioned confusion matrix is computed in this section using the model performance. Table 3 below lists all of our suggested work's accuracy-based performances (XG BOOST). Based on the aforementioned confusion matrix, performance metrics including accuracy (AC), precision (PR), recall (RE), and F-measure (F1) are calculated. The whole categorization is depicted in Fig. 9.

# These reports are produced from the confusion matrix using the following equations:

# 1. Precision

# 2. Recall

# 3. F1 Rating

# ***Table 3***

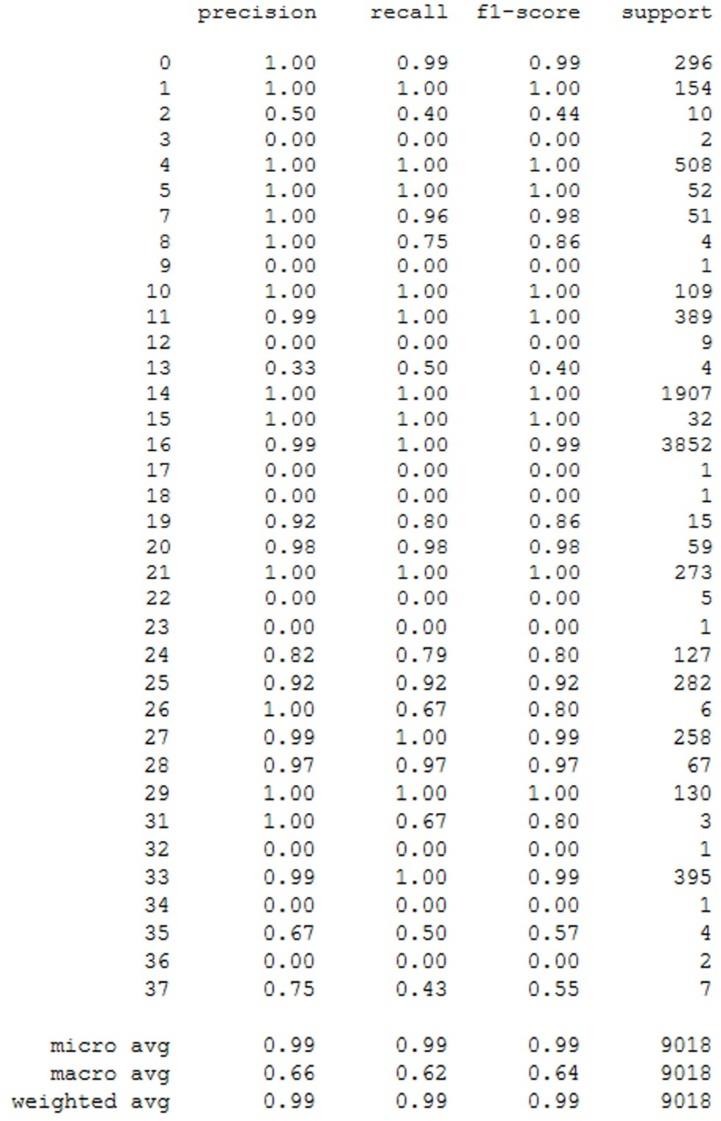
# *Performance Measure*

|  |  |  |  |
| --- | --- | --- | --- |
| **Accuracy (%)** | **Precision (%)** | **Recall (%)** | **F1 (%)** |
| 75 | 75 | 75 | 75 |

According to the findings in table 3, the accuracy of recall (RE) and precision (PR) for the categorization of cyberattacks is 75% each respectively. Our model's average accuracy (AC) is 75%, which corresponds to an F1 score of 75%.

*First Results Validation*

We utilized Sklearn library validation to identify the accuracy of our results during results validation and verification. Additionally, utilised for all test and train verification. The Scikit-learn validation package demonstrated the correctness of our suggested work in Fig. 11.



**Fig. 10: Second Classification Report of XGBoost**



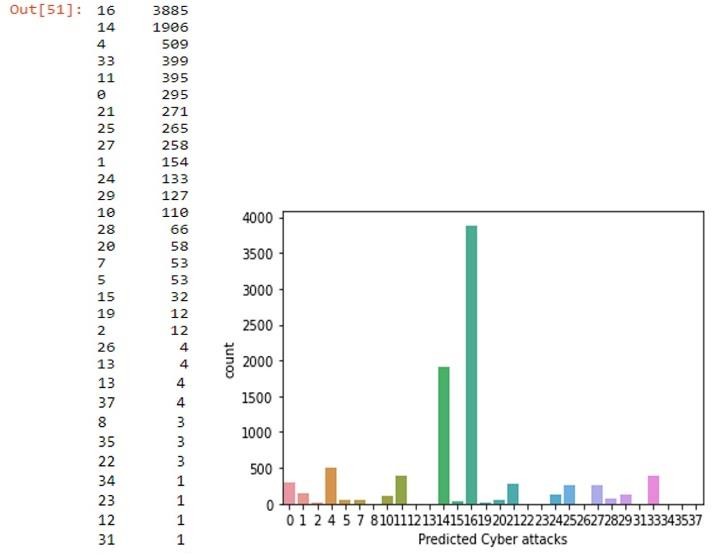
**Fig. 11: First Results Validation**

*Second Results Validation*

This work uses the Scikit-Learn library validation to identify how accurate our results were and to validate the results. All train and test verification is also done using this. The correctness of our suggested work as demonstrated by the Scikit-learn validation package is depicted in the Fig. 12. Subsequently, Fig. 13 shows new attacks which are predicted by our proposed models.



**Fig. 12: Second Results Validation**



**Fig. 13: Predicted Attacks**

The above figure shows our predicted attacks obtained by our proposed models. In our proposed model we used a 30% test set from our actual data as a considered validation test. As compared to our existing attacks 75% obtained accurate results by accuracy justification.

**Conclusion**

This study offers a systematic method for categorizing and forecasting cyberattacks. Different sorts of cyber-attacks were categorized using a variety of approaches. We employed the categorization methods Random Forest and XGBoost. We develop a confusion matrix to identify the model performance following the application of the machine learning model. According to the report, the recall (RE) and precision (PR) for the first classification using Random Forest are both 69%. Our model's average accuracy (AC), which was compared with SVM, is 69%, demonstrating its superiority. The F1 69% score is represented by the average accuracy. Precision (PR) and recall (RE) accuracy for the second classification for the XGBoost model were both shown in the study to be 75% and 75%, respectively. Our model's average accuracy (AC) is 75%. Both models performed on average 69% to 75% accurately, which is superior than other well-known approaches' performance of 63%. The classification of cyberattacks using ANN is currently being tested.

**References**

Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In *Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1* (pp. 121-131). Springer Singapore.

Albladi, S. M., & Weir, G. R. (2018). A semi-automated security advisory system to resist cyber-attack in social networks. In *Computational Collective Intelligence: 10th International Conference, ICCCI 2018, Bristol, UK, September 5-7, 2018, Proceedings, Part I 10* (pp. 146-156). Springer International Publishing.

Alqubaiti, Z. Y. (2016). The Paradox of Social Media Security: A Study of IT Students’ Perceptions versus Behavior on Using Facebook.

Ahmad, W., Ahmed, S., Sheeraz, N., Khan, A., Ishtiaq, A., & Saba, M. (2020, February). Localization Error Computation for RSSI Based Positioning System in VANETs. In *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)* (pp. 1-6). IEEE.

Almukaynizi, M., Grimm, A., Nunes, E., Shakarian, J., & Shakarian, P. (2017, October). Predicting cyber threats through hacker social networks in darkweb and deepweb forums. In *Proceedings of the 2017 International Conference of the Computational Social Science Society of the Americas* (pp. 1-7).

Albladi, S. M., & Weir, G. R. (2018). A semi-automated security advisory system to resist cyber-attack in social networks.

Chambers, N., Fry, B., & McMasters, J. (2018, June). Detecting denial-of-service attacks from social media text: Applying nlp to computer security. In *Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers)* (pp. 1626-1635).

Fang, X., Xu, M., Xu, S., & Zhao, P. (2019). A deep learning framework for predicting cyber-attack rates. *EURASIP Journal on Information security*, *2019*, 1-11.

Husnain, G., Anwar, S., Sikander, G., Ali, A., & Lim, S. (2023). A Bio-Inspired Cluster Optimization Schema for Efficient Routing in Vehicular Ad Hoc Networks (VANETs). *Energies*, *16*(3), 1456.

Husnain, G., Anwar, S., Shahzad, F., Sikander, G., Tariq, R., Bakhtyar, M., & Lim, S. (2022). An Intelligent Harris Hawks Optimization Based Cluster Optimization Scheme for VANETs. *Journal of Sensors*, 2022.

Husnain, G., & Anwar, S. (2022). An intelligent probabilistic whale optimization algorithm (i-WOA) for clustering in vehicular ad hoc networks. *International Journal of Wireless Information Networks*, *29*(2), 143-156

Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2018). Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys & Tutorials*, *21*(1), 640-660.

Javed, A., Burnap, P., & Rana, O. (2019). Prediction of drive-by download attacks on Twitter. *Information Processing & Management*, *56*(3), 1133-1145.

Ju, A., Guo, Y., Ye, Z., Li, T., & Ma, J. (2019). Hetemsd: A big data analytics framework for targeted cyber-attacks detection using heterogeneous multisource data. *Security and Communication Networks*, *2019*.

Kim, Y., Kim, I., & Park, N. (2014). Analysis of cyber attacks and security intelligence. In *Mobile, Ubiquitous, and Intelligent Computing: MUSIC 2013* (pp. 489-494). Springer Berlin Heidelberg., and intelligent computing. Springer, Berlin, Heidelberg, 2014. 489- 494.

Onoh, G. (2018, August). Predicting cyber-attacks using publicly available data. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 6, No. 1, pp. 18-18).

Okutan, A., Yang, S. J., & McConky, K. (2017, April). Predicting cyber attacks with bayesian networks using unconventional signals. In *Proceedings of the 12th Annual Conference on Cyber and Information Security Research* (pp. 1-4).

Sarkar, S., Almukaynizi, M., Shakarian, J., & Shakarian, P. (2019). Predicting enterprise cyber incidents using social network analysis on dark web hacker forums. *The Cyber Defense Review*, 87-102.

Saeed, N., Ahmad, W., & Bhatti, D. M. S. (2018, March). Localization of vehicular ad-hoc networks with RSS based distance estimation. In *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1-6). IEEE.

Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2018). Data-driven cybersecurity incident prediction: A survey. *IEEE communications surveys & tutorials*, *21*(2), 1744-1772.

Shu, K., Sliva, A., Sampson, J., & Liu, H. (2018). Understanding cyber attack behaviors with sentiment information on social media. In *Social, Cultural, and Behavioral Modeling: 11th International Conference, SBP-BRiMS 2018, Washington, DC, USA, July 10-13, 2018, Proceedings 11* (pp. 377-388). Springer International Publishing.

Rege, M., & Mbah, R. B. K. (2018). Machine learning for cyber defense and attack. *Data Analytics*, *2018*, 83.

Wang, Z., & Zhang, Y. (2017, August). DDoS Event Forecasting using Twitter Data. In *IJCAI* (pp. 4151-4157).

Xu, M., Schweitzer, K. M., Bateman, R. M., & Xu, S. (2018). Modeling and predicting cyber hacking breaches. *IEEE Transactions on Information Forensics and Security*, *13*(11), 2856-2871.

1. Department of Computer Science, IQRA National University Peshawar 25100, Pakistan [tahz432@gmail.com](mailto:tahz432@gmail.com) [↑](#footnote-ref-1)
2. Corresponding Author, Department of Computer Science, IQRA National University Peshawar 25100, Pakistan, Department of Mechatronics Engineering, University of Engineering and Technology, Peshawar, 25100, Pakistan, [ghassan.husnain@gmail.com](mailto:ghassan.husnain@gmail.com) [↑](#footnote-ref-2)
3. Department of Computer Science, IQRA National University Peshawar 25100, Pakistan, [waqas.ahmad777@gmail.com](mailto:waqas.ahmad777@gmail.com) [↑](#footnote-ref-3)
4. University of Engineering and Technology, Peshawar, 25100, Pakistan, [gulbadan@uetpeshawar.edu.pk](mailto:gulbadan@uetpeshawar.edu.pk) [↑](#footnote-ref-4)
5. Department of Computer Systems Engineering, University of Engineering and Technology, Peshawar 25000, Pakistan, [muniba@uetpeshawar.edu.pk](mailto:muniba@uetpeshawar.edu.pk) [↑](#footnote-ref-5)