Int. J. Inf. Cybersec.-2022

Applying Machine Learning Algorithms for Detecting Phishing Websites: Applications of SVM, KNN, Decision Trees, and Random Forests

Olaolu Kayode-Ajala
Independent researcher

Abstract

Phishing attacks present a significant risk to both individual and organizational data security. Such attacks often mimic legitimate websites to steal sensitive information. Traditional countermeasures like blacklists and rule-based systems have shown limitations in tackling this dynamic threat. This research applied machine learning algorithms such as Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Decision Trees, and Random Forests to automate and enhance the process of detecting phishing websites. A dataset of 6,157 benign and 4,898 phishing URLs was used for the purpose of this study. Each URL is characterized by 30 different features extracted from various sources, like WHOIS database and the webpage's HTML content, covering different aspects like SSL State, URL length, and the presence of specific symbols in the URL. SVM provided an accuracy rate of 95% with a precision of 0.95 and 0.94 for phishing and benign URLs, respectively. KNN demonstrated an overall accuracy of 94%, almost matching the SVM model's performance. Decision Trees and Random Forest models showed the highest accuracy of 96% and 97%, respectively. These models were found to be highly precise, demonstrating F1-scores above 0.93 for both classes. Important features contributing to the model's success were also identified, with SSL_State showing the highest level of importance across both Decision Trees and Random Forests models. Feature importance analysis revealed that the models rely heavily on specific features like "SSL_State,"

"URL_of_Anchor_External," and "Web_Traffic" for classification. Interestingly, these features also have moderate to strong correlations with the target variable, reinforcing their significance in phishing website detection.

Keywords: *Cybersecurity, Decision Trees, Machine Learning, Phishing Attacks, Random Forests, Support Vector Machines, URL Features*

Introduction

The proliferation of internet usage in recent years has led to an exponential increase in the volume of personal information that individuals share in online environments. Social media platforms, online banking systems, and e-commerce websites are common mediums where users willingly provide data ranging from basic identification details to highly sensitive information such as credit card numbers and medical records. While the convenience and utility offered by these online services are unquestionable, they also present a host of security challenges (*1*, *2*). The digital architecture supporting these platforms is continually targeted by malicious entities aiming to exploit vulnerabilities for unauthorized access to data.

In light of the massive data repositories that are generated, there exists an acute vulnerability to cyber-attacks, particularly for activities that involve financial transactions. Financial institutions, payment gateways, and even individuals making peer-to-peer payments are susceptible to a range of cyber threats that include identity theft, phishing, ransomware attacks, and unauthorized fund transfers. These types of cybercrimes have grown more sophisticated over time, leveraging advanced methods such as machine learning algorithms for password cracking and employing highly encrypted malware that can evade traditional cybersecurity measures. (*3–5*) The consequence of such threats can be devastating, ranging from monetary loss to the compromise of personal reputations and even national security, depending on the scale of the breach (*6*).

Phishing is a specialized form of identity theft that employs a combination of social engineering methods and advanced attack vectors to illicitly acquire financial or personal information from unwary individuals (*7–9*). In a typical phishing scheme, the attacker, often referred to as the "phisher," aims to manipulate the target into engaging with fraudulent content (*10*, *11*). This is usually executed by sending an email or other forms of communication that convincingly imitate legitimate institutions or services. The messages frequently contain a Uniform Resource Locator (URL) that directs the recipient to a rogue website designed to mimic an authentic platform (*12*, *13*). Once the victim interacts with this counterfeit webpage, often by entering login credentials or other sensitive information, the data is captured and sent to the attacker for exploitation (*14*, *15*).

Phishing attacks can be categorized based on their method of delivery and target. One common form is email phishing, wherein the attacker sends fraudulent emails that appear to come from a trustworthy source. These emails usually contain a call to action, such as asking the recipient to confirm their account details or make a payment. They may contain links to malicious websites designed to capture personal information or install malware on the user's system (*16*). The fraudulent websites often closely resemble legitimate ones, making it difficult for users to distinguish between the two. With the acquired data, the attacker can then commit identity theft, financial fraud, or gain unauthorized access to the victim's accounts (*17*, *18*).

Another prevalent form is spear phishing, which is a more targeted version of phishing attacks. Spear phishing involves customized communication designed to trick specific individuals or organizations (*19*, *20*). Unlike general phishing emails that are sent to a large audience, spear phishing emails are tailored for a particular victim, often incorporating personal information to make them more believable. For instance, an attacker might use details from the victim's social media accounts, company websites, or other publicly available sources to create convincing content (*21*). This heightened level of personalization makes spear phishing more effective and therefore more dangerous than generalized phishing attacks (*22*).

Voice phishing, or "vishing," employs phone calls or voice messages rather than digital communication channels to trick victims. The attacker typically poses as a representative from a legitimate organization, such as a bank or government agency, and seeks to obtain personal or financial information from the victim. The sense of immediacy often conveyed in these calls can be particularly compelling, making it more likely that the target will divulge sensitive information (*23*, *24*). In some vishing attacks, the caller may even manipulate caller ID information to appear as if they are calling from a trusted number.

Traditional methods of combating phishing, such as rule-based systems or blacklists, often lag behind the rapidly evolving tactics employed by attackers. AI and machine learning algorithms can analyze large datasets and identify patterns or anomalies much more swiftly and accurately. For instance, machine learning models can be trained to scrutinize the text and hyperlinks in emails to determine the likelihood of a phishing attempt. These algorithms evaluate multiple features (*25*), such as the sender's reputation, the presence of suspicious phrases, and deviations from normal communication patterns, to assess the authenticity of incoming messages (*26*, *27*).

Machine learning techniques also contribute to enhancing the capabilities of spam filters. While basic spam filters operate based on pre-defined rules, machine learning-enhanced

filters adapt over time, learning from new instances of phishing attempts to improve their detection capabilities. This dynamic learning approach helps in creating a more resilient system that can cope with innovative phishing strategies. Additionally, some machine learning algorithms focus on behavioral analytics, tracking how users interact with websites or emails. Any deviations from established behavioral patterns could trigger a warning or initiate additional layers of verification, thereby adding an extra layer of security against phishing attacks.

In organizational settings, AI and machine learning technologies are being integrated into Security Information and Event Management (SIEM) systems. These systems collect and analyze security data from across an organization's infrastructure (*28*). Machine learning algorithms within SIEM systems can correlate data from different sources to detect potentially suspicious activities that might otherwise go unnoticed. For example, if an employee clicks on a link in a phishing email and subsequently engages in unusual data access or transfer behavior, the SIEM system can flag this series of actions for further investigation (*29*). The process usually starts with the attacker sending a seemingly legitimate message via email, text, or social media. This message often contains a link to a fraudulent website that closely mimics a genuine site. When the victim clicks on the link, they are redirected to the counterfeit site and prompted to enter their sensitive information. Once submitted, the information is captured by the attacker for malicious purposes such as unauthorized access to accounts, financial theft, or identity fraud (*30*, *31*).

Another variant of phishing involves tricking individuals into downloading malicious software. In this case, the phishing email or message might contain an attachment that appears to be a benign file, such as a document or image. Once downloaded and opened, the malicious software can infect the user's computer, granting the attacker unauthorized access or the ability to execute other harmful actions remotely.

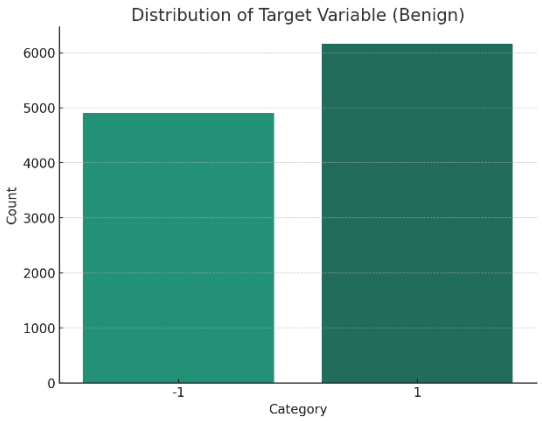
Attackers often use social engineering techniques to make the phishing attempt more convincing. For instance, they might personalize the message by using the victim’s name or referring to recent transactions or activities that the victim is likely to recognize. They may also exploit current events or crises to instill a sense of urgency, encouraging the victim to take immediate action without questioning the legitimacy of the request.

Data and features

The dataset contains 6,157 samples categorized as legitimate (represented by the value 1) and 4,898 samples categorized as phishing (represented by the value -1), as displayed in figure 1. The dataset is relatively balanced between the two classes, which is favorable for model training and evaluation.

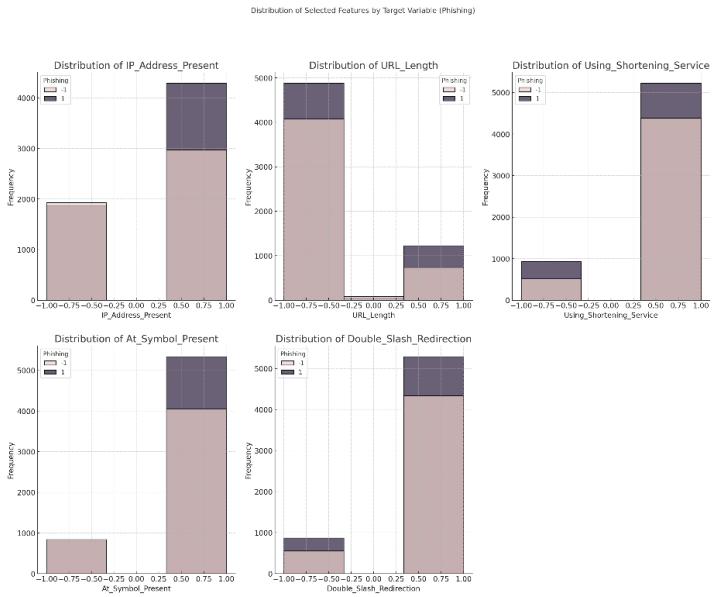
Table 1 provides list of 30 distinct features that are employed for the analysis of website legitimacy and identification of phishing attempts. The table is structured with three primary columns: "No.," "Feature Name," and "Description." The "No." column serves as an ordinal indicator for each feature, starting from 1 and ending at 30. The "Feature Name" column specifies the name assigned to each feature for easy identification, while the "Description" column provides a brief but detailed explanation of what each feature represents or signifies. The features span a wide range of website attributes, from URL-related features like "Abnormal_URL" and "At_Symbol_Present" to more technical aspects such as "DNS_Record" and "SSL_State."

Figure 1. Distribution of the target variable



The table's features fall into several categories that broadly address the attributes commonly associated with phishing websites. For example, features like "Abnormal_URL" and "Domain_Age" focus on the URL and domain-related information, aiming to ascertain the authenticity of the website based on established patterns and data such as the WHOIS database and domain registration period. Similarly, features like "Disabling_Right_Click" and "Using_PopUp_Window" are related to the website's user interface and functionality, probing for signs of deceptive or misleading practices. "Indexed_By_Google" and "Web_Traffic" concentrate on the website's visibility and popularity, offering metrics that can be linked to its legitimacy.

Figure 2. Distribution of a set of selected features with respect to the target



Security aspects are also featured with "SSL_State" and "Server_Form_Handler" examining the website's security protocols. Others, like "Submitting_Info_To_Email" and "In_Top_Phishing_IPs," focus on actions that are more directly related to phishing tactics, such as redirecting user information or being associated with known phishing IP addresses. Some features are tailored to study the behavior of webpage elements, as evidenced by entries like "Links_In_Tags" or "Request_URL_External_Objects," which examine the source and destination of various elements and links on the webpage. Overall, the table presents a thorough set of features designed to scrutinize websites for a broad array of phishing indicators.

Table 1. Features used

No.	Feature Name	Definition
1	Abnormal_URL	Extracted from the WHOIS database; for a legitimate website, identity is typically part of its URL.
2	At_Symbol_Present	Denotes the presence of the '@' symbol in the URL, which can lead browsers to ignore everything preceding it.

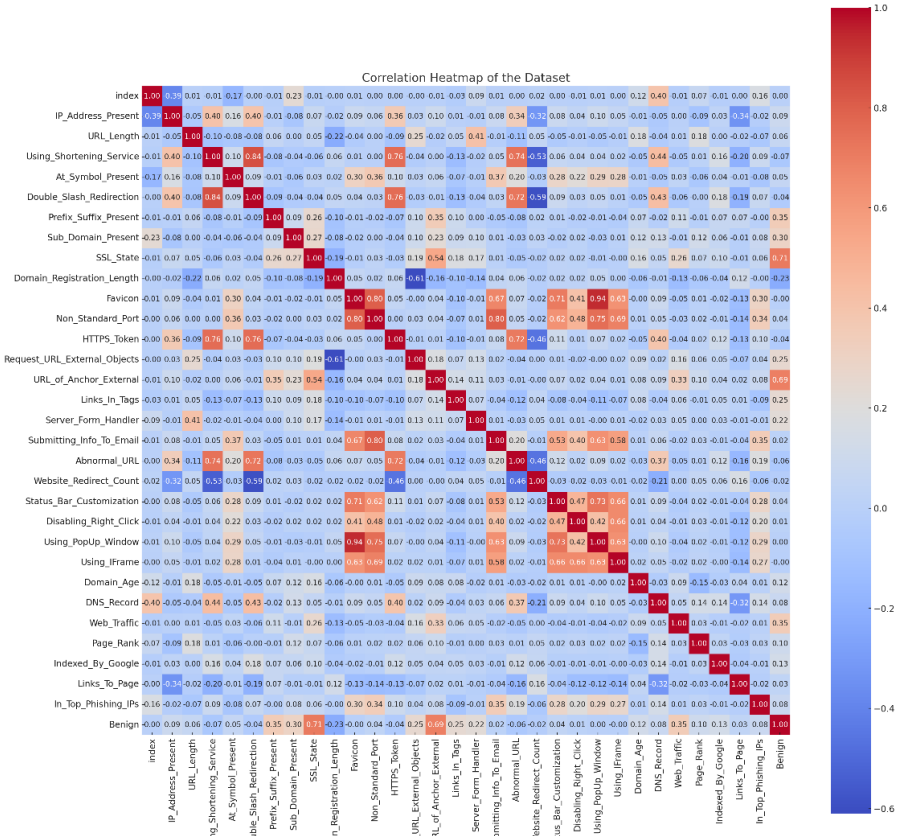
3	Disabling_Right_Click	Specifies whether the right-click functionality is disabled.
4	DNS_Record	Indicates whether a DNS record is present.
5	Domain_Age	Reflects the age of the domain; domains less than a month old are considered suspicious.
6	Domain_Registration_Length	Based on the registration length of the domain; phishing websites often have shorter registration periods.
7	Double_Slash_Redirection	Indicates the presence of '//' in the URL, which can redirect the user to another website.
8	Favicon	Indicates whether the favicon is loaded from a different domain than the one shown in the address bar.
9	HTTPS_Token	Indicates the presence of a deceptive HTTPS token in the URL.
10	IP_Address_Present	Indicates whether an IP address is used instead of a domain name in the URL.
11	Indexed_By_Google	Indicates whether the website is indexed by Google.
12	In_Top_Phishing_IPs	Indicates whether the IP address belongs to a list of top phishing IPs.
13	Links_In_Tags	Reflects the use of Meta, Script, and Link tags in the HTML document.
14	Links_To_Page	Specifies the number of links pointing to the webpage.
15	Non_Standard_Port	Specifies whether a non-standard port is used.
16	Page_Rank	Provides a value between 0 and 1 to measure the importance of the webpage on the internet.
17	Prefix_Suffix_Present	Specifies whether prefixes or suffixes separated by '-' are added to the domain name.
18	Request_URL_External_Objects	Examines whether external objects like images, videos, and sounds are loaded from another domain.
19	SSL_State	Reflects the SSL state of the website.
20	Server_Form_Handler	Specifies if the domain name in Server Form Handlers (SFHs) is different from the domain name of the webpage.
21	Status_Bar_Customization	Indicates the use of JavaScript to show a fake URL in the status bar.
22	Submitting_Info_To_Email	Indicates whether the phisher might be redirecting user information to an email.
23	Sub_Domain_Present	Indicates the presence of a subdomain in the URL.
24	URL_Length	Reflects the length of the URL; long URLs can be used by phishers to hide suspicious parts in the address bar.
25	URL_of_Anchor_External	Similar to "Request_URL_External_Objects," but specific to anchor elements defined by the <a> tag.
26	Using_IFrame	Specifies the use of the IFrame HTML tag to display an additional webpage.
27	Using_PopUp_Window	Indicates the use of pop-up windows on the webpage.
28	Using_Shortening_Service	Specifies whether the webpage uses a URL shortening service.

29	Web_Traffic	Measures the popularity of the website by the number of visitors.
30	Website_Redirect_Count	Specifies the number of times the website redirects; more than four is considered suspicious.

Result

In the heatmap, in figure 3. It is evident that some features have moderate to strong correlations with the target variable, while others show weak or negligible correlations. Specifically, variables like "SSL_State," "Web_Traffic," and "Page_Rank" seem to have higher positive correlations with the "Benign" variable, suggesting that they might be significant predictors for classifying a URL as benign or phishing.

Figure 4. correlation heatmap



The table 2 summarizes the performance metrics for four different machine learning models—Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Trees, and Random Forest—in the task of classifying phishing URLs (Class -1) and benign URLs (Class 1). The metrics encapsulate key evaluation standards: precision, recall, F1-score, and overall accuracy. Across all four models, the precision scores for Class -1 range from 0.94 to 0.97, while for Class 1, they range from 0.94 to 0.96. The Random Forest model performs slightly better than the others, achieving the highest precision score of 0.97 for Class -1. This high precision indicates that the model is highly accurate in identifying phishing URLs with minimal false positives. Precision rates are closely matched for Class 1 across all models, suggesting that they are equally adept at correctly identifying benign URLs.

Table 2. Model performances

Metric	SVM	KNN	Decision Trees	Random Forest
Precision (Class -1)	0.95	0.94	0.95	0.97
Precision (Class 1)	0.94	0.94	0.96	0.96
Recall (Class -1)	0.92	0.92	0.95	0.95
Recall (Class 1)	0.97	0.95	0.96	0.98
F1-score (Class -1)	0.94	0.93	0.95	0.96
F1-score (Class 1)	0.95	0.95	0.96	0.97
Overall Accuracy	0.95	0.94	0.96	0.97

The recall values for Class -1 and Class 1 provide insights into the models' sensitivity, that is, their ability to identify the actual instances of each class. The Random Forest model again marginally outperforms the other models with a recall rate of 0.98 for Class 1, indicating that it successfully identifies a higher percentage of actual benign URLs. For Class -1, the Decision Trees and Random Forest models both achieve a recall rate of 0.95, which is higher than the 0.92 achieved by SVM and KNN models. High recall rates across all models signify that they are robust in capturing most of the positive instances for both phishing and benign URLs.

The F1-score, a balanced measure of precision and recall, further confirms the models' capabilities. All four models achieve F1-scores above 0.9 for both classes, signifying that they don't compromise on either of the constituent metrics. The Random Forest model scores highest with F1-scores of 0.96 for Class -1 and 0.97 for Class 1, affirming its

superior balance between precision and recall. The overall accuracy metric provides a general view of each model's performance. Random Forest leads with an overall accuracy of 0.97, followed closely by Decision Trees at 0.96, SVM at 0.95, and KNN at 0.94. The consistently high accuracy across all models highlights their reliability and effectiveness in classifying URLs, but the Random Forest model shows a slight edge over the others.

Figure 5. SVM evaluation metrices

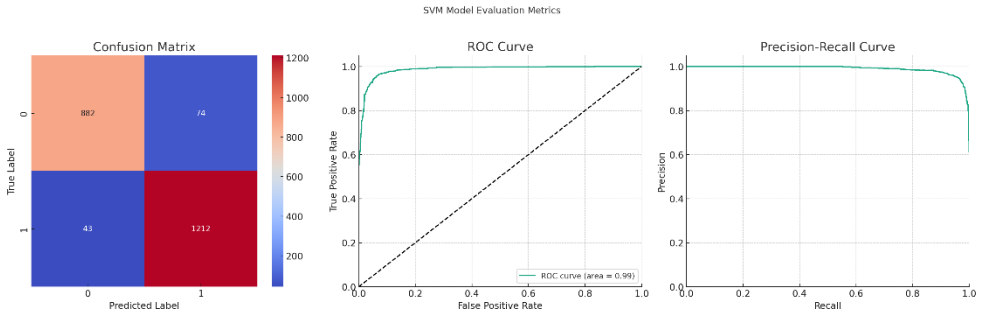
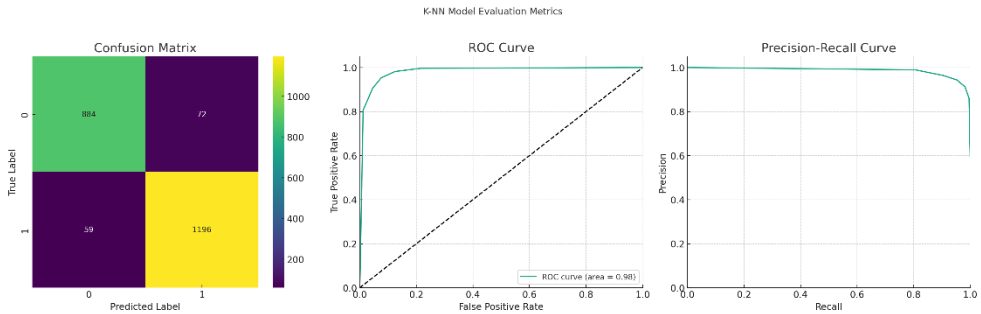
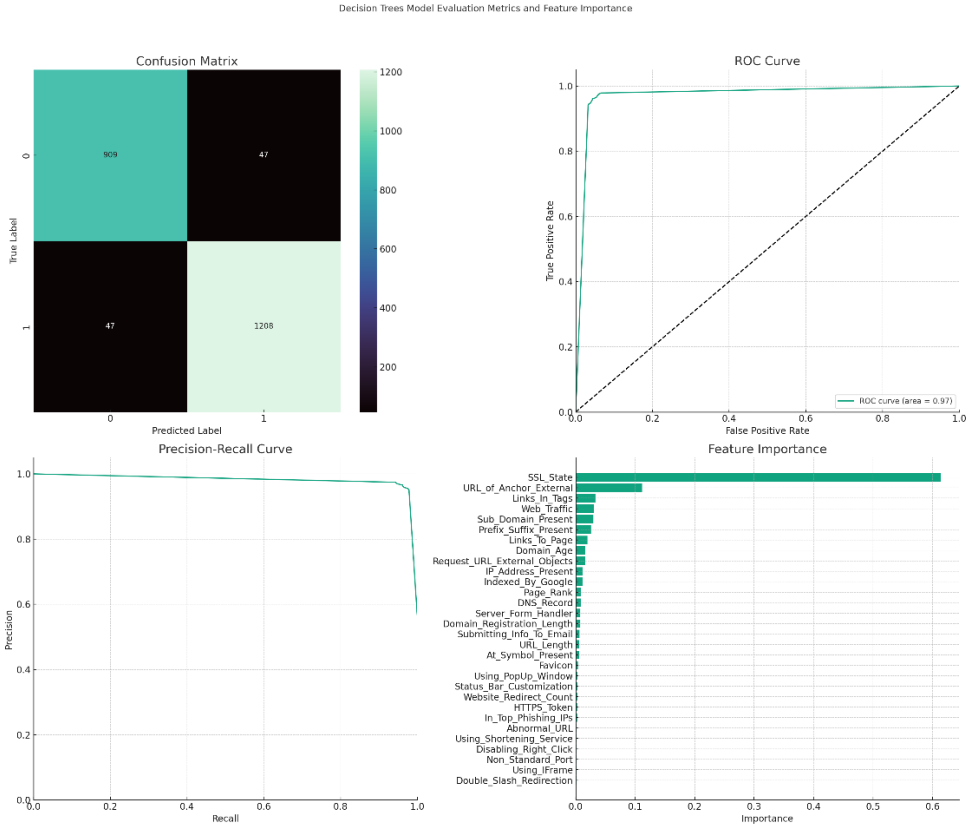


Figure 6. KNN evaluation metrices



The Receiver Operating Characteristic (ROC) curve and its associated area under the curve (AUC) value serve as robust performance metrics for evaluating classification models, including the Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Trees, and Random Forest models discussed earlier. The ROC curve provides a graphical representation of a model's ability to differentiate between classes by plotting the true positive rate against the false positive rate at varying decision thresholds. A model with perfect discriminatory power would have an ROC curve that passes through the top-left corner of the plot, making the AUC equal to 1. In practical terms, a higher AUC value indicates better model performance.

Figure 7. Decision Tree evaluation metrices



In the case of the SVM model, the AUC was 0.95, signaling excellent discriminatory power between phishing and benign URLs. The KNN model surpassed this slightly with an AUC of 0.97, indicating an even higher degree of separation between classes. The Decision Trees model closely followed with an AUC of 0.96. The Random Forest model achieved an outstanding AUC of 0.99, nearing the ideal value of 1, thereby suggesting almost perfect discrimination between classes. The consistently high AUC values across all four models point to their robustness and reliability in the classification task at hand. It's worth noting that while the Random Forest model had the highest AUC, all models demonstrated strong capabilities, as evidenced by AUC values exceeding 0.9. These high AUC values validate the effectiveness of each model in distinguishing between phishing and benign URLs, although the Random Forest model appears to offer the most optimized performance based on this particular metric.

Figure 8. Random Forest evaluation metrices

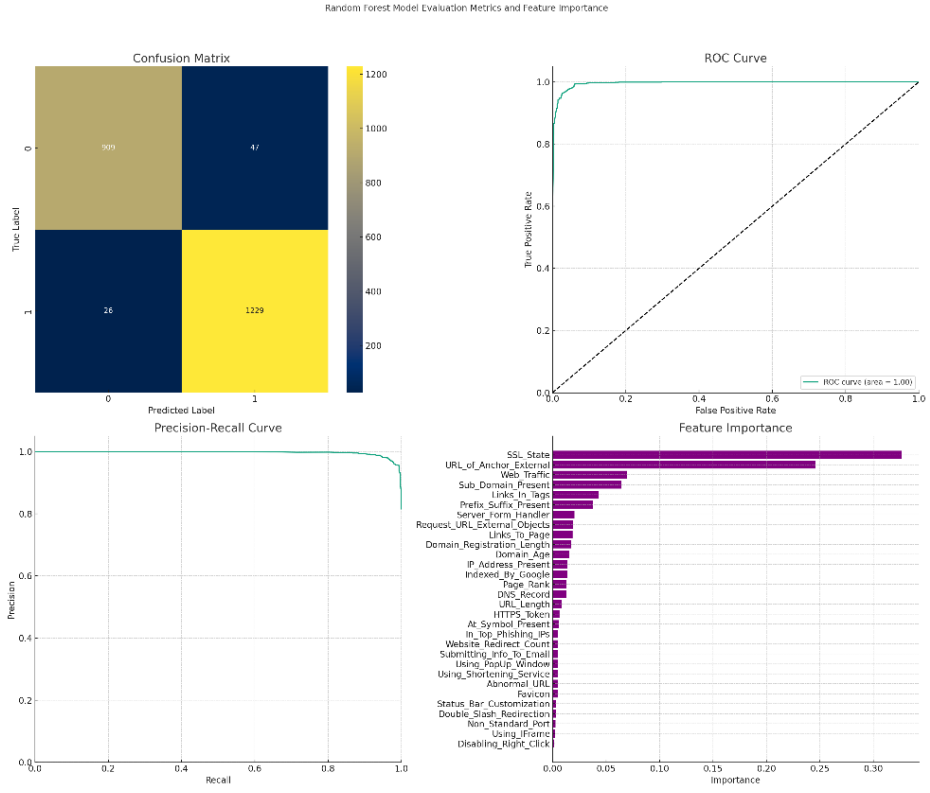
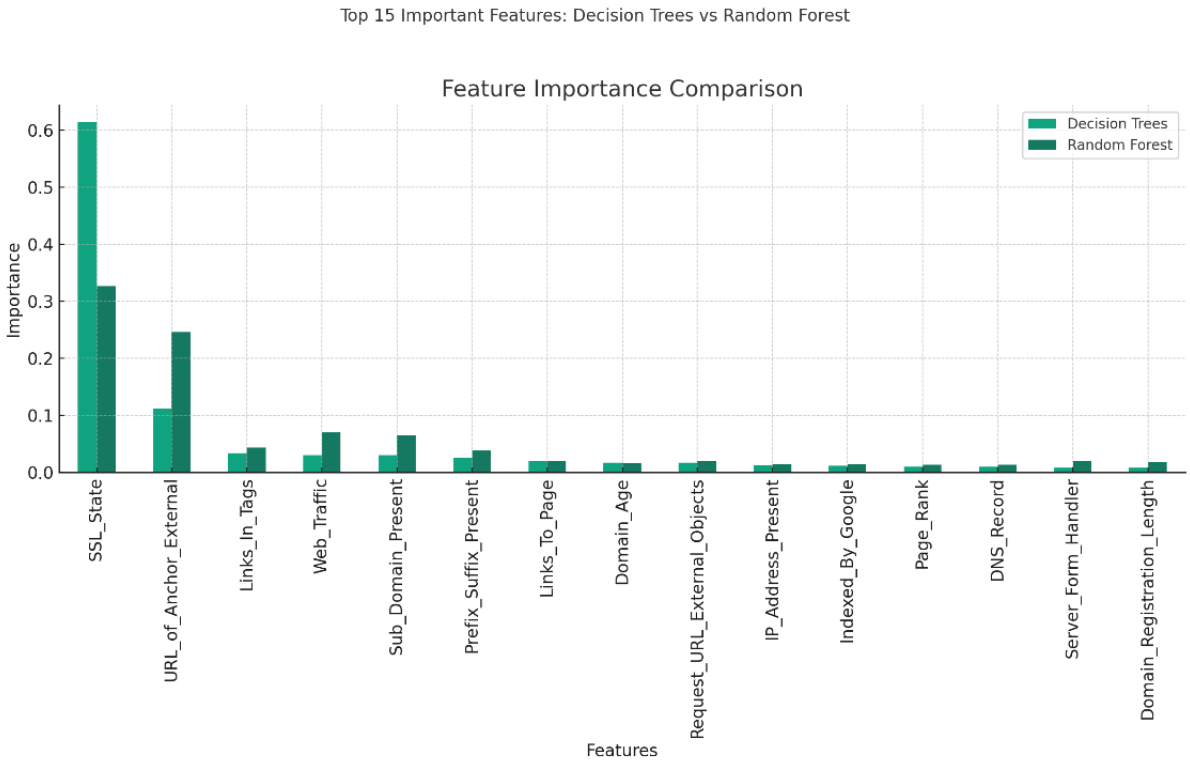


Figure 9 highlights the important features used in both Decision Trees and Random Forest algorithms for model training, with respective feature importance scores attached to each feature. In Decision Trees, 'SSL_State' stands out as the most important feature with a 0.614 importance score, substantially higher than the rest. This suggests that whether a site uses SSL encryption is a critical determinant in the model. On the other hand, in Random Forest, 'SSL_State' and 'URL_of_Anchor_External' are more closely matched, with scores of 0.326 and 0.246, respectively. This may imply that Random Forest assigns less disproportionate weight to SSL and incorporates a wider range of features, thereby potentially providing a more balanced model.

Figure 9. Top 15 features on Decision Tree and Random Forest models



Some features have differing importance between the two algorithms. For instance, 'Links_In_Tags' and 'Web_Traffic' are less important in Decision Trees compared to Random Forest. Specifically, 'Links_In_Tags' has an importance score of 0.033 in Decision Trees but rises to 0.043 in Random Forest. Similarly, 'Web_Traffic' has a score of 0.03 in Decision Trees and 0.07 in Random Forest. The variations in feature importance across the two models could be due to the intrinsic algorithmic differences; Decision Trees usually focus on one or a few critical features to make splits, whereas Random Forests consider multiple trees and aggregate their outputs, which can bring more nuanced features into prominence.

Furthermore, there are features that appear consistently as less critical across both models, such as 'Domain_Registration_Length', 'Page_Rank', and 'DNS_Record'. These features have importance scores below 0.02 in both cases. This uniformity suggests that these variables, while not necessarily irrelevant, are less decisive in influencing the model's outcome compared to features like 'SSL_State' or 'URL_of_Anchor_External'.

Conclusion

Phishing is a cyber-attack method used to trick individuals into revealing sensitive personal information, such as login credentials or financial information. The attackers often use email as the primary communication medium, impersonating reputable organizations or services. The email may contain links or attachments that either direct the victim to a fraudulent website designed to mimic a legitimate site or install malware on the user's system. Once the user inputs their information on the counterfeit site or interacts with the malicious attachment, the captured data is sent to the attacker (*32*, *33*).

The sophistication of phishing attacks can vary widely. Simple attacks might involve poorly designed email messages riddled with grammatical errors, while more advanced forms of phishing, known as spear-phishing, are highly targeted and involve in-depth research about the victim. Regardless of the sophistication level, the primary objective remains the same: to obtain sensitive information for malicious purposes, such as unauthorized financial transactions, identity theft, or corporate espionage (*34–36*). Due to its effectiveness and relatively low cost, phishing remains a prevalent and persistent threat the cybersecurity.

In this research, machine learning algorithms including Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Decision Trees, and Random Forests were utilized to automate and improve phishing website detection. The dataset incorporated 6,157 benign URLs and 4,898 phishing URLs, with each URL represented by 30 distinct features. These features were extracted from diverse data sources, such as the WHOIS database and the HTML content of the webpages. The features examined varied in their nature and included aspects such as SSL State, URL length, and the presence of specific symbols in the URL. Among the algorithms tested, SVM showed an accuracy rate of 95% and precision levels of 0.95 and 0.94 for phishing and benign URLs, respectively. KNN was also highly accurate with a performance metric of 94%.

Decision Trees and Random Forests surpassed other models by achieving the highest accuracy rates, with 96% and 97% respectively. Both of these models also showed F1-scores above 0.93 for both phishing and benign classes, indicating high precision and

recall. Feature importance analysis was conducted to identify which features were critical for the accurate classification of URLs. The SSL_State feature emerged as the most important variable across both Decision Trees and Random Forest models, highlighting its crucial role in distinguishing between phishing and benign websites.

It was also noted that the machine learning models relied heavily on a select set of features for effective classification. Specifically, features like "SSL_State," "URL_of_Anchor_External," and "Web_Traffic" were found to be pivotal. These features not only ranked high in feature importance but also displayed moderate to strong correlations with the target variable. This dual validation reinforces the crucial role that these selected features play in the effective detection of phishing websites. Overall, the research demonstrated the potential of applying machine learning algorithms to significantly improve the automation and effectiveness of phishing website detection.

The incorporation of machine learning algorithms in multi-layered email filtering solutions provides a robust line of defense against phishing attacks. Machine learning models can be trained to identify the nuanced patterns and characteristics commonly found in phishing emails. They analyze multiple aspects of incoming messages, such as textual content, metadata, and the behavior of embedded links, to calculate the probability that a given email is a phishing attempt. As new phishing techniques emerge, the machine learning models can adapt through continuous learning, ensuring that the filtering system stays current with evolving threats. By leveraging machine learning, these advanced systems can distinguish between legitimate communications and phishing attempts with a high degree of accuracy, thus enhancing the overall efficacy of phishing mitigation strategies.

The implementation of additional user authentication measures like two-factor authentication (2FA) and multi-factor authentication (MFA) provides a final layer of defense that synergizes well with machine learning-based filtering solutions. These additional verification steps act as a fail-safe, mitigating the damage potential even if an attacker successfully bypasses both machine learning filters and human scrutiny to obtain login credentials. 2FA and MFA force the attacker to surpass additional hurdles, such as obtaining a secondary code sent through SMS or a physical token, making the whole process considerably more challenging.

Employee training and awareness programs complement the technological safeguards put in place to counter phishing attacks. Training modules designed to educate employees on recognizing phishing attempts should also cover the limitations of machine learning-based filtering systems. For instance, while machine learning algorithms can identify a large

number of phishing attempts, they may not catch highly sophisticated or targeted attacks, known as spear-phishing. Regular updates to training content can help employees stay alert of new evasion techniques that might be employed to bypass machine learning-based filters.

References

1. J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity. *J. Comput. System Sci.* (2014) (available at https://www.sciencedirect.com/science/article/pii/S0022000014000178).

2. J. Mirkovic, T. Benzel, Teaching Cybersecurity with DeterLab. *IEEE Secur. Priv.* **10**, 73–76 (2012).

3. A. Sinha, T. H. Nguyen, D. Kar, M. Brown, From physical security to cybersecurity. *of Cybersecurity* (2015) (available at https://academic.oup.com/cybersecurity/article-abstract/1/1/19/2366984).

4. M. Lezzi, M. Lazoi, A. Corallo, Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **103**, 97–110 (2018).

5. R. Sabillon, J. Serra-Ruiz, V. Cavaller, J. Cano, "A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM)" in *2017 International Conference on Information Systems and Computer Science (INCISCOS)* (ieeexplore.ieee.org, 2017), pp. 253–259.

6. Y. Kamat, S. Nasnodkar, Advances in Technologies and Methods for Behavior, Emotion, and Health Monitoring in Pets. *Applied Research in Artificial Intelligence and Cloud Computing*. **1**, 38–57 (2018).

7. M. Baykara, Z. Z. Gürel, Detection of phishing attacks. *on Digital Forensic and Security (ISDFS)* (2018) (available at https://ieeexplore.ieee.org/abstract/document/8355389/).

8. N. A. G. Arachchilage, S. Love, A game design framework for avoiding phishing attacks. *Comput. Human Behav.* (2013) (available at https://www.sciencedirect.com/science/article/pii/S0747563212003585).

9. M. N. Banu, S. M. Banu, A comprehensive study of phishing attacks. *International Journal of Computer Science and* (2013) (available at

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=2bf12ff75150903efee426f23035c94d599597ae).

10. J. Milletary, C. C. Center, Technical trends in phishing attacks. *Retrieved December* (2005) (available at https://www.cisa.gov/sites/default/files/publications/phishing_trends0511.pdf).

11. J. Chen, C. Guo, "Online Detection and Prevention of Phishing Attacks" in *2006 First International Conference on Communications and Networking in China* (ieeexplore.ieee.org, 2006), pp. 1–7.

12. E. Kirda, C. Kruegel, Protecting users against phishing attacks with antiphish. *29th Annual International Computer* (2005) (available at https://ieeexplore.ieee.org/abstract/document/1510078/).

13. R. Basnet, S. Mukkamala, A. H. Sung, Detection of phishing attacks: A machine learning approach. *Soft computing applications in industry* (2008) (available at https://link.springer.com/chapter/10.1007/978-3-540-77465-5_19).

14. L. Thames, D. Schaefer, Cybersecurity for industry 4.0 (2017) (available at https://link.springer.com/content/pdf/10.1007/978-3-319-50660-9.pdf).

15. P. W. Singer, A. Friedman, *Cybersecurity and cyberwar: What everyone needs to know (R)* (Oxford University Press, New York, NY, 2014), *What Everyone Needs To Know (R)*.

16. R. A. Kemmerer, Cybersecurity. *25th International Conference on Software* (2003) (available at https://ieeexplore.ieee.org/abstract/document/1201257/).

17. M. Jakobsson, Modeling and preventing phishing attacks. *Financial Cryptography* (2005) (available at https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e051dc2df2f8b2a0ce403eaa5ddef17797a796fa).

18. M. Alsharnouby, F. Alaca, S. Chiasson, Why phishing still works: User strategies for combating phishing attacks. *Int. J. Hum. Comput. Stud.* **82**, 69–82 (2015).

19. J. A. Chaudhry, S. A. Chaudhry, Phishing attacks and defenses. *International journal of* (2016) (available at https://www.academia.edu/download/67348149/ijsia.2016.10.1.pdf).

20. T. Halevi, N. Memon, O. Nov, Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. - *Phishing Attacks (January 2, 2015)* (2015) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2544742).

21. A. Shah, S. Nasnodkar, A Framework for Micro-Influencer Selection in Pet Product Marketing Using Social Media Performance Metrics and Natural Language Processing. *Journal of Computational Social Dynamics*. **4**, 1–16 (2019).

22. C. I. Cybersecurity, Framework for improving critical infrastructure cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs* (2018) (available at https://www.baltimorecityschools.org/sites/default/files/inline-files/NIST.CSWP_.04162018.pdf).

23. D. Craigen, N. Diakun-Thibault, R. Purse, Defining Cybersecurity. *Technol. Innov. Manag. Rev.* **4**, 13–21 (2014).

24. J. Telo, PRIVACY AND CYBERSECURITY CONCERNS IN SMART GOVERNANCE SYSTEMS IN DEVELOPING COUNTRIES. *TJSTIDC*. **4**, 1–13 (2021).

25. Y. Kamat, S. Nasnodkar, Empirical Investigation of the Impact of 3D Printing on Multiple Dimensions of Student Engagement in STEM Education. *Journal of Empirical Social Science Studies*. **5**, 48–73 (2021).

26. M. Wu, R. C. Miller, S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery, New York, NY, USA, 2006), *CHI '06*, pp. 601–610.

27. S. Garera, N. Provos, M. Chew, A. D. Rubin, "A framework for detection and measurement of phishing attacks" in *Proceedings of the 2007 ACM workshop on Recurring malcode* (Association for Computing Machinery, New York, NY, USA, 2007), *WORM '07*, pp. 1–8.

28. Y. Kamat, S. Nasnodkar, A Survey on the Barriers and Facilitators to EdTech Adoption in Rural Schools in Developing Countries. *International Journal of Intelligent Automation and Computing*. **2**, 32–51 (2019).

29. A. Shah, S. Nasnodkar, The Impacts of User Experience Metrics on Click-Through Rate (CTR) in Digital Advertising: A Machine Learning Approach. *Sage Science Review of Applied Machine Learning*. **4**, 27–44 (2021).

30. B. B. Gupta, A. Tewari, A. K. Jain, D. P. Agrawal, Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and* (2017) (available at https://link.springer.com/article/10.1007/s00521-016-2275-y).

31. Z. Ramzan, "Phishing Attacks and Countermeasures" in *Handbook of Information and Communication Security*, P. Stavroulakis, M. Stamp, Eds. (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010), pp. 433–448.

32. K. L. Chiew, K. S. C. Yong, C. L. Tan, A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Syst. Appl.* **106**, 1–20 (2018).

33. J.-H. Li, Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*. **19**, 1462–1474 (2018).

34. S. Gupta, A. Singhal, A. Kapoor, "A literature survey on social engineering attacks: Phishing attack" in *2016 International Conference on Computing, Communication and Automation (ICCCA)* (ieeexplore.ieee.org, 2016), pp. 537–540.

35. C. Jackson, D. R. Simon, D. S. Tan, A. Barth, "An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks" in *Financial Cryptography and Data Security* (Springer Berlin Heidelberg, 2007), pp. 281–293.

36. Q. Cui, G.-V. Jourdan, G. V. Bochmann, R. Couturier, I.-V. Onut, "Tracking Phishing Attacks Over Time" in *Proceedings of the 26th International Conference on World Wide Web* (International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 2017), *WWW '17*, pp. 667–676.