Analysis of Cybersecurity Using Machine Learning Techniques

Asma Tahseen[1], Md Imtiyaz Ali[2],

[1]Assistant Professor, Department of Computer Science and Engineering, Anurag University, Hyderabad.

[2]Assistant Professor, Department of Information Technology, Vignana Bharthi Institute of Technology, Hyderabad.

Abstract: Machine learning (ML) is a subset of artificial intelligence (AI) that deals with creating computer programs that can identify patterns in past data, learn from it, and make rational decisions with minimal or no human intervention. Safeguarding digital systems, including computers, servers, mobile phones, networks, and associated data from malicious attacks is referred to as cyber security. The two central parts of uniting cyber security with machine learning involve making allowance for cyber security in areas where machine learning applies, as well as leveraging the ability of machine learning in making possible cyber security. It may suit us by having varied beneficial contributions that incorporate fortifying machine learning models regarding their security, further maximizing cyber security methodologies towards maximum proficiency, as well as supporting easy, zero human contact zero-day attacks detection effectively. The field of cyber security has become increasingly complex because of the rapid growth of technology, posing several challenges to the protection of sensitive information and critical infrastructures. The aim of this paper is to apply three distinct systems that utilize machine learning in the context of cyber security. The first system examines the potential utilization of reinforcement learning to enhance cyber security. Reinforcement learning algorithms are trained to make the optimal decisions from their interactions with the environment by trial and error, which can be beneficial in adapting to new cyber threats. The second method targets malware detection as evasive and polymorphic malware have been challenging to detect using traditional signature-based detection. Multiple machine learning and deep learning techniques are employed in this endeavor to precisely detect and classify malicious software. The third solution employs machine learning and deep learning methods to solve the key issue of network intrusion detection. The performance of every system's machine learning model will be tested during the project through an array of datasets with evaluation metrics.

Keywords: Machine Learning, Machine Learning in Cyber Security, Cybersecurity.

Introduction: In this era, the cyberspace is expanding at a faster rate as a main source for a node to node information exchange with all its beauty and difficulties. The cyberspace is an important source to reach an unlimited amount of information and resources across the world. In 2017, the rate of internet usage was 48% worldwide, subsequently it rose to 81% for developing nations. The extensive scope of cyberspace involves much more than the internet alone, such as users, system resources, participant technical knowledge, and much more. Moreover, the cyber world plays a big role in the numerous vulnerabilities to cyberattacks and threats. Cybersecurity is a set of numerous strategies, tools, and processes designed to defend cyberspace from threats and cyberattacks. Cybercrimes are growing faster than the existing cybersecurity system in today's computer and information technology world. A computer system's susceptibility to threats can be traced to several factors, such as poor system configuration, inexperienced personnel, and a lack of techniques. Further development needs to be achieved in developing cybersecurity techniques because of the growing cyber threats.
Attack methods are evolving rapidly to breach systems and avoid generic signature-based protection, just as web and mobile technologies are doing so. Because they can rapidly respond to new and unknowable situations, machine learning methods offer potential solutions that can be utilized to solve such challenging and complicated problems. Numerous various machine learning methods have been effectively utilized to solve numerous problems in computer and information security. This paper discusses and highlights several machine-learning applications in cyber security. Machine learning: One of the mainly applied advanced techniques used to detect cybercrime is machine learning methods. Machine learning methods can be utilized to solve the weaknesses and limitations that traditional detection techniques have.

Cybersecurity

In the past half-century, the information and communication technology (ICT) sector has developed enormously, which is everywhere and heavily linked with our contemporary society. Hence, defending ICT systems and programs against cyber-attacks has seriously been a matter of concern of the security policymakers in recent days. The action of defending ICT systems from multiple cyber-threats or attacks came to be designated as cybersecurity. There are a number of aspects that relate to cybersecurity: information and communication technology protection measures; raw data and information contained therein and their processing and transmitting; related virtual and physical components of the systems; the level of protection from the implementation of those measures; and ultimately the related field of professional activity. In general, cybersecurity issues with the knowledge of various cyber-attacks and developing corresponding defense strategies that maintain some properties. Confidentiality is a property employed to avoid access and revelation of information to unauthorized individuals, entities or systems. Integrity is a property employed to avoid any alteration or destruction of information in an unauthorized way. Availability is a characteristic utilized for the guarantee of timely and reliable access of information assets and systems to an authorized entity.

Machine Learning in Cyber Security: The uptick in cyber attacks has made machine learning in cybersecurity a must-have for many companies. Although cyber attacks continue to grow in number and complexity, machine learning is evolving to address new threats. Machine learning's ability to analyze large amounts of data and spot patterns makes it ideal for detecting attacks in their earliest stages, exposing network vulnerabilities and anticipating when and how future cyber attacks will occur[1]. Three ty types of machine learning in cybersecurity There are three types of machine learning applied in cybersecurity: supervised learning, unsupervised learning and reinforcement learning[2],[3].

Supervised learning is where an algorithm is trained on labeled data, thereby learning how to structure data from the relationship between inputs and outputs. Human intervention is usually necessary to guide algorithms during training. Supervised learning is employed by machine learning algorithms to label data as neutral or malicious, detect threats such as denial-of-service attacks, and predict future cyber attacks[4]. Unsupervised learning is an algorithm trained on raw or unlabeled data, and it classifies and labels data automatically without human intervention. Security teams use unsupervised learning to train algorithms to identify new and more sophisticated cyber attacks, particularly as hackers learn various methods of breaching company defenses. Reinforcement learning is a error-and-trial method in which an algorithm acquires new functions by being rewarded for the right moves and penalized for wrong moves. Machine learning algorithms apply this method in cybersecurity to make them better equipped to identify more types of cyber attacks. Organizations also utilize reinforcement learning in order to automate routine tasks, leading to more effective IT and security procedures. Advantages of Machine Learning in Cybersecurity: With its myriad applications, machine learning is highly beneficial for IT and security professionals. Machine learning is able to adapt and improve in learning new functions as well as improve in executing existing ones independently, leading to automated processes[5],[6],[7]. Security and IT professionals can then leave the simple tasks to machine learning and use their time and resources for taking care of emerging cyber attacks, rectifying critical bugs and doing other complex tasks.

Capacity to Process Large Data Sets: Human beings can find it difficult to work with big data, but machine learning can rapidly process and analyze bigger data sets. Computer algorithms can identify trends more rapidly than human beings and notify teams of emerging cyber attacks. IT and security professionals can immediately act, eliminating cyber attacks at their nascent stages before they can proliferate. Improved Security Protocols: Examing a business's security architecture, machine learning code can identify vulnerabilities, suggest patches and assist teams in preparing for all types of cyber attacks. Through this process, security and IT teams are able to act against threats before they even occur, setting up the processes and infrastructure necessary to repel more sophisticated attacks. Adaptable Defense Systems: Not only does machine learning anticipate known cyber attacks[8],[9], but it can also learn about potential future attacks that are yet to be discovered by most organizations. Security teams can then strengthen their companies against escalating threats by tightening their security tech stacks and teaching employees about novel social engineering schemes and other cyber attacks[10],[11].

Methodology:

With increasing use of machine learning in cybersecurity, the identification and response of threats have been made more effective. The method of utilizing machine learning in the field of cybersecurity is discussed deeply in this paper, highlighting the pros, cons, and use cases of all the methods mentioned.

Data Collection and Preprocessing: Acquisition of Relevant Data: Finding and collecting cybersecurity datasets to train and test models. Data Cleaning and Transformation: Preprocessing methods for dealing with missing data, outliers, and maintaining data quality. Feature Extraction and Engineering: Choice of useful features and feature engineering for enriching model performance.

Model Selection and Evaluation: Algorithm Selection: Selecting suitable machine learning algorithms, e.g., decision trees, support vector machines, or neural networks, depending on the problem and data types[12],[13]. Training and Testing: Dividing the dataset into training and testing sets, maintaining suitable sample sizes, and evaluating model generalization. Performance Metrics: Identifying evaluation metrics such as accuracy, precision, recall, F1-score, and area under the curve (AUC) to quantify the performance of the models.

Model Training and Optimization: Model Training Methods: Utilizing supervised, unsupervised, or semi-supervised learning methods depending on data availability and labeling. Hyperparameter Tuning: Model parameter optimization to maximize performance using grid search, random search, or Bayesian optimization techniques. Regularization and Overfitting Prevention: Using methods such as L1 and L2 regularization, dropout, and early stopping to avoid overfitting.. Deployment and Integration: Real-time Monitoring: Putting models into actual systems to constantly monitor and provide instant responses to cyber threats. Integration with Security Infrastructure: Introducing machine learning models into established security infrastructure, like intrusion detection or firewalls. Model Updates and Maintenance: Creating methods for updating models using new information and adjusting to shifting threat landscapes.

Spam

This is done by training a machine learning model using a dataset of labeled emails, with each email labeled as either spam or not spam. When the machine learning model is trained, it identifies patterns and features that differentiate between spam emails and legitimate emails. These patterns might be certain words or phrases frequently used in spam emails, the occurrence of specific types of attachments or URLs, or features of the sender of the email. After training the model, it can be used in a production setting, where it can scan incoming emails and predict if they are spam or not. The model checks different features extracted from the email, including the subject line, sender's address, content, and other applicable metadata. Depending on the model's prediction, the email can be classified accordingly. Spam messages can be filtered out, not allowing them to reach users' mailboxes, while valid messages can be passed through. It should be noted that the machine learning model must be periodically updated and tuned to keep up with new spamming methods and trends. Since spammers continuously change their strategies, the model must be retrained using new data to maintain its accuracy and efficiency in classifying spam.

Phishing Detection: Phishing is targeted at stealing individual sensitive information. Researchers [] have determined three main categories of anti-phishing measures: detective (monitoring, content filtering, anti-spam), preventive (authentication, patch and change management), and corrective (site takedown, forensics) ones.

Table 1: Main Categories of Anti-Phishing Measures

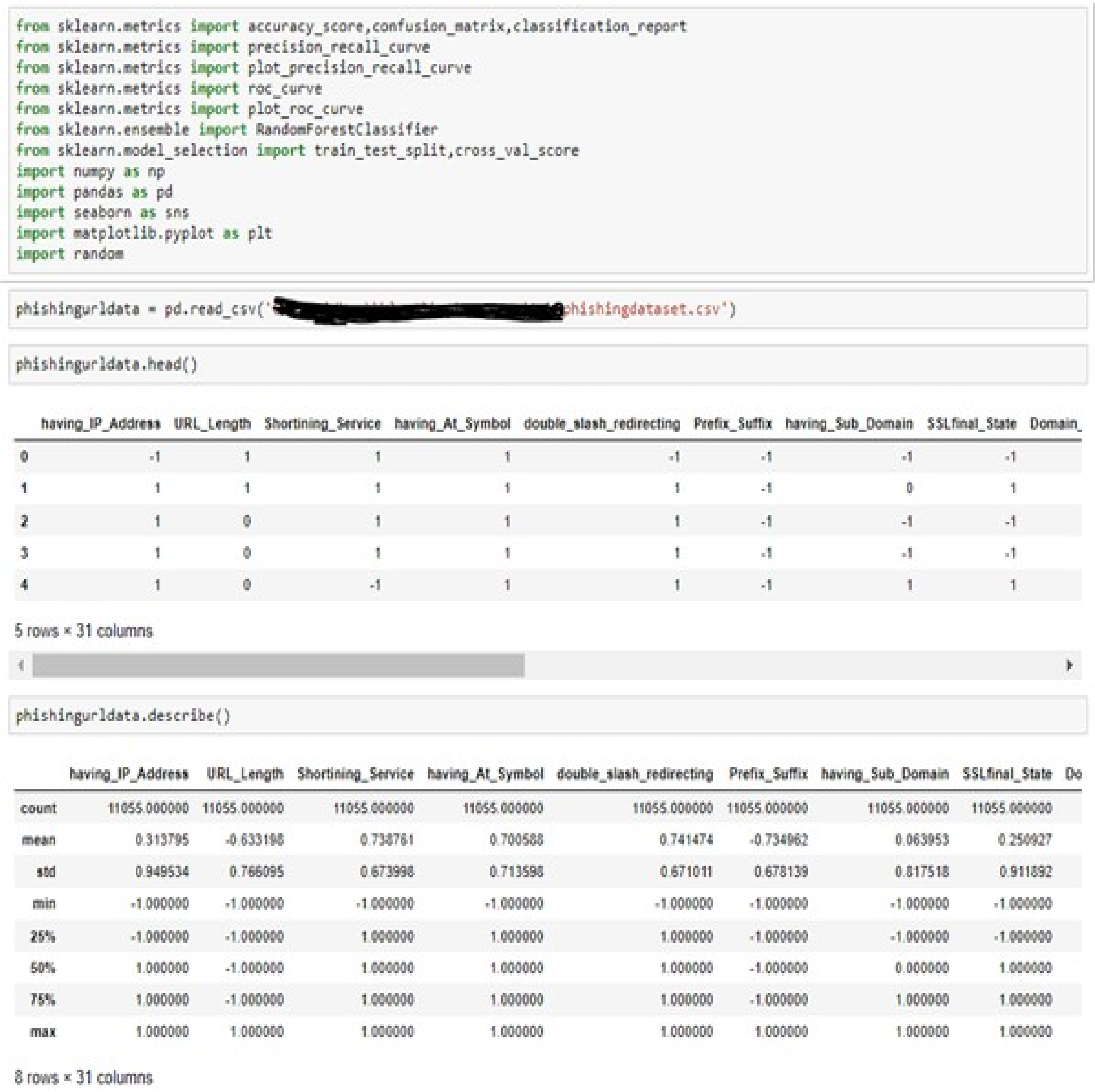
Detective Solutions	Preventive Solutions	Corrective Solutions
• Monitors account life cycle • Brand monitoring • Disables web duplication • Performs content filtering Anti-Malware • Anti-Spam	• Authentication • Patch and change management • Email authentication • Web application security	• Phishing site takedown • Forensics and investigation

Implementation and Results:

Phishing is another prevalent form of cyber-attack in which a cyber criminal sends an imitation message that will mislead an individual to disclose confidential information to the attacker or to download malicious software onto the target's infrastructure, including ransomware. Machine learning algorithms are among the most potent and effective methods in phishing website detection. Phishing attacks share some prevalent characteristics that can be detected using machine learning techniques.

By working with a data set consisting of key features or attributes of URLs, I was successful in predicting phishing websites by adopting a machine learning model. For more on the dataset, see UCI Machine Learning Repository. Below is the python code snippet.
I imported this dataset analytics platform that comprises machine learning, data discovery, text analytics and advanced visualization and dashboarding.

sophisticated visualization and dashboarding.



```
from sklearn.metrics import accuracy_score,confusion_matrix,classification_report
from sklearn.metrics import precision_recall_curve
from sklearn.metrics import plot_precision_recall_curve
from sklearn.metrics import roc_curve
from sklearn.metrics import plot_roc_curve
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split,cross_val_score
import numpy as np
import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt
import random
```

```
phishingurldata = pd.read_csv('[redacted]phishingdataset.csv')
```

```
phishingurldata.head()
```

	having_IP_Address	URL_Length	Shortining_Service	having_At_Symbol	double_slash_redirecting	Prefix_Suffix	having_Sub_Domain	SSLfinal_State	Domain_
0	-1	1	1	1	-1	-1	-1	-1	
1	1	1	1	1	1	-1	0	1	
2	1	0	1	1	1	-1	-1	-1	
3	1	0	1	1	1	-1	-1	-1	
4	1	0	-1	1	1	-1	1	1	

5 rows × 31 columns

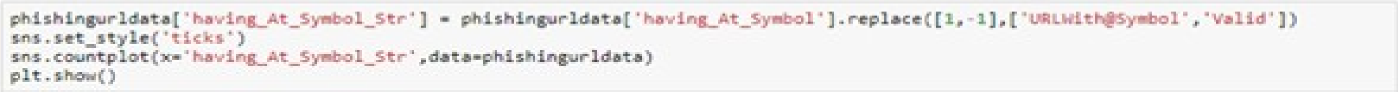
```
phishingurldata.describe()
```

	having_IP_Address	URL_Length	Shortining_Service	having_At_Symbol	double_slash_redirecting	Prefix_Suffix	having_Sub_Domain	SSLfinal_State	Do
count	11055.000000	11055.000000	11055.000000	11055.000000	11055.000000	11055.000000	11055.000000	11055.000000	
mean	0.313795	-0.633198	0.738761	0.700588	0.741474	-0.734962	0.063953	0.250927	
std	0.949534	0.766095	0.673998	0.713598	0.671011	0.678139	0.817518	0.911892	
min	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000	-1.000000	
25%	-1.000000	-1.000000	1.000000	1.000000	1.000000	-1.000000	-1.000000	-1.000000	
50%	1.000000	-1.000000	1.000000	1.000000	1.000000	-1.000000	0.000000	1.000000	
75%	1.000000	-1.000000	1.000000	1.000000	1.000000	-1.000000	1.000000	1.000000	
max	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	

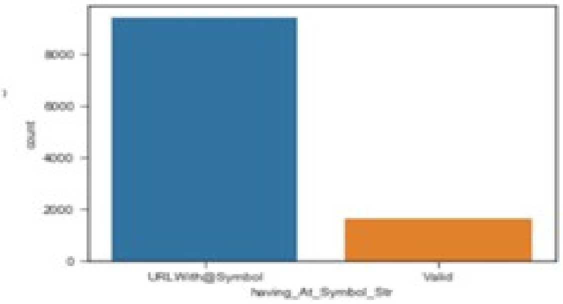
8 rows × 31 columns

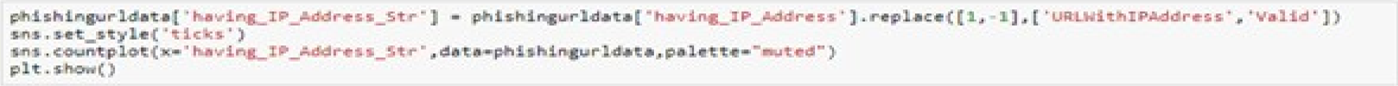
Data Exploration

The dataset has 30 features. Here I explored some of the features. The URL has a detailed description of each feature and the values derived, by applying the condition such as length, PageRank, google index, age etc. applied on the attributes of the target URL.

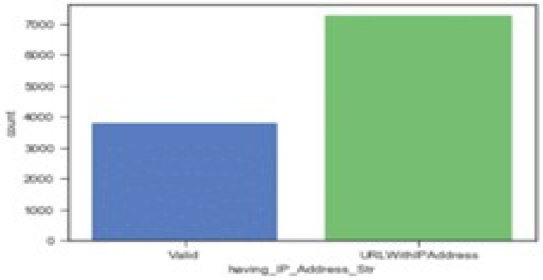


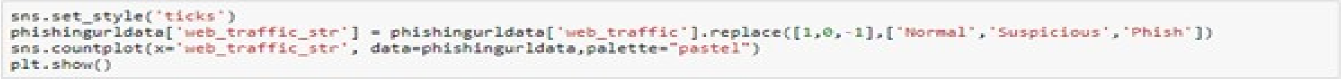
```
phishingurldata['having_At_Symbol_Str'] = phishingurldata['having_At_Symbol'].replace([1,-1],['URLWith@Symbol','Valid'])
sns.set_style('ticks')
sns.countplot(x='having_At_Symbol_Str',data=phishingurldata)
plt.show()
```



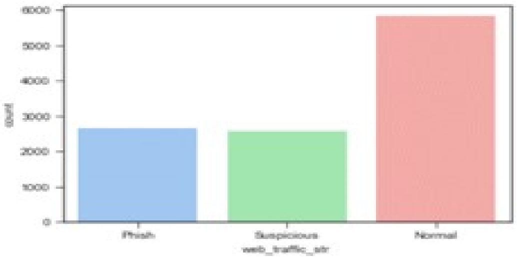


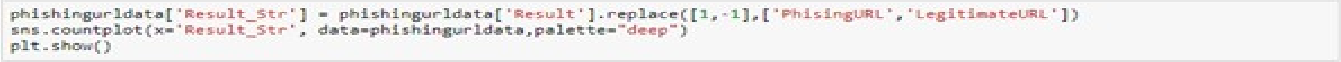
```
phishingurldata['having_IP_Address_Str'] = phishingurldata['having_IP_Address'].replace([1,-1],['URLWithIPAddress','Valid'])
sns.set_style('ticks')
sns.countplot(x='having_IP_Address_Str',data=phishingurldata,palette="muted")
plt.show()
```



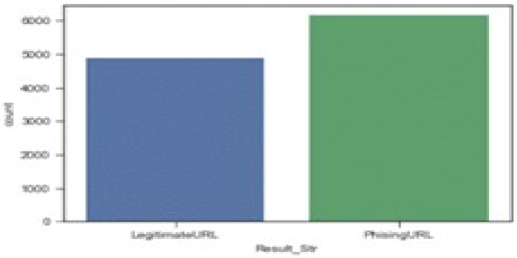


```
sns.set_style('ticks')
phishingurldata['web_traffic_str'] = phishingurldata['web_traffic'].replace([1,0,-1],['Normal','Suspicious','Phish'])
sns.countplot(x='web_traffic_str', data=phishingurldata,palette="pastel")
plt.show()
```

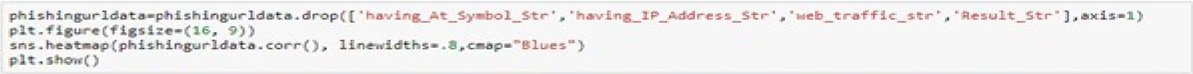




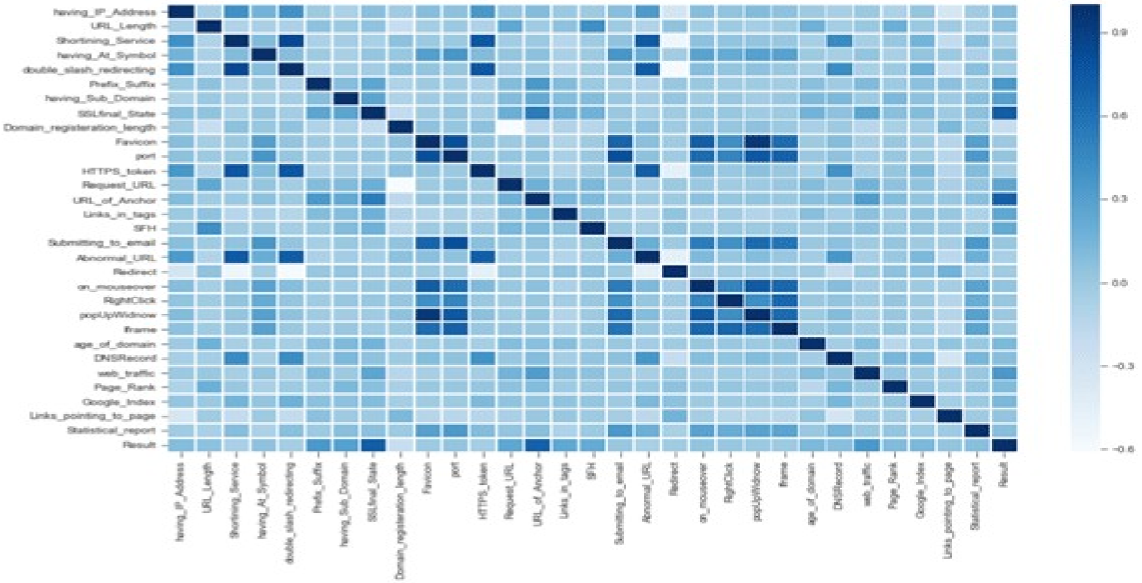
```
phishingurldata['Result_Str'] = phishingurldata['Result'].replace([1,-1],['PhisingURL','LegitimateURL'])
sns.countplot(x='Result_Str', data=phishingurldata,palette="deep")
plt.show()
```



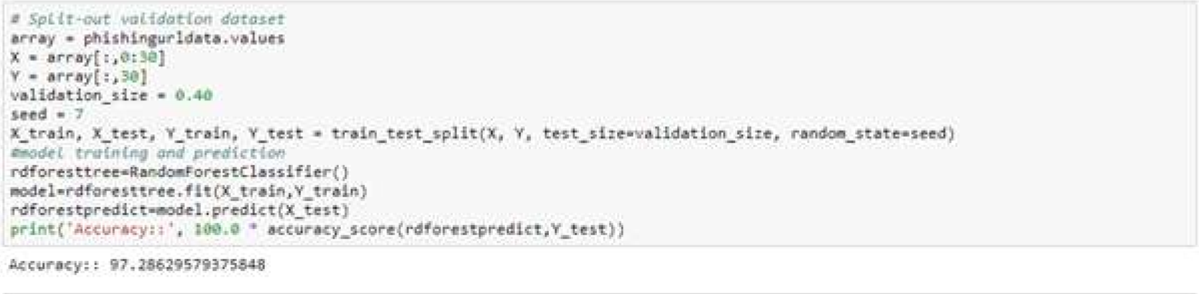
Below is the correlation heatmap, each square showing the correlation between the variables on each axis.



```
phishingurldata=phishingurldata.drop(['having_At_Symbol_Str','having_IP_Address_Str','web_traffic_str','Result_Str'],axis=1)
plt.figure(figsize=(16, 9))
sns.heatmap(phishingurldata.corr(), linewidths=.8,cmap="Blues")
plt.show()
```



Random Forest Classifier algorithm has been fitted on the training dataset and applied on the test dataset. This model has around 97 percent accuracy.



```
# Split-out validation dataset
array = phishingurldata.values
X = array[:,0:30]
Y = array[:,30]
validation_size = 0.40
seed = 7
X_train, X_test, Y_train, Y_test = train_test_split(X, Y, test_size=validation_size, random_state=seed)
#model training and prediction
rdforesttree=RandomForestClassifier()
model=rdforesttree.fit(X_train,Y_train)
rdforestpredict=model.predict(X_test)
print('Accuracy::', 100.0 * accuracy_score(rdforestpredict,Y_test))

Accuracy:: 97.28629579375848
```

The classification report shown below is used to measure the quality of predictions from the algorithm. It displays the model's precision, recall and F1 score. The metrics are calculated by using true and false positives and true and false negatives. There are four ways to check if the predictions are right or wrong:

- TN / True Negative: when a case was negative and predicted negative
- TP / True Positive: when a case was positive and predicted positive
- FN / False Negative: when a case was positive but predicted negative
- FP / False Positive: when a case was negative but predicted positive

Precision – Accuracy of positive predictions.

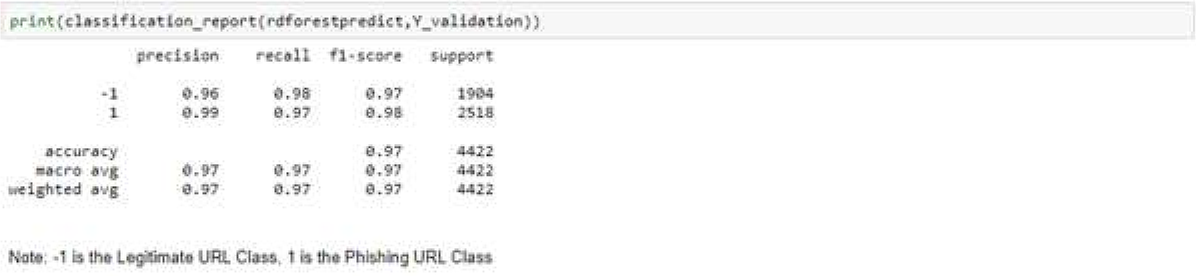
Precision = TP/(TP + FP)

Recall: Fraction of positives that were correctly identified.

Recall = TP/(TP+FN)

The F1 score is a weighted harmonic mean of precision and recall such that the best score is 1.0 and the worst is 0.0.

F1 Score = 2*(Recall * Precision) / (Recall + Precision)



```
print(classification_report(rdforestpredict,Y_validation))
```

```
              precision    recall  f1-score   support

          -1       0.96      0.98      0.97      1904
           1       0.99      0.97      0.98      2518

    accuracy                           0.97      4422
   macro avg       0.97      0.97      0.97      4422
weighted avg       0.97      0.97      0.97      4422
```

Note: -1 is the Legitimate URL Class, 1 is the Phishing URL Class

The accuracy can be further improved by applying other algorithms or tuning the parameters; however, this blog is mainly focused on demonstrating one of the use cases leveraging ML in cybersecurity.

Data plays a vital role in the field of machine learning and the availability of quality data that support the environment will reduce false positives. However, as this example shows, machine learning as a complement to cybersecurity can be more proactive and efficient.

Conclusion:

In summary, machine learning methods are proving to be very effective in the cybersecurity field. Conventional detection methods have proved to be inadequate in terms of responding to the evolving character of cybercrimes, owing to the sheer growth of cyber threats and attacks. By designing intelligent and automatic systems that are capable of examining large volumes of data, identify patterns, and identify possible security vulnerabilities in real-time, machine learning offers an answer. This article has discussed various applications of machine learning in cybersecurity, including spam classification, malware detection, intrusion detection, and others. These software developers utilize machine learning techniques to enhance threat detection and response times. Machine learning algorithms are capable of learning the difference between valid and malicious activity by training on labeled data, allowing one to detect cyber threats and attacks. However, there are challenges to implementing machine learning in cybersecurity. The quality and diversity of training data play an important role in determining the performance of machine-learning models. Accessing relevant and representative data is challenging, particularly considering the speed at which cyber threats are evolving. To respond to new attack methods, check their validity, and optimize their effectiveness, machine-learning models must also be constantly updated and retrained. Applying machine learning with large data and iota security also poses privacy and security concerns. In employing large data to enhance the efficacy of machine learning models, confidentiality and data privacy need to be maintained. Techniques such as federated learning have enabled collaboration in threat intelligence without compromising raw data privacy. It can also be utilized further in the investment fields, security, self-driving car etc. Current Deep learning can also be utilized in these sections. All these works paved ways for deeper research on deep learning methodologies in order to obtain better results and challenging cryptographic implementations.

References

[1] Rivest, R.L. (1993). Cryptography and machine learning. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds) Advances in Cryptology — ASIACRYPT '91. ASIACRYPT 1991. Lecture Notes in Computer Science, vol 739.

Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-57332-1_36

[2] Alani, M. (2019). Applications of Machine Learning in Cryptography: A Survey. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP '19). Association for Computing Machinery, New York, NY, USA, pp. 23–27. https://doi.org/ 10.1145/3309074.3309092.

[3] Tom Mitchell (1997). Machine Learning. First ed., McGraw Hill. pp. 414.

[4] Ethem Alpaydin (2010). Introduction to Machine Learning. 2nd ed., The MIT Press Cambridge.

Massachusetts, London, England. pp. 579.

[5] Mishra, S., & Bali, S. (2013). Public key cryptography using genetic algorithm. International J Recent Technol. Eng.(IJRTE), 2(2), 150-154.

[6] Kumar, Krishan and Sagar, Vikas. (2014). A Symmetric Key Cryptographic Algorithm Using Counter

Propagation Network (CPN). 10.1145/2677855.2677906.

[7] Sahana,S,K., and Mahanti,P.K. (2015). An Analysis of Email Encryption using Neural Cryptography. Journal of Multidisciplinary Engineering Science and Technology, Volume-2(1), pp. 83-87, ISSN: 3159- 0040, www.jmest.org/wp-content/uploads/JMESTN42350307.pdf.

[8] Atee, Hayfaa and Ahmad, Robiah & Noor, Norliza & Yasari, Abidulkarim. (2016). Machine learning-based

key generating for cryptography. 11. 1829-1834. 10.3923/jeasci.2016.1829.1834.

[9] Sharma Kartik; Aggarwal Ashutosh; Singhania Tanay; Gupta Deepak; Khanna Ashish (2019). Hiding Data in Images Using Cryptography and Deep Neural Network. Journal of Artificial Intelligence and Systems, 1, 143–162. https://doi.org/10.33969/AIS.2019.11009.

[10] Naveena, V., and Satyanarayana, D.S. (2019). Symmetric Cryptography using Neural Networks. ”

International Research Journal of Engineering and Technology (IRJET), 6(8), 1556-1558.

[11] Thoms GRW, Muresan R, Al-Dweik A (2019). Chaotic encryption algorithm with key-controlled neural networks for intelligent transportation systems. IEEE Access. 7:158697–158709. doi: 10.1109/ACCESS.2019.2950007.

[12] Wang, Peng, and Xiang Li. (2021). "TEDL: A Text Encryption Method Based on Deep Learning" Applied

Sciences 11, no. 4: 1781. https://doi.org/10.3390/app11041781.